



*Sustainable Energy Authority of Ireland*

## **CODE OF GOVERNANCE FRAMEWORK**

**Version: 5 February 2025**

## **Table of Contents**

### **Contents**

- 1. Introduction**
  - 2. Code of Governance Framework**
  - 3. Code of Business Conduct**
  - 4. Obligations**
  - 5. Review of Code**
  - 6. Procedures for the Conduct of Board Meetings**
- 

### **Appendices**

- 2.4 Appendix 1 – Formal Schedule of Matters for Board Decision**
- 2.5 Appendix 2 – Code of Business Conduct for SEAI Board Members/Employees**
- 2.6 Appendix 3 – Functions of the Board Secretary**
- 2.7 Appendix 4 – Committees of the Board**
- 2.8 Appendix 5 – Policy for Dealing with Conflicts of Interest**
- 2.9 Appendix 6 – Procedure for Dealing with Conflicts of Interest**
- 2.10 Appendix 7 - SEAI Internal Audit Charter**
- 2.11 Appendix 8 – Procedure for Board members to obtain Independent Professional Advice**
- 2.12 Appendix 9 - Principles of a Quality Customer Service for Customers and Clients of the Public Service (1997)**
- 2.13 Appendix 10 - SEAI Protected Disclosures (Whistleblowing) Policy & Procedure, Disclosures Policy**
- 2.14 Appendix 11 - SEAI Anti-Fraud, Bribery & Corruption Policy V3**
- 2.15 Appendix 12 – Business Continuity Policy V3.1**
- 2.16 Appendix 13 – Risk Management Policy & Operational Framework V3.4**
- 2.17 Appendix 14 - Data Protection Policy V.3**
- 2.18 Appendix 15 - Data Breach Policy and Procedure V.1**
- 2.19 Appendix 16 - Organisation Chart**
- 2.20 Appendix 17 - Delegated Authorities Framework Overview**
- 2.21 Appendix 18 – SWIFT 3000 Certification**
- 2.22 Appendix 19 – ISO27001:2022 Certification**

## 1. Introduction

The Sustainable Energy Authority of Ireland (SEAI) is committed to operating to the highest standards of efficient and effective corporate governance.

This is particularly important given the values that drive the approach and behaviour of SEAI and the need for the Authority to subject itself to the highest standards of scrutiny.

The SEAI Strategy for the period 2022- 2025, approved by the Board in January 2022, and as approved by the Minister for Environment Climate and Communications, in accordance with the Code of Practice for the Governance of State Bodies, sets out the following Strategic Goals:

- Delivering our targets
- Communicating our message
- Collaborating with others
- Building capacity and developing knowledge
- Engaging with and supporting staff.

The Strategy sets out that the achievement of these goals is underpinned by a strong Corporate Governance Framework through accountability, transparency and probity. There will be a focus on the sustainable success of the organisation over the longer term.

This SEAI Code of Governance Framework, which is approved by the Board on an annual basis, sets out the systems and processes by which the Authority directs and controls its functions and manages its business. It is intended to guide the Board (and staff, where appropriate) of the Authority in performing their duties to the highest standards of accountability, integrity and propriety. It also brings together the policies and procedures for corporate governance into one reference point and contains the following key documents:

- **Code of Governance Framework**

This Code sets out the appropriate structures and procedures to ensure that the governance and accountability arrangements are robust and effective across the Authority.

- **Code of Business Conduct**

This Code sets out the guidelines for ensuring that the Authority conducts its business to the highest possible standards of integrity and ethics and reflects the obligations on staff, Board members and individuals contracted by the Authority in carrying out their public duties.

- **Conduct of Board meetings**

The procedures adopted by the Board of the Authority for the conduct of meetings of the Board are set out.

- **Formal Schedule of Matters for Board Decision**

This Schedule outlines the matters specifically reserved to it for decision to ensure that the direction and control of the Authority is firmly managed by the Board.

- **Duties and responsibilities of the Chair, Board members and CEO**

This sets out the overall responsibilities of the SEAI Chair, CEO and Board members.

- **Functions of the Board Secretary**

This sets out the functions performed by the Board Secretary.

- **Committees of the Board**

This sets out the general rules for Committees of the Board, a list of the Committees established by the Board and the membership and the Terms of Reference for those Committees.

- **Conflict of Interest Policy**

This Policy reflects the emphasis, which the Authority places on the avoidance of occasions where conflicts of interest may arise and sets out principles for the management of real and potential conflicts of interest.

- **Conflict of Interest Procedure**

This procedure sets out the practical means by which a conflict of interest or potential conflict of interest situation is managed.

- **Code and Charter for the Internal Audit Function**

This sets out a formal charter for the internal Audit function. The Code includes an internal audit reporting structure and the Terms of Reference for the function and reflects the specific requirements of the Code of Practice for the Governance of State Bodies.

- **Principles of Quality Customer Service for Customers and Clients of the Public Service.**

This document outlines these principles that are actively promoted by the Authority.

- **Organisation Chart**

This document sets out the current organisation structure.

- **Protected Disclosures/Disclosures Policy**

This document sets out the SEAI Protected Disclosures Policy and Procedures/Disclosures Policy, which has been revised in the context of the Protected Disclosures (Amendment) Act 2022.

- **Risk Management Framework**

This document sets out the comprehensive overall SEAI Risk Management framework.

- **Business Continuity and Fraud Policies**

This document sets out the Business Continuity and Fraud Policies approved by the Board.

**Overall, it is intended that this Code of Governance Framework will be part of the induction programme for Board members and staff and will be subject to annual review by the Board and updated as required.**

## **2. Code of Governance Framework**

### **2.1 Context**

In accordance with the provisions of the Sustainable Energy Act 2002 and informed by the Framework for Corporate and Financial Governance as well as the Code of Practice for the Governance of State Bodies (revised in August 2016 and updated by Annex 2020 in September 2020), this Code of Governance Framework for the Authority was originally compiled and approved by the Board at its meeting on 2 June 2010. A copy of the Code had been forwarded to the Department of Environment Climate and Communications (DECC) and it is published on the SEAI Website.

The Board has agreed to keep this Code under continuous review and to update it on an annual basis in accordance with the development of the Authority and any additional new public sector requirements. The Board approved this latest version in February 2025.

This Code provides for appropriate structures and procedures to ensure a robust framework for the governance and accountability of the Sustainable Energy Authority of Ireland.

### **2.2 Definitions**

In this Code of Governance Framework, the following expressions, unless the context otherwise requires, have the following meanings: -

*'Act', the Sustainable Energy Act 2002, establishing the Sustainable Energy Authority of Ireland, as amended by the Energy Act 2016.*

*'Authority', the Sustainable Energy Authority of Ireland established under the Act.*

*'Board', the Board of the Authority, appointed by the Minister under the Act.*

*'Chief Executive Officer' or 'CEO', a person appointed to the post of Chief Executive Officer of the Authority.*

*'Minister' means the Minister for the Environment, Climate and Communications.*

### **2.3 The Authority - Introduction**

The Authority is a body corporate with functions and responsibilities as set out under Section 6 of the Act. This Code of Governance Framework sets out a corporate governance best practice framework within which the Authority wishes to operate. It includes standards of conduct and probity that the Board Members, staff members and anybody contracted by the Authority are required to observe. Members of the Board, the staff or anybody contracted by the Authority subscribe to an identified Code of Business Conduct.

#### **The key functions of the Authority are as follows:**

The Functions of the Authority as set out in Section 6 of the Sustainable Energy Act 2002 are as follows:

#### **6.— (1) The functions of the Authority shall be—**

- a) to promote and assist environmentally and economically sustainable production, supply and use of energy,
- b) to promote and assist energy efficiency and renewable sources of energy,
- c) to promote and assist the reduction of greenhouse gas emissions and transboundary air pollutants associated with the production, supply and use of energy,
- d) to promote and assist the minimising of the impact on the environment of the production, supply and use of energy,

- e) to promote and assist research, development and demonstration of technologies connected with the foregoing paragraphs of this subsection,
- f) to provide advice, information and guidance—
  - i. to the Minister and such other Ministers or bodies as the Minister may direct, and
  - ii. to energy suppliers and users,

relating to the matters specified in the foregoing paragraphs of this subsection.

- (2) The Authority shall have all such powers as are necessary for or are incidental to the performance of its functions under this Act, including—

- a) co-operating with the Central Statistics Office and acting as an agent of that Office in relation to matters related to the functions of the Authority,
- b) the compilation, extraction and dissemination of information and projections relating to energy production and use (including implications relating to the sourcing, transformation, transmission, distribution and emissions thereof),
- c) the licensing, regulation and control of activities related to the functions were directed by the Minister from time to time,
- d) the initiation, development, administration, participation in and promotion of schemes and programmes of action,
- e) the promotion of and assistance with participation in international programmes,
- f) the provision of assistance in the co-ordination of activities carried out in the State related to sustainable energy,
- g) the assessment of energy technologies and markets for the purpose of promoting best practice,
- h) encouraging the establishment and development of companies involved in the provision of services,
- i) the exchange of information with organisations outside the State and participation in international activities,
- j) representation of a Minister of the Government at meetings of international bodies were requested to do so by the Minister,

in connection with the matters referred to in *subsection (1)*.

- (3) The Authority may perform any of its functions through or by a member of its staff duly authorised by the Authority in that behalf.

- (4) The Authority shall have all such powers as are necessary for or are incidental to the performance of its functions under this Act.

## **2.4 Guiding Principles of the Authority**

The Authority will observe the highest standards of probity in relation to the stewardship of public funds and the exercise of its functions; maximise value for money, through ensuring that duties are delivered in the most economical, efficient, and effective way, within available resources; and demonstrate adherence to the Authority's core functions in accordance with the Act. The Authority is accountable to the body public and the Minister, for its activities, its stewardship of public funds and the extent to which key performance targets and objectives have been met. The SEAI Strategy for the period 2022-2025 and the underpinning annual business plans sets out the specific targets and key performance indicators and metrics.

## **2.5 Structure of the Authority**

### **2.5.1 Introduction**

Section 10 of the Act provides that the Board is the governing body of the Authority with the power to perform the functions of the Authority. The Chief Executive Officer (CEO) is responsible to the Board for the implementation of the Board's policies. The CEO, in turn, delegates or sub delegates functions to the Senior Management Team.

### **2.5.2 Duties and responsibilities of the Chairperson:**

Overall, the Chair should display high standards of integrity and probity and set expectations regarding culture, values, and behaviour for SEAI and for the tone of discussions at the SEAI Board. He/she should ensure that Board discussion and dialogue is both constructive and challenging and promotes a culture of openness and debate by facilitating the effective contribution of all Board members and key staff.

The specific duties of the Chairperson are as follows:

- Effective management of the Board Agenda and ensuring that adequate time is available for discussion on all Agenda items, and in particular, strategic issues.
- representing the Authority in its dealings with the Minister in order to ensure that the Minister is advised of matters relating to the Authority.
- ensuring effective communication with stakeholders
- providing effective leadership to the Board and ensuring that the Board is supplied with the relevant information which is accurate, timely and clear and which is of suitable quality to enable Board members to carry out their duties in a satisfactory and appropriate manner.
- ensuring Board members understand their respective roles and responsibilities and that the Board works effectively and efficiently.
- ensuring that the Board meets regularly (normally the SEAI Board meets on 9-11 times a year) and that the collective responsibility and authority of the Board is safeguarded.
- chairing the meetings and ensuring that the minutes of the meeting accurately record the decisions taken and, where appropriate, the views of individual Board members
- ensuring that all meetings of the Board are conducted in accordance with the approved procedures and the Authority's Code of Business Conduct
- establishing all relevant Board Committees. This shall include an Audit and Risk Committee, and any other Committees considered necessary.
- confirm to the Minister for the Environment Climate and Communications that the Authority has complied with the Codes of Business Conduct
- ensuring that the Board, in reaching decisions, takes proper account of guidance provided by the Minister.
- submitting to the Minister for the Environment Climate and Communications, in conjunction with the Annual Report and Financial Statements of SEAI, a comprehensive report in accordance with the Business and Financial requirements section of the revised Code of Practice for the Governance of State Bodies (August 2016).
- confirming annually to the Minister for the Environment Climate and Communications that the Authority has a system of internal controls in place in accordance with the revised Statement of Internal Controls (SIC) as set out in the Code of Practice for the Governance of State Bodies.

### **2.5.3 Duties and Responsibilities of Board Members**

Board members have a fiduciary duty to act in good faith and in the interests of SEAI. They should bring an independent judgement to bear on issues of strategy, performance, resources, key appointments, and standards of conduct.

The Board members (including the Chairperson) shall have collective responsibility to:

- provide leadership and direction to SEAI within a framework of prudent and effective controls which enables risk to be assessed and managed.
- establish the strategic direction of the Authority, within the framework laid down by the Act. The Board should also agree on the strategic aims of SEAI with the Minister and DECC, to the extent relevant, and ensure optimal use of resources to meet its objectives to direct, support and evaluate the CEO.
- ensure that the Authority complies with all statutory and administrative requirements for the use of public funds.
- fully engage in impartial and balanced consideration of all issues and ensure that the Authority has an appropriate system of internal controls in accordance with the Code of Practice for the Governance of State Bodies.
- ensure compliance with and approve the overall risk management and risk appetite framework and monitor its effectiveness. In practice, this activity is delegated to the Audit and Risk Committee, which reports to the Board on a regular basis.
- contribute to any Committee of the Board, as appropriate.
- share corporate responsibility for all Board decisions.
- be objective in their work on behalf of the Authority.
- ensure full compliance with Conflict-of-Interest Policy and Procedure and Codes of Governance and Business Conduct
- treat documents marked for non-disclosure as confidential to themselves, not discuss them with others outside the Authority, and liaise with the Board Secretary in relation to disposal.
- put in place procedures whereby employees of the Authority, may, in confidence, raise concern about possible irregularities in financial reporting or other matters and for ensuring meaningful follow up of matters raised in this way.

In addition, each Board member is individually responsible for:

- on appointment to the Board, furnishing to the Secretary to the Board, details relating to his/her employment and all other business interests including shareholdings, professional relationships, etc. which could involve a conflict of interest or could materially influence the member in relation to the performance of his/her functions as a member of the Board.
- complying with all aspects of this Code of Governance Framework, which includes their declaration of all relevant interests.
- informing the Board, via the Chairperson, of any new appointments they accept which may impinge on, or conflict with, their duties as a Board member.
- acting in good faith and in the best interests of the Authority
- not disclosing, without the consent of the Board, save in accordance with law, any information obtained by him or her while performing duties as a member of the Board, responding to any information requests made directly to him or her relating to the activities of the Authority, including referring any request to the Chairperson (or the Secretary of the Authority on his or her behalf) for appropriate processing.
- not misusing information gained in the course of their public service for personal gain or political purpose.



- ensuring, in so far as possible, a 100% attendance at all Board and Committee meetings

#### **2.5.4 Key Duties and Reporting Responsibilities of the Board corporately**

To ensure continued integrity and transparency, and to avoid public concern or loss of confidence, the Board should ensure that appropriate policies are in place so that members of staff take decisions objectively and steps are taken to avoid or deal with any potential conflicts of interest, whether actual or perceived. These policies should ensure that any potential or actual conflicts of interest, arising in the case of decision making by Board members and employees, are addressed.

The Board shall also execute the following functions:

- The Board shall have a formal schedule of matters specifically reserved to it for decision.
- In a Board resolution, lay down formal procedures whereby Board Members, in the furtherance of their duties, may take independent professional advice, if necessary, at the reasonable expense of the Authority.
- The preparation and adoption of a strategic plan is a primary responsibility of the Board. Such plans should set appropriate objectives and goals and identify relevant indicators and targets against which performance can be clearly measured. In this regard, the Board should adopt a statement of strategy for a period 3-5 years ahead and the implementation of the strategy by the management should be supported through the annual planning and budgeting cycle. The SEAI Strategy for 2022-2025 was approved by the Board in January 2022 and is published on the SEAI Website. It was formally launched in June 2022 following consultations with the Minister, in accordance with the Code of Practice for the Governance of State Bodies.
- The Board holds and retains overall responsibility for the discharge of the key functions specified in the Act. It shall comply with all statutory regulations and legal obligations, which apply to the Authority. Where individual Board members become aware of any non-compliance, they are required to bring this to the attention of the Board with the intention of having the matter rectified. The matter shall also be brought to the attention of the Minister by the Chairperson.
- The Board is vigilant in ensuring that the Chairperson advises the Minister on any matter relevant to him/her as principal stakeholder and of any significant matter of public concern.
- The Minister is notified of any matter for his/her decision or direction as required by the Act.
- An Annual Report shall be submitted to the Minister and published. In addition, the accounts shall be provided to the Minister and the Minister for Finance/ Minister for Public Expenditure and Reform, where applicable, as required by this Code of Governance.
- The Board shall approve financial and accounting policies and supervise the production and submission of Annual Accounts. In the context of the Annual Statement of Accounts, the Board shall report that the Authority is a going concern along with any assumptions or qualifications, which are necessary.
- The Board shall seek all necessary information to ensure that the Annual Report to the Minister and the Annual Accounts present a balanced and understandable assessment of the Authority's position and performance.
- The Annual Report and Financial Statements shall also include the relevant information and comply with the reporting requirements as set out in the Business and Financial Reporting Annex to the revised Code of Practice for the Governance of State Bodies (2016). It should also comply with the specific requirements of the Guide to the Implications for the Annual Financial Statements and the Annual Report issued by the C&AG, in consultation with the Department of Public Expenditure and Reform in November 2017.
- The Annual Accounts shall include details of fees paid to each Board Member, the expenses paid to the Board, broken down by category, and the salary of the CEO, payments made to the CEO under performance-related pay schemes (if applicable) and the total value of the CEO's superannuation benefits or any additional benefits provided.

- The Annual Accounts are audited by the Comptroller and Auditor General either directly or on an outsourced basis, reporting to the C&AG. The Board through its Audit and Risk Committee should have a discussion with the external auditors at least once a year, without employees of the Authority present, to ensure that there are no unresolved issues of concern.
- The Board shall approve the internal control structure of the Authority and receive periodic reports on the effectiveness of these provisions. Internal controls should be reviewed annually as part of the Statement of Internal Controls as required by the Code of Practice for the Governance of State Bodies. The Board is required to confirm annually to the Minister for Environment Climate and Communications that SEAI has a system of internal control in place.
- The Board should approve the annual business plans and should formally consider an evaluation of performance by reference to the plan and budget on an annual basis and reflect this, as appropriate, in the Annual Report.
- The Board shall ensure that decisions on all major items of expenditure should be aligned with medium to long-term strategies to ensure that such expenditure is focussed on clearly defined objectives and outcomes. A performance measurement system should be put in place to assess the effectiveness and outcomes, and these should be reported to the Board.
- The Board shall approve capital and current/revenue budgets and monitor expenditure.
- The Board shall select and appoint the CEO. The succession to the post of CEO and the recruitment procedure for the appointment, which involves public advertisement, shall be a primary concern of the Board. It shall approve the related contract of employment, including remuneration, in consultation with the Department of Environment Climate and Communications and the Department of Finance/Public Expenditure and Reform and institute a process of annual performance appraisal.
- The Board shall be responsible for the appointment and the removal (if necessary) of the Board Secretary.
- The Board shall approve procedures for the making of all senior appointments to ensure objectivity and the quality of these appointments.
- Contracts for the acquisition and disposal of major assets and all transactions (grants, procurements etc.) in excess of €1m capital and current, shall be approved by the Board in accordance with processes, including electronic circulation, as approved by the Board. The revised Delegation of Authority Framework (DAF) was approved by the Board in July 2022. Specific delegations from this arrangement may be agreed by the Board in relation to the operation and Terms of Reference of certain Committees, as appropriate.
- The Board should satisfy itself that the requirements for public procurement are adhered to and are fully conversant with the current value thresholds for the application of EU and national procurement guidelines and rules/regulations.
- The Board, through the CEO and senior management, shall ensure the appropriate expertise of the personnel responsible for the purchasing function of the Authority and that they are properly conversant with all developments in this area.
- The Board shall ensure that, in the event of payment of grants, subsidies and similar type payments all Tax Clearance requirements as set out in Department of Finance Circulars 43/2006, 44/2006 updated March 2020 relating to Public Sector Contracts, are adhered to.
- Where the Authority proposes the establishment of joint ventures, subsidiaries, or an expansion of the Authority's current remit, the Board shall be required to receive approval in relation to same from the Minister.
- The Board shall ensure that a robust and qualified Executive Leadership Team (ELT) and Senior Management Team (SMT) structure are in place.
- The Board shall meet at least twice a year, without Executive Board members or SEAI management present, to discuss any matters deemed relevant.
- The Board shall appoint Committees as it sees fit and determine their Terms of Reference.
- The Board should constantly review its own operation and seek to identify ways of improving its effectiveness.

### **2.5.5 Senior Independent Board Member (SIBM).**

The SEAI Board shall select a Senior Independent Board Member (SIBM). The rationale and role for the position are as follows.

#### **Rationale**

- The role of the SIBM is designed to support the process of creating an effective Board and one which is seen to be balanced and independent.

#### **Appointment**

- The SIBM should be appointed by the Board. The Chair should absent himself or herself from any discussion leading to this appointment.
- The appointment should be for not longer than 3 years but may be less if retiring at end of term and/or the maximum time limit for Board membership impacts.

#### **Role**

##### *An Effective Board*

- Led by the SIBM, the non-executive directors should meet without the Chairman present at least annually to appraise the Chairman's performance and on other such occasions as are deemed appropriate. The Senior Independent Board Member may meet Board members on a one-to-one basis or alternatively in a group format.

##### *Board Balance and Independence*

- The SIBM should be available to Board members if they have concerns or wish to raise any matter with the Senior Independent Board Member who may then decide to raise the matter with the Board Chair or Board member(s) or CEO as appropriate.

**Note – The Board appointed Ann Markey as the Senior Independent Board Member (SIBM) on 26 April 2022 for a three-year term.**

### **2.5.6 Duties and Responsibilities of CEO**

The CEO, appointed by the Board, is responsible for:

- reporting to the Board and presenting the Board with strategic and operational plans for its review and approval.
- carrying on, managing, and controlling generally, the administration and business of the Authority and is responsible to the Board for the performance of his/her functions and for the implementation of the policies of the Authority.
- performing such other functions as may be assigned to him or her under the Act or as may be delegated to him or her by the Board.
- supplying the Board with information (including financial information) relating to the performance of his or her functions, as the Board may require.
- complying with all aspects of this Code of Governance Framework, which includes his or her declaration of all relevant interests.
- informing the Board, via the Chairperson, of any new appointment he or she accepts which may impinge on or conflict with, his or her duties as CEO, acting in good faith and in the best interests of the Authority.

- not disclosing, without the consent of the Board, save in accordance with law, any information obtained by him or her while performing duties as CEO.
- not misusing information gained in the course of his or her public service for personal gain or political purpose.

The Chief Executive shall not hold any other office or position or carry on any business, trade, or profession without the consent of the Board.

#### **2.5.7 Internal Audit Function**

SEAI should have a properly constituted independent internal audit process to operate in accordance with the provisions of the Code of Practice for the Governance of State Bodies. The Internal Audit function should be independent of the activities of its audits in order to create an environment where it can make unbiased judgements and provide impartial advice to management. The operation of the Internal Audit function should comply with the Internal Audit Charter, which are included within this Code of Governance Framework. Currently, the SEAI Internal Audit Function is outsourced to Forvis Mazars following a competitive procurement process carried out in September 2022 and will be re-tendered in 2025.

#### **2.5.8 Devolved Functions**

The Board may delegate any of its functions to the CEO. Directors/Heads of departments are individually accountable for assigned areas of delivery and control and are directly responsible to the CEO. Directors/Heads of departments may be required to report periodically to the Board thereon at the CEO's request.

#### **2.5.9 Authority, Membership and Meetings of the Board**

- The Seal of the Authority shall be authenticated by the signature of the Chairperson or such other member of the Authority, authorised by the Board, to act in that behalf, and by the signature of an officer of the Authority, authorised by the Authority in that behalf.
- The Board's authority is derived from Section 10 of the Act 2002 and the appointment of the Chairperson and Board members by the Minister pursuant to the Act.
- The Board shall consist of twelve members (The Chairperson and 11 other members including the CEO, who is an *ex officio* member).
- It is the Chairperson's duty to ensure that no individual member, or interest, has excessive influence on decision-making and that all members have an equal opportunity to participate in debate and final decisions.
- Board decisions are made by consensus or, if necessary, by a majority of the members present. The voting procedure is as laid down in Section 12 (5) of the Act. Decisions of the Board shall be recorded in the minutes.
- Meetings of the Board should take place as are necessary, for the performance of its functions but in any case, not normally less than six times annually.

#### **2.5.10 Board Secretariat**

A full description of this function is set out as part of this Code of Governance Framework

- The Board Secretary is responsible for arranging Board meetings in accordance with the normal procedures adopted by the Board and ensuring that Board procedures are followed, and applicable rules and regulations are complied with.

- Applicable rules include those laid down in the Act and any directions, which may be issued by the Minister.
- All members of the Board have access to the Board Secretary for advice and services.
- The Board Secretary shall ensure induction, training and maintenance of corporate governance material and information for Board members.
- The Board Secretary shall co-ordinate an objective performance management process for the review of the performance of the Chairperson of the Board and the Committees of the Board on a regular basis.
- The Board Secretary will maintain a record of the Seal of the Authority.
- In accordance with the Code of Practice for the Governance of State Bodies, the Board is required to ensure that the person appointed as Secretary of the Board has the skills necessary to discharge their statutory and legal duties and the Board should approve the appointment and removal of the Board Secretary.

#### **2.5.11 Briefing for new Board Members**

- Board members shall undergo orientation through a planned induction programme to ensure that they understand their responsibilities and duties, and the Authority's functions and services, including their obligations in relation to confidentiality and to act in good faith and in the best interests of the Authority.
- The Secretary of the Board shall supply new Board members with appropriate induction material.
- All new Board members shall formally acknowledge in writing that they understand and will comply with their responsibilities as Board members.

#### **2.5.12 Disclosure of Interests**

To avoid conflicts of interest and the possibility of unjust enrichment, members of the Board and staff of the Authority are required to declare/disclose personal or 'connected' interests, which might conflict with those of the Authority. The regulations relating to 'disclosure' form part of the SEAI Code of Business Conduct for Board members, also staff, and the Authority's Conflict of Interest procedure.

### **2.6. Reporting Processes and Guidelines**

#### **2.6.1 Introduction**

It is the responsibility of the CEO, and the Directors to ensure that the Board is supplied with accurate and timely information, which enables it and the Chairperson to perform their respective functions under the Act and their legal obligations and responsibilities to the Minister and other stakeholders.

#### **2.6.2 Performance Management**

Members of the Board shall review the achievements of the Authority and the effectiveness of their individual and collective performance on an annual basis against set objectives for performance improvement.

Evaluation mechanisms of the key strategic objectives and targets of the Authority shall be utilised in accordance with the SEAI Performance Growth Plans. These mechanisms shall include:

- I. financial performance;*
- II. staff performance;*
- III. quality, efficiency and effectiveness of the Authority's operations;*
- IV. customer service;*

#### *V. strategic objectives and milestones.*

The Board shall set performance criteria for the CEO annually, which it shall evaluate through the Performance Management and Remuneration Committee.

The Board shall make a report to the Minister with a progress report of an approved corporate plan for the Authority in its Annual Report and, at the request of the Minister, at other times that the Minister may specify, in accordance with Section 25 of the Act.

The Board shall seek Ministerial approval for any significant amendments to pension benefits of the CEO and staff as appropriate.

### **2.6.3 Board Committees**

The Board shall establish Committees for specified purposes, which can include appointees who are not members of the Board but have special knowledge and experience related to the purpose of the Committee.

The Terms of Reference of Committees shall be determined by the Board. These Committees shall act and furnish reports as directed by the Board.

Additional Committees of the Board shall, but are not limited to, include the Audit and Risk Committee (ARC), the Performance Management and Remuneration Committee (PMRC), the Business and Public Sector Committee (BPSC), the National Retrofit Delivery Body Committee (NRDB), and the Research and Policy Insights Committee (RPIC). All Committees established by the Board shall be evaluated and reviewed by the Board on an annual basis.

The Chair may, with the approval of the Board, establish an “ad hoc” Committee, as appropriate, to oversee a specific issue or process e.g., Selection of a new CEO.

A full list of the Committees, membership of the Committees, the General Rules applying to the Committees and the respective Terms of Reference are included within this Framework.

### **2.7 Internal Controls**

The Board is committed to a strategy, which minimises risks to all of its stakeholders through a comprehensive system of internal controls, whilst maximising potential for flexibility, innovation and best practice in delivery of its strategic objectives. The Board recognises and acknowledges its responsibility for the Authority’s system of internal financial, non-financial and operational controls.

An effective programme of internal controls, incorporated into an overall quality system, will inform the Board in relation to significant risks for which they are responsible. Internal controls shall also assist in the development and review of the Authority’s services.

The internal controls include defined performance indicators, written policies and procedures, clearly defined lines of accountability, and the delegation of authority. It makes provision for comprehensive reporting and analysis of the performance indicators on a regular basis, against approved standards and budgets, as well as compliance with legal/governmental requirements. The responsibility for the adequacy, extent and operations of these systems is delegated to the CEO.

#### **2.7.1 Specific controls have been developed in relation to the following areas:**

- Financial Performance (including Internal Audit)

- Corporate Services (including human resources, facilities, equipment management, health and safety, insurance, legal, records and contract management).
- Research and Policy Insights
- National Retrofit Delivery Body
- Business and Public Sector and Transport
- IT and Cybersecurity

#### **2.7.2 Specific internal control procedures are in place in relation to:**

- internal audit
- risk management
- risk appetite
- public procurement
- financial reporting
- business continuity
- fraud prevention
- delegation of authority framework

These controls are enhanced by the Committees, appointed by the Board, including, but not limited to, the Committees outlined at 2.6.3 above.

Findings/Recommendations arising from Internal Audits carried out by the Internal Audit function are presented to the Audit and Risk Committee and reported to the Board. Follow ups on audit recommendations made are reviewed by the ARC at regular intervals.

### **2.8 Remuneration and Expenses**

Remuneration and allowances for expenses, where applicable, are payable by the Authority out of funds at its disposal to members of the Board and the members of Committees of the Board, in accordance with Section 10 (7) of the Act.

All aspects of travel and subsistence allowances will be in accordance with the Authority's own policies and procedures, which will comply, with any current public sector rate guidelines as issued by the Minister for Finance/ Public Expenditure and Reform.

### **2.9 The Codes of Business Conduct**

The Codes of Business Conduct (separate Codes have been developed for SEAI Staff and SEAI Board members), set out behaviour by which it requires staff and Board Members of the Authority to conduct its duties and is in accordance with the Ethical Principles outlined. These Codes reflect the principles set out in the Code of Practice for the Governance of State Bodies.

The requirements of the Companies' Acts in relation to the behaviour of Board Members (non-Executive Directors) shall inform and apply to the members of the Board.

The Code of Business Conduct for Board members has been adopted by the Board and is published on the SEAI Website. A copy of the Code of Business Conduct for staff members is provided to each staff member and is available in the Employee Information handbook.

The Chairperson shall report to the Minister and affirm that the Codes of Business Conduct are in place and will report on compliance in relation to same.

## **2.10 Quality of Service**

The mission of the Authority is that SEAI is at the heart of delivering Ireland's energy revolution. To achieve this, the Authority has set out a vision of SEAI to be a leading authority, driving Ireland's sustainable energy transformation for the benefit of society.

To achieve these objectives the Board is fully committed to customer quality principles and pursues a comprehensive and continuously reviewed quality improvement programme.

A formal reporting structure is in place so that the Board receives, through the CEO and other nominated officers, regular updates on departmental activities.

In its work, the Authority will be independent in the exercise of its responsibilities and in the discharge of its functions, embody a strong commitment to best international practice and achieving excellence in SEAI work and results. The Authority maintains a creative and open stance to the support of policy, enterprise and technological innovations. SEAI will be open to the adoption of new approaches and flexible in their incorporation into the programmes and structures in pursuit of agreed objectives. The organisation will be results orientated and will transparently measure performance against goals and properly value all stakeholders. SEAI operates a very effective Voice of the Customer feedback process.

The staff of the Authority delivers quality services with courtesy and sensitivity and with minimum delay to foster a climate of mutual respect between the Authority's clients and the staff. Where commercially feasible to do so, the Authority promotes the standards of service outlined in the Government's "Principles of Quality Customer Service for Customers and Clients of the Public Service" (1997) which accompany these Corporate Governance Documents. The Authority also has a Customer Charter in compliance with the Code of Practice for the Governance of State Bodies.

## **2.11. Code of Practice Reports**

The following reports are produced in the context of this Code of Governance:

### **Strategic Plan**

A Strategic Plan must be submitted to the Minister. The Board approved the new SEAI Strategy for 2022-2025 in January 2022 and this was formally launched in June 2022, following appropriate consultation with the Minister for Environment Climate and Communications.

### **Progress Reports**

Progress reports are to be included in the Authority's Annual Report on the implementation of the approved Strategic Plan.

### **Work Programme/Output Statement**

A comprehensive Work Programme is submitted to the Minister in the context of the determination of the proposed expenditure / budget allocations for the coming financial year. In addition, the outputs achieved for each year are demonstrated. The 2023-2026 Oversight Agreement was drawn up by DECC in partnership with SEAI and signed in December 2023. The Performance Delivery Agreement (PDA) sits under the Oversight Agreement and sets out deliverables, targets and metrics for the year. The 2024 PDA was signed in November 2024.



## **Code of Governance Framework**

This Code of Governance Framework has been submitted to DECC. The updated version of the Code will be submitted to the Governance Section in DECC, when approved by the Board.

## **Annual Accounts**

The Annual Accounts of the Authority shall be submitted to the Comptroller and Auditor General for audit as soon as practicable and not later than 3 months after the end of the financial year to which the accounts relate.

## **Annual Report**

The Authority shall prepare an Annual Report in relation to the Authority's functions not later than the 30th of June each year.

## **3. Code of Business Conduct**

### **3.1 Introduction**

The Authority comes under the Ethics in Public Office Acts, following the signing into law by the Minister for Finance of the Ethics in Public Office Prescribed Public Bodies, Designated Directorships of and Positions in Public Bodies) Regulations 2005 (S.I. No 672 of 2005). It is from this legislation and the requirements of the new Code of Practice for the Governance of State Bodies launched by the Minister for Public Expenditure and Reform in August 2016 that the SEAI Code of Governance Framework has been devised.

It is the objective of the Authority to ensure that the highest possible standards of integrity and ethics are maintained. This document sets out guidelines as to how this will be achieved. Guidelines are formulated to reflect obligations on Board and staff members in carrying out their public duties.

It is the responsibility of:

- *Board Members of the Authority*
- *Members of all SEAI Board Committees*
- *Chief Executive/Board Secretary*
- *Directors.*
- *All staff of the Authority*

to ensure that they are compliant with the relevant Codes of Business Conduct. A Copy of the Code of Business Conduct for SEAI Board Members and Staff members is included at Appendix 2 of this Code of Governance Framework.

### **3.2 Conflict of Interest**

This section of the Code of Governance Framework should be read in conjunction with the Board's Conflict of Interests Policy and Procedure, which form part of the Corporate Governance Framework Documents.

The Authority recognises that Board membership and employment in a public sector setting can provide potential for conflict of interest. The principal circumstances giving rise to such possibilities in the Authority's case include instances where a Board/staff member:

- *holds an interest directly or indirectly in groupings or enterprises which deal commercially and/or contractually with the Authority.*
- *or where a family member can influence procurement decisions and the awarding of contracts for which groupings or enterprises, with which he/she is associated directly or indirectly, are competing.*

In the former case, Board members and the Chief Executive are required to declare such an interest to the Chairperson of the Board/ Board Secretary. The Chairperson should make his/her declaration to the Board Secretary and staff members (other than the Chief Executive) are required to similarly declare such an interest to the Chief Executive/Board Secretary.

In the latter case, Board and staff members are required to similarly declare such an interest and step aside from the related procurement/contract review, selection and awarding process.

### **3.3 Disclosure of Interests/ Avoidance of Conflict of Interest**

To avoid conflicts of interest and the possibility of unjust enrichments each Board member furnishes to the Secretary of the Board details of his or her employment and all other business interests including share holdings, which ***could involve a conflict of interest or could materially influence his or her functions as a member of the Board.*** Interests of family and other connected persons or bodies are also declared.

The Secretary maintains a confidential register of Board Members' interests, which is updated annually. Only the Chairperson, Chief Executive and Secretary have access to the register. When a matter arises, which may relate to interests of the Chairperson, the Senior Independent Board Member takes the Chair at the relevant Board meeting.

Where individual Board members become aware of non-compliance with any such obligation, they should immediately bring this to the attention of their fellow Board members with a view to having the matter rectified. The matter should also be brought to the attention of the Minister by the Chairperson.

As it is recognised that the interests of a Board member and persons connected with him/her can change at short notice, a Board member should, in cases where he/she receives documents (through Diligent Boards, email or otherwise) relating to his/her interests or of those connected with him/her, inform the Secretary to the Board at the earliest opportunity.

Documents relating to dealings where a Board member has an interest are not made available to the particular member concerned. Where such documents are accessed in error or otherwise, the Secretary should be informed. A member absents himself/herself from discussions relating to such dealings. Where a question arises as to whether or not a case relates to a member's interests, the Chairperson adjudicates.

The Chief Executive and the Directors are required to complete a register of interests in line with the above. When a matter arises, which might involve a conflict of interest the Chief Executive is required to inform the Chairperson. Similarly, any potential conflict of interest by Directors / Heads of departments or others as appropriate should be notified to the Chief Executive.

### **3.4 Attraction of Benefits**

The Authority recognises that certain Board and staff members may attract benefits in cash or in kind over and above normal remuneration (for example director fees, salary, travel, subsistence) in respect of associations and activities arising purely and solely by virtue of their position in the organisation. In such cases, Board members and the Chief Executive are required to disclose such positions to the Chairperson of

the Board. Staff members (other than the Chief Executive) are required to similarly disclose such positions to the Chief Executive.

### **3.5 Unjust Enrichments**

The Authority recognises that having regard to the nature of their duties and responsibilities, some Board and Staff members may be exposed to the possibility of inviting and/or attracting offers of personal enrichments. Such enrichments, when established to be materially significant and/or calculated to engender or reward bias are regarded by the Authority as unjust and are prohibited.

### **3.6 Engagement in Outside Employments**

The Authority recognises and acknowledges that Staff Members are required to devote their full-time attention and abilities to the tasks associated with their position in the organisation. Staff members may not engage in or be connected with any outside employment, appointments, or activities unless authorised in writing to do so by Sustainable Energy Authority of Ireland. It is the responsibility of the employee to inform the Sustainable Energy Authority of Ireland of any such activities.

### **3.7 Ethical Principles**

Having regard to the nature of their position, all Board and certain staff members are privy to information and material which is confidential to the organisation and its clients. All Board and relevant staff members are required to maintain confidentiality in such matters.

All Board and staff members are required to operate within these guidelines, which are designed to ensure the maintenance of acceptable standards of integrity of the Authority.

Former Board and staff members are required to maintain confidentiality in regard to the business of the Board.

### **3.8 Work and Environment**

Board and Committee members should place the highest priority on promoting and preserving the health and safety of all employees of the Authority. They should also minimise any detrimental impact of the operations of the Board on the environment.

### **3.9 Appropriate Behaviour**

To ensure that the Board Members and all staff are adequately informed on appropriate behaviour the Authority has developed specific policies and procedures in relation to:

- Protected Disclosures (Whistle-blowing) Policy
- Anti-Fraud, Bribery and Corruption Policy
- Disciplinary and Grievance procedures
- Protected Disclosures Policy
- Child Protection Policy
- Social Media Policy

### **3.10 Fairness**

The Board and Committee Members should:

- Comply with employment equality and equal status legislation
- Commit to fairness of all business dealings.
- Value all Clients / Stakeholders and treat all equally.

### **3.11 Information**

The Board and staff shall facilitate access to general information relating to the Authority in a way that is open and that enhances accountability to the public.

The Board and staff shall maintain confidentiality concerning information of the commercial interests of the Authority and especially on client data.

The Board and staff shall ensure compliance with statutory provisions relating to information.

- Board members, in the furtherance of their duties, may take independent professional advice, if necessary, at the reasonable expense of the Authority.
- The Board shall observe appropriate prior consultation procedures with third parties where, it is proposed to release sensitive information in the public interest.
- The Board shall comply with relevant statutory provisions relating to access of information (e.g., The Freedom of Information Act or the Data Protection Act).

**Note: Where queries arise in relation to the release of information under the provisions of the Freedom of Information Act, these should be directed, in writing, to the Freedom of Information Officer at the Authority.**

## **4.Obligations**

The Board and Staff of the Authority are committed to this Code of Governance Framework adopted by the Board, and all statutory obligations.

An obligation of loyalty to the Authority is recognised together with a commitment to the highest standards of business ethics by both the Board and staff.

Board members use all reasonable endeavours to attend 100% of Board and Committee meetings.

Board Members must ensure that there are adequate controls in place to prevent fraud including controls to ensure compliance with prescribed procedures in relation to claiming of expenses for business travel. The Authority has in place procedures relating to the acceptance of positions / consultancies post-employment or resignation to avoid conflicts of interest or breaches of confidentiality.

## **5. Review of Code of Governance Framework**

This Code will be reviewed on an annual basis.

## **6.Procedures for the Conduct of Board meetings**

### **6.1 Introduction**

These Procedures are adopted by the Authority in order to regulate, the procedures and business of the Board.

## **6.2 General Principles**

The Board has generally adopted the following principles:

- a) The Board operates on the principles of collective responsibility, support and respect. Normally, decisions will be taken by consensus.
- b) Board members should normally speak with one voice in public on Authority issues. If a different approach were to be followed, this would first have to be discussed by the Board. A Board member should inform the Chairperson (or the Senior Independent Board Member, in the absence of the Chairperson) before making public statements relating to Authority business.
- c) All decisions will be recorded. Minority views will not normally be made public, although if a vote is necessary, the outcome of this will be recorded in the Board minutes. If a Board member resigns because of disagreement with a Board decision, he or she may state the basis for the disagreement but may not publicly disclose the view of other Board members.
- d) Board members (other than those who disagreed with a decision) may be nominated to explain and articulate specific decisions.

## **6.3 Meetings**

- a) The Board normally holds ten meetings in each year (at least four meetings are required under the Act) and such other meetings as may be necessary for the performance of its functions. The meetings are held at such times and at such places as the Board from time to time decides. Should circumstances arise, which in the opinion of the Chairperson, would make it inconvenient for a large number of members to attend a meeting he or she may direct that the meeting be deferred to a later date to be fixed by him or her.
- b) A Board meeting may, at any reasonable time, be convened by the Chairperson or the Senior Independent Board Member in the Chairpersons absence, following discussion with the Chairperson or on request from at least three Board members.
- c) Meetings, other than the schedule of formal meetings may be held via teleconference for holding urgent discussions on issues arising. Board members must undertake to ensure privacy during such calls. Post the COVID 19 pandemic, physical Board meetings are held in 3 Park Place and members can participate remotely, if necessary, for business reasons. In general, most SEAI Committee meetings continue to be held remotely via Microsoft Teams.
- d) At least four clear working days before any meeting of the Board, the Board Agenda and associated meeting papers are forwarded, through the SEAI Board document management system - oneAdvanced to every member of the Board by the Board Secretary. A Board meeting may exceptionally be called at less than four clear workings days' notice. Such shorter notice will be valid only if ratified at the Board meeting called at short notice. Notice of a Board meeting will be given to Board members in writing (generally by email). Failure to receive notice of a Board meeting will not invalidate that Board meeting or any business transacted at that meeting.
- e) The meetings of the Board will be held in private.
- f) Papers may be tabled at a Board meeting with the Chairperson's permission (or, in his or her absence, the permission of the Senior Independent Board member).

- g) The procedure for obtaining Board approval between Board meetings is set out in Section 7 below.

#### **6.4 Proceedings at Meetings**

At a meeting of the Board:

- a) The Chairperson of the Board shall, if he or she is present, be Chairperson of the meeting.
- b) If the Chairperson of the Board is not present, or the office of the Chairperson is vacant, the members of the Board who are present shall choose one of their number, to be Chairperson of the meeting. In normal circumstances this is likely to be the Senior Independent Board Member
- c) The quorum of the Board shall be 5 members in accordance with the Act.
- d) A Board member is not counted in the quorum on an item in respect of which he or she has a conflict of interest or is not entitled to take a decision.

#### **6.5 Decision Making**

Decisions by the Board will normally be made by consensus rather than by formal vote. Failing consensus, decisions will be made by a vote when:

- the Chairperson feels that there is a body of opinion among Board members at the Board meeting which disagrees with a proposal or has expressed reservations about it and no clear consensus has emerged; or
- a Board member who is present requests that a vote be taken, and this is supported by at least one other Board member; or the Chairperson feels that a vote is appropriate.

When a vote is taken, a decision will be by simple majority in accordance with the Act. In the case of a tied vote, the Chairperson will have a casting vote in addition to his or her original vote.

#### **6.6 Conflict of Interest**

Each Board member must comply with the policy and procedure for conflicts of interests, which has been approved by the Board and which are included in this Code of Governance Framework.

#### **6.7 Procedure for Obtaining Board Approval**

##### **Between Board Meetings**

The Chairperson shall decide when an issue is of a sufficiently urgent nature to warrant the taking of a decision by the Board by written/ electronic procedure in the interval between meetings of the Board and a process has been put in place to notify the Board of any such decisions required.

In normal circumstances, such decisions relate to large procurement/grants, which require Board approval, and these are advised to the Board in advance. The request for a decision shall be communicated to Board members at a previous Board meeting or otherwise by e-mail and shall:

- 3. Be in compliance with the procedures agreed by the Board in relation to such matters regarding written procedure/electronic circulation.
- 4. State the nature of the decision requested.
- 5. Provide information on the urgent nature of the decision.

6. Provide detailed information to enable the members of the Board to take the decision.
  - Set out a final deadline for members of the Board to seek additional information or clarification on the issue to be decided.
  - Set out a final deadline and procedures for members of the Board to inform the Secretary of their decisions.

In the event, that any member of the Board seeks additional clarification or information on the issue to be decided, a copy of that information will be sent to all members of the Board.

The Board, in March 2018, approved a decision-making procedure, for processing grants/procurements proposals.

The decision of the Board will be communicated by the Secretary to all members of the Board by e-mail or through the Board document management system - oneAdvanced as soon as it practicable after the decision has been taken.

Decisions taken by written procedure, between meetings of the Board, will be recorded in the minutes of the subsequent Board meeting.

## **6.8 Minutes of Meetings**

Minutes of the proceedings of a meeting of the Board will be drawn up by the Board Secretary. The Board Secretary will record names of Board members present and absent, and apologies for absence, at a meeting of the Board in the minutes of the meeting.

In cases where a formal vote is taken the names of members voting on any question arising at a meeting of the Board will be recorded in the minutes of the proceedings of the meeting and where applicable, the record will show which member(s) voted for and against that question and which member(s) abstained.

When minutes of proceedings have been adopted and confirmed by the Board, it will not be in order for any member of the Board to question their accuracy nor seek their amendment at subsequent meetings.

## **6.9 Order of Business**

The Board Agenda should address:

- Quorum and Statement / Conflict of Interest declaration requirements
- Corporate Risk Review (as an Agenda Item and through Reports from the Audit and Risk Committee)
- Verification of Minutes of previous meeting
- Minuting of decisions taken between formal Board meetings, (e.g. Grants/Procurements)
- Matters arising/ Action Points
- CEO Report
- Chairperson's Report
- Consideration of Board Committee reports
- SEAI Strategy/ Business Plans developments
- Reports from the Directors/Heads of departments (senior management), as appropriate, including updates on specific programmes/schemes.
- Finance and Expenditure Reports
- Consideration of procurement and grant proposals, in excess of €1m as required or confirming decisions on electronic circulations in accordance with agreed Board procedures and Delegated Authority Framework (DAF).
- Governance matters

- Update on Board Work Plans under AOB.
- Any other business as set forth on the Agenda.

At a special meeting of the Board, only business specified in the notice convening that meeting will be transacted at that meeting.

#### **6.10 Delegations**

- The Board may delegate the discharge of a function, but the exercise of a delegated power should be in accordance with policies agreed by the Board.
- The Board delegates to the CEO, the discharge of all functions of the Authority other than:
  - any matter reserved to the Board
  - any matter delegated to a Committee of the Board.
- The Board may make delegations or vary, revoke or add to existing delegations.
- Any delegation made by the Board may be limited or made subject to any condition. For example, the Board may delegate a function only for a limited period or for a particular matter. The nature and scope of new delegations will be recorded in the minutes.
- The Board may itself discharge a function even though it has delegated the discharge of that function.
- There is delegated from the Board to each Committee of the Board the discharge of those functions, which fall within their respective Terms of Reference, other than any matter reserved to the Board. The Board may instruct Authority staff, or a Committee, as to how to exercise a delegated authority.
- The Board authorises the CEO to sign contracts or other documents on behalf of the Authority and to delegate this authority to one or more Authority employees.

#### **6.11 Committees**

The Board may establish standing Committees and ad hoc Committees as appropriate.

The Board will appoint members to any Committee it establishes and may appoint persons who are not members of the Board but have special knowledge and experience related to the purpose of the Committee.

The Committees appointed by the Board will, in the transaction of their business, comply with any directions which the Board may give from time to time either in general or for individual Committees.

The Board may take advice or consider recommendations from any Committee of the Board as set out in the Committee's Terms of Reference.

#### **6.12 Code(s) of Conduct**

Board members will comply with the Code of Business Conduct, which have been approved by the Board and are set out in this Code of Governance Framework.

#### **6.13 Reviewing the Board's Performance**



The Board will review its own performance and that of its Committees in accordance with the requirements of the Code of Practice for the Governance of State Bodies.

#### **6.14 Confidentiality**

Reports, documents and briefings issued to members in relation to Board matters must be treated as confidential until such time as the Board has had an opportunity to discuss and make decisions on their contents, including their distribution outside the Board membership.

#### **6.15 Issue of Statements on Behalf of the Board**

Only the Chairperson shall issue any statement on Board matters to the press or the public on behalf of the Board. The CEO, with the agreement of the Chairperson, may also make such statements.

#### **6.16 General**

The Chairperson will have power to decide upon any procedural matter arising and not covered by these existing procedures.

#### **6.17 Commencement**

These procedures came into operation on 1 July 2010, having been adopted by the SEAI Board at its meeting on 2 June 2010 and they have been reviewed on an annual basis since then (in January each year). The latest review took place on 5 February 2025.

**SIGNED:**



**Dermot Byrne**  
Chair



**William Walsh**  
Chief Executive

## Appendix 1 – Formal Schedule of Matters for Board Decision

### 1. Introduction

**“Each State body should be clear about its mandate and from that identify the various functions, roles and responsibilities entailed in the delivery of that mandate. The Board is collectively responsible for leading and directing the State body’s activities. While the Board may delegate particular functions to management the exercise of the power of delegation does not absolve the Board from the duty to supervise the discharge of the delegated functions. The Board should fulfil key functions, including reviewing and guiding strategic direction and major plans of action, risk management policies and procedures, annual budgets and business plans, setting performance objectives, monitoring implementation and State body performance, and overseeing major capital expenditure and investment decisions. The Board should act on a fully informed and ethical basis, in good faith, with due diligence and care, and in the best interest of the State body, having due regard to its legal responsibilities and the objectives set by Government. The Board should promote the development of the capacity of the State body including the capability of its leadership and staff. The Board is responsible for holding the CEO and senior management to account for the effective performance of their responsibilities. “**

(Section 1 – Role of the Board - Revised Code of Practice for the Governance of State Bodies- issued in August 2016).

In addition, Section 1.7 of the Revised Code, which was formally adopted by the SEAI Board on 29 September 2016, requires that, the Board *“should have a formal Schedule of Matters specifically reserved to it for decision to ensure that the direction and control of the Body is firmly in its hands.* It sets out a number of issues that should be included.

### 2. Legislative Background

Section 10 of the Sustainable Energy Act 2002, sets out the precise legal requirements for the SEAI Board, including its composition, competencies, method and terms of appointment of members and Chairperson, remuneration, cessation and resignation of members, including removal by the Minister. Sections 11, 12 and 13 set out the general provisions in relation to the Chairperson, meetings and procedures of the Board and the Committees to be established by the Board.

The overall function of the Board as set out in Sections 10(1) and 10(2) are that the Board will consist of 12 members and that the Board *“shall direct the functions of the Authority in accordance with this Act and shall satisfy itself as to the adequacy of the systems in place for that purpose and will keep under review the performance of the Authority”.*

The Board is, as set out in the Code, ultimately responsible for *“compliance with all statutory obligations applicable to the State Body that may be set out in legislation governing the establishment of the body or in other legislation. The Board shall satisfy itself that all such obligations are identified and made known to it”.*

Against this comprehensive legal background and in order to satisfy the requirements of the Revised Code of Practice, for the Governance of State Bodies the SEAI Board, at its meeting on 2 June 2010, formally approved the Schedule of Matters Reserved for Board decision as set out at Para graph 3 below and this has been reviewed and enhanced on an annual basis since.

Overall, the Board is responsible for setting the broad policies of the Authority and delegates to management, Board Committees and Advisory/Ad Hoc Committees, if any, the responsibility for their

implementation. In its own activities and in its use of Committees and Working groups, the Board operates towards achieving good corporate governance.

### **3. Formal Schedule of Matters for Board Decision**

#### **Introduction**

It is a requirement for SEAI to have a formal schedule of matters specifically reserved to it for decision, in order to ensure that the direction and control of the Authority is specifically and demonstrably in the hands of the Board.

The following sections therefore sets out the responsibilities of the SEAI Board and some specific matters reserved for the Board.

#### **Managerial Functions**

- Ensuring that, through the arrangements in place, a balanced, true and understandable assessment of SEAI is made when preparing the Annual Report and Annual accounts.
- Approve the Annual Financial Statements and authorising the Chairperson and one other member to sign them on behalf of the Board (usually the Chief Executive Officer or the Chairperson the Audit & Risk Committee)
- Ensuring that, through the arrangements in place, statutory obligations applicable to SEAI, as set out in the Sustainable Energy Act 2002, or in other relevant legislation are identified and complied with.
- Ensuring that, through the arrangements in place, non-statutory obligations applicable to SEAI, as set out in the Code of Practice for the Governance of State Bodies, Department of Finance/Public Expenditure, NDP Delivery and Reform Circulars and in Circulars from the Department of the Environment, Climate and Communications etc. are complied with.
- Approve the Organisational Strategic Plan and/or Corporate Plan, the annual operating plan and Budget for SEAI.
- Approve the appointment, remuneration, assessment of performance and succession planning for, the Chief Executive Officer.
- Delegation of sufficient powers to the SEAI Executive Leadership Team and the Chief Executive Officer of SEAI, to enable the business of SEAI to be carried on effectively between Board meetings.
- Oversee the discharge by the Chief Executive Officer, and the Executive Leadership Team of the day-to-day business of SEAI.
- Ensuring, through the arrangements in place, compliance with statutory and administrative requirements in relation to the approval of the number, grading and conditions of appointment of all staff.
- Significant amendments to the pension benefits of the CEO and staff (which require Ministerial approval).

#### **Board Membership and Board Committees**

- Establish an Audit and Risk Committee in accordance with the provisions of the Code of Practice for the Governance of State Bodies.
- Appoint the Chairperson, members of the Committee and approve the Terms of Reference of the Audit and Risk Committee and all other Committees established by the Board.

## **Contracts/ Grants/ Procurement**

- Approve all transactions (within the Budget approved by the Board) whose value exceeds €1m in accordance with the electronic circulation/approval process approved by the Board. This applies to both capital and current revenue items and transactions.
- Approve all property leases.
- Approve terms of major contracts, investments and capital projects, significant acquisitions, disposals, and retirement of assets of SEAI or its subsidiaries (if established)

## **Internal Controls and Risk Management**

- Ensure maintenance of a sound system of internal controls, including financial, operational and compliance controls, and risk management processes, with appropriate reference to the Code of Practice for the Governance of State Bodies.
- Monitor the effectiveness of the SEAI risk management processes and systems, including the Risk Appetite Statement (which should be approved by the Board) to ensure the effective identification, monitoring and control of external risks, and identification of opportunities, to support the SEAI statutory objectives. In practice, this is delegated to the Audit and Risk Committee, which reports back to the Board at regular intervals.
- Undertake an annual assessment of the effectiveness of internal control and risk management processes (including financial, operational and compliance controls and risk management systems) in accordance with the revised requirements, for the Statement of Internal Controls (SIC) as set out in the Code of Practice for the Governance of State Bodies.
- Authorisation to open bank accounts
- Authorisation of signatories to attest the seal of SEAI.

## **Miscellaneous**

- Undertake, as appropriate, a formal and rigorous review of its own performance, that of its committees and individual directors.
- Take any specific decisions that the Board or SEAI management consider to be of such significance as to require to be taken by the Board.

## **Appendix 2 – Code of Business Conduct for SEAI Board Members/Employees**

### **Sustainable Energy Authority of Ireland**

#### **Code of Business Conduct for SEAI Board Members**

**“Each State body should be clear about its mandate and from that identify the various functions, roles and responsibilities entailed in the delivery of that mandate. The Board is collectively responsible for leading and directing the State body’s activities. While the Board may delegate particular functions to management the exercise of the power of delegation does not absolve the Board from the duty to supervise the discharge of the delegated functions. The Board should fulfil key functions, including reviewing and guiding strategic direction and major plans of action, risk management policies and procedures, annual budgets and business plans, setting performance objectives, monitoring implementation and State body performance, and overseeing major capital expenditure and investment decisions. The Board should act on a fully informed and ethical basis, in good faith, with due diligence and care, and in the best interest of the State body, having due regard to its legal responsibilities and the objectives set by Government. The Board should promote the development of the capacity of the State body including the capability of its leadership and staff. The Board is responsible for holding the CEO and senior management to account for the effective performance of their responsibilities”**

(Section 1 – Role of the Board - Revised Code of Practice for the Governance of State Bodies- issued in August 2016).

## **Introduction**

### **SEAI Mission Statement**

Our mission is to be at the heart of delivering Ireland's energy revolution. We drive the reduction and replacement of fossil fuel usage. We are a knowledge led organisation. We partner with citizens, communities, innovators, funders and educators.

### **SEAI Vision**

To be a leading authority driving Ireland's sustainable energy transformation for the benefit of society.

### **The SEAI Code of Business Conduct**

The Code of Practice for the Governance of State Bodies (2016) is a revised and updated version of the Code of Practice for the Governance of State Bodies (2001 and 2009) and an expansion of the State Bodies Guidelines (1992). The SEAI Board, at its meeting on 29 September 2016 was formally notified of the revised Code of Practice and the Board formally adopted the new Code on that day.

In order to comply with the Code of Practice, the Chairperson of the Board of SEAI is obliged to confirm to the Minister for Environment, Climate and Communications that a number of control functions are carried out by SEAI, including the issuing of a Code of Business Conduct for Board members and that this is being adhered to.

The SEAI Code of Business Conduct sets out in written form, the agreed standards of principle and practice which inform the conduct of the Board of SEAI. A separate document setting out a Code of Business Conduct for all SEAI employees is issued to staff members.

#### **The purpose and intent of the Code is:**

- To enable SEAI to provide a professional and effective service to its clients/stakeholders;
- To establish an agreed set of ethical principles;
- To promote and maintain confidence and trust;
- To prevent development or acceptance of unethical practices;
- To meet the requirements under the Act and also the Revised Code of Practice for the Governance of State Bodies (2016).

## **Code of Business Conduct for SEAI Board Members**

### **General Principles:**

Board Members should observe the highest standards of honesty and integrity. To ensure this, they should adhere to the following principles:

### **Integrity**

Board Members:

- Must disclose any outside interests that are in conflict or potential conflict with the business of SEAI in accordance with the Code of Practice for the Governance of State Bodies and Section 18 of the Act.
- Not participate in discussions or decisions involving conflicts of interest whether or not such conflicts have previously been disclosed.
- Avoid giving or receiving corporate gifts, hospitality, preferential treatment or benefits which might affect or appear to affect the ability of the donor or the recipient to make independent judgment on business transactions.
- Ensure that purchasing activities of goods/services are conducted in accordance with best business practice.
- Ensure that SEAI accounts and reports accurately reflect their business performance and are not misleading or designed to be misleading.
- Not acquire information or business secrets by improper means through the course of their duties/work
- Not use any information obtained by virtue of their position for the purpose of any dealing (direct or indirect) in shares, property or otherwise.
- Ensure a culture of claiming expenses only as appropriate to business needs and in accordance with good practice in the public sector generally.
- Avoid the use of SEAI resources or time for personal gain or for the benefit of persons/organisations unconnected with the body or its activities or for the benefit of competitors.
- Ensure that there is non-disclosure of privileged or confidential information when Board membership ceases. In addition, Board members should ensure that acceptance of further employment where the potential for conflict of interest arises should be avoided during a reasonable time period after the Board membership ceases. Any issues or clarifications, arising from this, should be addressed to the Board Secretary.

### **Information**

Board Members should:

- Support the provision of access by SEAI to general information relating to SEAI activities in a way that is open and that enhances its accountability to the general public.
- Respect the confidentiality of sensitive information held by SEAI. This would constitute material such as:
  - commercially sensitive information (including but not limited to future plans or details of major organisational or other changes such as restructuring)
  - personal information
  - Information received in confidence by SEAI, particularly in relation to grant or procurement applications. Directors should note that SEAI considers any grant or procurement applications to be confidential subject to its obligations under law, including the Freedom of information Act. SEAI does not disclose information about a

grant/procurement application or its status to a third party unless the applicant specifically requests SEAI to do so. Once an application for grant support or a procurement decision has been made, the details may be made available to the public.

- Observe appropriate prior consultation procedures with third parties where, exceptionally, it is proposed to release sensitive information in the public interest.
- Comply with relevant statutory provisions relating to access to information (e.g., Data Protection Act, Freedom of Information Act and the Standards in Public Office Act).

## **Confidentiality**

Board Members should:

- Ensure that they maintain the confidentiality of all information obtained by virtue of their position. This principle of confidentiality of information is enshrined in Section 19 of the Sustainable Energy Act, 2002.
- Ensure they do not retain any documentation obtained during their term as Director and should return such documentation to the Secretary or otherwise indicate to the Secretary that all such documentation has been disposed of in an appropriate manner.

## **Obligations**

Board Members should:

- Fulfil all regulatory and statutory obligations imposed on SEAI.
- Comply with detailed tendering and purchasing procedures as well as complying with prescribed levels of authority for sanctioning any relevant expenditure.
- Ensure that there are adequate controls in place to prevent fraud including controls to ensure compliance with prescribed procedures in relation to claiming of expenses for business travel.
- Use all reasonable endeavours to ensure that they can have a 100% attendance at the SEAI Board and/or Committee Meetings (as applicable).
- Comply with conformity procedures laid down by the Board in relation to conflict-of-interest situations, including, in regard to acceptance of positions following engagement by a State Body that may give rise to the potential for conflicts of interest and to confidentiality concerns.
- Acknowledge their duty to conform to the highest standards of business ethics, including compliance with the Ethics in Public Office Acts 1995 and 2001.

## **Loyalty**

Board Members should:

- Acknowledge the responsibility to be loyal to SEAI and to be fully committed in all its business activities while mindful that the organisation itself must at all times take into account the interests of its stakeholders.

## **Fairness**

Board Members should:



- Comply with employment equality and equal status legislation.
- Commit to fairness in all business dealings.
- Value clients/stakeholders and treat all clients/stakeholders equally.

### **Work/External Environment**

Board Members should ensure that:

- The health and safety of employees is promoted and preserved.
- Community concerns are fully considered.
- Any detrimental impact of the operations on the environment is minimised.

### **Responsibility**

The Chairperson of the SEAI Board should:

- Circulate this Code of Business Conduct along with guidelines on disclosure of interests to all Directors, Committee Members, Management and Staff for their retention.
- Provide guidance and direction on the policies and procedures.
- Ensure that the above recipients acknowledge receipt and understanding of the same.
- Prepare a governance framework in order to provide practical guidance and direction to the Board of Directors.

### **Appropriate Behaviour**

To ensure that Board Members, Committee Members and all staff are adequately informed to avoid being accused of inappropriate behaviour, the following policies and procedures are in place and available from SEAI.

- Protected Disclosure (Whistleblowing) Policy and procedures (revised in the context of the Protected of Disclosures Act)
- Anti-Fraud, Bribery & Corruption Policy
- Bullying, Harassment & Sexual Harassment Policy
- Disciplinary & Grievance procedures
- Child Protection Policy
- Social Media Policy

### **Professional advice**

SEAI Board members may, in furtherance of their duties, take independent professional advice, if necessary, at the reasonable expense of SEAI, in accordance with agreed procedures for such action.

### **Review**

#### *The Board*

- Commits to review the Code as appropriate.

## **Code of Business Conduct for Staff Members (updated 21 July 2023)**

### **Purpose of Code of Business Conduct**

The purpose of this Code of Conduct is to ensure that SEAI staff functions according to a set of agreed ethical principles, which support the development of trust, confidence and teamwork in SEAI and promote a high-performance culture. It allows SEAI to meet the requirements under the revised Code of Practice for the Governance of State Bodies (2016). This code will be reviewed on an annual basis as part of the review of the SEAI Code of Governance Framework to ensure it continues to reflect the values of SEAI and the standards of business conduct expected from staff of SEAI. Staff members will strive to prevent the development or acceptance of unethical practices and perform their duties in accordance with the highest ethical standards, including:

### **Integrity**

Staff will

- Ensure the effectiveness of SEAI through carrying out responsibilities and duties energetically, proactively, ethically and honestly.
- Act in accordance with the principles of good corporate governance as set out in the SEAI Code of Governance Framework
- Avoid involvement in outside employment/business interests in conflict or in potential conflict with the business of SEAI.
- Avoid acquiring information or business secrets by improper means.
- Carry out purchasing of goods/services in accordance with best business practices.
- Claim expenses only as appropriate to business needs and in accordance with good practice in the public sector generally.
- Prepare accounts and/or reports that accurately reflect SEAI business performance and are not misleading or designed to be misleading.
- Avoid giving or receiving corporate gifts, hospitality, preferential treatment or benefits, which might affect or appear to affect the ability of the donor or recipient to make independent judgment on business transactions.
- Avoid using SEAI's resources or time for personal gain, or for the benefit of persons or organisations unconnected with SEAI and its activities.
- Act in the public interest

## **Information**

Staff will

- Support the provision of public access to general information about SEAI's activities in a way that is open and that enhances its accountability to the general public.
- Respect the confidentiality of confidential information held by SEAI, including commercially sensitive information, personal information and information received in confidence by SEAI.
- Observe appropriate prior consultation procedures with third parties where it is proposed to release sensitive information in the public interest.
- Comply with relevant statutory provisions relating to access to information (e.g. GDPR, Freedom of Information and Standards in Public Office).

## **Statutory and regulatory obligations**

Staff will

- Comply with all regulatory and statutory obligations imposed on SEAI.
- Comply with detailed tendering and purchasing procedures, and with prescribed levels of authority for sanctioning any relevant expenditure.
- Introduce controls to prevent fraud, including adequate controls to ensure compliance with prescribed procedures in relation to claiming of expenses for business travel.
- Conform to the highest standard of business ethics.

## **Loyalty**

Staff will

- Be loyal to SEAI and fully committed to all its business objectives and activities, while mindful that SEAI itself must at all times take into account the interests of its stakeholders.
- Be loyal to and support colleagues in the exercise of their duties in pursuit of SEAI's business objectives and strategy.

## **Fairness**

Staff will

- Protect the dignity and integrity of each individual associated or working with SEAI by complying with employment equality and equal-status legislation as set out in the SEAI Dignity at Work Policy.
- Demonstrate commitment to fairness in all business dealings.
- Value clients/stakeholders and treat all clients/stakeholders fairly and equally.

## Values







### Our Culture and Values

Culture is defined as “the pattern of basic assumptions that a group has invented, discovered or developed in learning to cope with its problems of external adaptation or internal integration, and that worked well enough to be considered valid, and therefore taught to new members as the correct way to perceive, think and feel in relation to those problems”.

The culture of an organisation can simply be expressed as “how we do things around here”. It is the sum of everything that an organisation stands for and how it operates, its values, its beliefs, its mission, its behaviours and its interactions with employees and stakeholders.

Our target culture in SEAI is defined by our values, which were developed in consultation with our colleagues and management during the development of our Organisational Strategy.

These values are as follows:

					
<b>We are passionate</b>	<b>We are courageous</b>	<b>We are innovative</b>	<b>We are trusted</b>	<b>We are experts</b>	<b>We are collaborative</b>
<ul style="list-style-type: none"><li>• We are enthusiastic about our role in working towards a sustainable energy society.</li><li>• We channel our passion and commitment into the way we operate to ensure that we will deliver for all of Irish society.</li></ul>	<ul style="list-style-type: none"><li>• We understand the scale of Ireland's energy challenge and accept our role in meeting this challenge.</li><li>• We understand that every one of us has a part to play in delivering the energy changes that Ireland needs.</li></ul>	<ul style="list-style-type: none"><li>• We know that existing technologies and processes alone will not allow us to realise a fully sustainable energy society.</li><li>• We are continually learning, seeking new solutions, and constantly adapting to meet the demands of our fast-changing environment.</li></ul>	<ul style="list-style-type: none"><li>• We appreciate the trust placed in us by citizens, communities, business and Government, without it we could not deliver on our objectives.</li><li>• We respect this trust and seek to maintain it by operating transparently, working with integrity, holding ourselves accountable and functioning independently.</li></ul>	<ul style="list-style-type: none"><li>• We recognise the importance technical expertise plays in achieving a sustainable energy future.</li><li>• We seek to further enhance this expertise within SEAI through research, critical thinking, consultation, listening, analysis and delivery.</li></ul>	<ul style="list-style-type: none"><li>• We will not succeed by operating in isolation.</li><li>• We actively look to work with all those in Irish society; listening to ideas, acknowledging concerns, incorporating feedback and looking to build strong relationships to support every individual, community and business in Ireland to be a part of the sustainable energy revolution.</li></ul>

These values and behaviours form the cornerstone of our culture and the way in which we want to behave and act and form the basis of the SEAI culture. The values translate to a set of desirable behaviours as follows:

 <b>WE ARE PASSIONATE</b>	 <b>WE ARE COURAGEOUS</b>	 <b>WE ARE INNOVATIVE</b>	 <b>WE ARE TRUSTED</b>	 <b>WE ARE EXPERTS</b>	 <b>WE ARE COLLABORATIVE</b>
<input type="checkbox"/> I care about our customers' needs and understand that they are my primary priority.	<input type="checkbox"/> I speak up, stand up and have my voice heard in line with organisational messages.	<input type="checkbox"/> I play a part in driving innovative ideas, and process improvements.	<input type="checkbox"/> I give accurate technical advice to our stakeholders, as I challenge and trust the data we are responsible for producing.	<input type="checkbox"/> I commit to training and development and staying up to date.	<input type="checkbox"/> I engage in formal/informal information and knowledge sharing sessions. I share findings across the organisation and externally.
<input type="checkbox"/> I am proud to be part of SEAI and I care about the quality of work we deliver for citizens.	<input type="checkbox"/> I am open to new ideas & opinions and share my own opinions to invite discussion.	<input type="checkbox"/> I actively seek to continually develop professionally and upskill.	<input type="checkbox"/> I listen to my customers, reflect, and respond to address their needs.	<input type="checkbox"/> I am responsible for delivering agnostic advice and expertise.	<input type="checkbox"/> I recognise, value and leverage strengths of others.
<input type="checkbox"/> I believe in our purpose and am driven to deliver for the national good.	<input type="checkbox"/> I have integrity and make decisions in the organisation's best interest. I am accountable for those decisions.	<input type="checkbox"/> I am willing to collaborate with and constructively challenge colleagues and external stakeholders.	<input type="checkbox"/> I follow through on my commitments to customers and clients, and adhere to SEAI's fair and transparent processes.	<input type="checkbox"/> I am driven by delivering climate action, through the generation of key energy data and supporting energy policy and delivery programmes.	<input type="checkbox"/> I see different perspectives and I am ready to work outside my 'comfort' zone.

## Appropriate Behaviour

To ensure that SEAI staff members are adequately informed to avoid being accused of inappropriate behaviour, the following policies and procedures are in place and available from SEAI:

- Whistle-blowing policy (revised in context of Protection of Disclosures Act)
- Anti-Fraud Policy
- Bullying, Harassment & Sexual Harassment Policy
- Disciplinary Policy
- Grievance Procedures
- Child Protection Policy
- Social Media Policy

## REVIEW AND MONITORING

This policy will be reviewed on a regular basis for effectiveness in its implementation and operation. This will be done in line with changes in statute law, relevant case law and other developments. Any revisions or modifications necessary will be made and communicated to all employees as soon as is reasonably practicable in consultation and agreement with senior management.

## **Appendix 3 - Functions of the Board Secretary**

The following list includes functions typically performed by a person retained by a State Body in the role of Board Secretary. This is not a comprehensive list and the person performing this role may have to use his or her initiative to ensure that all core functions are fulfilled.

### **1. Board Meetings**

Facilitating the smooth operation of the SEAI formal decision making and reporting machinery, organising Board and Committee meetings, formulating meeting Agendas with the Chairperson and or the Chief Executive, collecting, organising and distributing such information, documents or other papers required for such meetings, ensuring that all meetings are minuted accurately, that such minutes are maintained and that all Board Committees are properly constituted and provided with Terms of Reference.

### **2. Functions of the Authority**

Ensuring that the Authority operates within its functions under the Sustainable Energy Act 2002 as may be amended from time to time and also in accordance with the revised Code of Practice for Governance of State Bodies issued in August 2016.

### **3. Books and Registers**

Maintaining such books and registers of the Authority as required under the Sustainable Energy Act 2002, the Code of Governance Framework of the Authority, the Board procedures and the Code of Practice for the Governance of State Bodies, as revised in August 2016.

### **4. Reporting Requirements**

Ensuring that the Authority submits such reports to the Minister, the Board and such other appropriate bodies as required under the Sustainable Energy Act 2002 as may be amended from time to time and the revised Code of Practice for the Governance of State Bodies.

### **5. Report on Accounts**

Inputting, as appropriate, into the publication and distribution of the Authority's Annual Report and Accounts, in consultation with the Authority's internal and external advisors.

### **6. Corporate Governance**

Reporting to the Chairperson on all Board governance matters and assisting the Chair in ensuring that relevant information is made available to the Board and its Committees. Reviewing developments in corporate governance, facilitating the proper induction of new members of the Board into their role, advising and assisting the members of the Board in respect of their duties and responsibilities, and acting as a channel of communication and information for the members of the Board.

Ensuring that Board members are informed as to their legal responsibilities and that they are familiar with the requirements and statutory provisions which have relevance for them in the exercise of their functions as Board members.

### **7. Seal of the Authority**

Ensuring safe custody and proper use of the seal of the Authority.

## **8. Authority Offices**

In consultation with the Chief Executive Officer and senior management and others as appropriate, establishing and administering the offices of the Authority, attending to the receipt, co-ordination and distribution of official correspondence received by the Authority, and ensuring the provision of facilities for the public inspection of appropriate Authority documents.

## **9. Authority Identity**

In consultation with the CEO and Directors ensuring that all business letters, notices and other official publications of the Authority show the name of the Authority and any other information as appropriate and that Authority nameplates are placed in a conspicuous place.

## **10. Induction**

Ensuring appropriate induction for all new Board Members in accordance with the Code of Practice for the Governance of State Bodies.

## **11. General Compliance**

Monitoring and putting in place procedures, which allow for compliance with relevant regulatory and legal requirements, particularly under the Sustainable Energy Act 2002, and the revised Code of Practice for the Governance of State Bodies 2016, including legal requirements and retention of documents, and ensuring that procedures are in place to allow adequate historical archive to be maintained.

## **Appendix 4- Committees of the Board**

### **1. Introduction**

- i. The Board refers to the Board of the Sustainable Energy Authority of Ireland, appointed by the then Minister for Public Enterprise under the Sustainable Energy Act 2002.
- ii. Committee(s) refers to any Committee(s) appointed by the Board, in accordance with the provisions of Section 13 of the Sustainable Energy Ireland Act 2002.

### **2. General Rules Applying to Committees**

- i. Committee members, including the Chair, are appointed by the Board for a period, which is determined by the Board.
- ii. The Terms of Reference for Committees (Constitutions) are agreed and can be amended by the Board as considered appropriate.
- iii. Committee Chairs will report on progress to the Board at each meeting of the Board.
- iv. Committees shall meet according to the provisions set out in their Terms of Reference.
- v. Committees can invite other Board members and procure or seek the advice and support from individuals or bodies outside of the Committee or Board membership, as appropriate.
- vi. The Board may appoint persons to a Committee who are not members of the Board, but have special knowledge and experience related to the purpose of the Committee.
- vii. Any disclosure of interests by any member of the Committee must be discussed with, and reported to, the Chairperson of the Board.
- viii. A quorum for a Committee meeting shall be in accordance with the Terms of Reference.
- ix. Any member or members of the Committee may at any time be removed by the Board and another or other persons appointed.
- x. The CEO or other designated officers, working on behalf of the Authority, will attend the Committee meetings, unless considered inappropriate by the Chair of the Committee.

### **3. Established Committees**

The following is a list of Committees and their current membership, which have been formed by the Board to support the work of the Authority:

- Audit and Risk Committee (ARC)
- Performance Management and Remuneration Committee (PMRC)
- Business and Public Sector Committee (BPSC)
- National Retrofit Delivery Body Committee (NRDB)
- Research and Policy Insights Committee (RPIC)



### **Performance Management and Remuneration Committee - Membership**

Dermot Byrne (Chair)	Chairperson of the Board,
Justina Corcoran	Board Member
Sharon O'Connor	Board Member

### **Audit & Risk Committee - Membership**

Ann Markey (Chair)	Board Member
Joe O'Carroll	Board Member
Robert Wasson	Board Member
Sharon O'Connor	Board Member
Martina Maher	External Member – (Risk Consultant)

### **Business and Public Sector Committee (BPSC)**

Committee Membership- all Board members

Joe O'Carroll (Chair)  
Ann Markey  
Barry McMullin  
Vacancy

### **National Retrofit Delivery Body Committee (NRDB)**

Committee Membership – all Board members

Maria O'Dwyer (Chair)  
Léan Doody  
Robert Wasson  
Ciarán Hayes

### **Research and Policy Insights Committee**

Committee Membership – all Board members

Justina Corcoran (Chair)  
Maria O'Dwyer  
Barry McMullin  
Ciarán Hayes

## **Terms of Reference for Sub-Committees of the Board – approved by the Board in September 2022**

### **Audit and Risk Committee**

**Terms of Reference – Approved by the Board on 24 February 2021 and reviewed by the Board in February 2025 as part of the review of this Code of Governance Framework.**

#### **Introduction**

The Audit and Risk Committee for SEAI is an essential Sub-Committee of the Board. Its primary functions are to assist the Authority in ensuring that it meets its relevant statutory functions and advise the Board on the robustness and effectiveness of the arrangements and status of the corporate governance, financial management, risk management and internal audit of the Authority.

#### **Scope and Authority**

- The functions of the Audit and Risk Committee extend to all of the operations of Sustainable Energy Authority of Ireland. The Committee shall operate under delegated authority from the Board, which is ultimately responsible for all matters relating to the presentation of the financial accounts and all issues arising from internal and external audits on SEAI.
- The Committee shall act as a channel of communication between the Board and management and the Comptroller and Auditor General and shall report to the Board with its recommendations, where it considers action or improvement is needed in any area under its remit.
- The Committee shall review the significant financial reporting issues and judgements made in connection with the SEAI Financial Statements and reports and the scope and effectiveness of SEAI internal controls. This will include financial, operational and compliance controls as well as systems established by management to identify, assess, manage and monitor key risks, both financial and operational, taking account of the key objectives as set out in the SEAI Strategic Plan.
- The Committee shall have explicit authority to investigate any matters within its terms of reference; the resources that it needs to do so and have full access to information.
- The Committee shall be able to obtain outside professional advice and, if necessary, invite outsiders with relevant experience to attend meetings.
- The Audit and Risk Committee shall have discussions with external auditors and internal auditors at least once a year, without the Chief Executive Officer or employees of SEAI being present, to ensure that there are no unresolved issues of concern.
- The Audit and Risk Committee is responsible for advising the Board on whether an appropriate regime of internal control is in operation but not for the formulation or implementation of such a regime.

#### **Composition**

- The Audit and Risk Committee shall comprise a maximum of five members, appointed by the Board. This shall comprise of at least three Non-Executive Board members and may include up to two external persons with the relevant financial/ accounting or other experience in order to fulfil the financial expertise requirements set out in the Code of Practice for the Governance of State Bodies.
- The overall composition of the Committee shall comprise of members who collectively possess the knowledge, skills, competencies and experience as set out in paragraphs 16 and 17 of the Guidance Notes for Audit and Risk Committees in the revised Code of Practice for the Governance of State Bodies.

- Each appointment to the Committee, approved by the Board, shall be formalised with a letter from the Chair of the Board of SEAI setting out the terms of the appointment. Committee members should also receive appropriate training and induction based on their specific needs.
- The Audit and Risk Committee Chair shall not be the Chair of the Board.
- The Secretary to the Board shall be the Secretary to the Audit and Risk Committee.
- Appointments, based on relevant assessment criteria, to the Committee shall be for a period of up to three years, which may be extended for a further three-year period. The Board may also appoint (co-opt) additional members to the Committee, on a short-term basis, in order to provide specialist skills, which may be needed at a particular time.

## **Responsibilities and Role**

The Audit and Risk Committee has responsibility for:

- Reviewing the Annual Financial Statements and other published statements and information as related to governance and financial issues on behalf of the Board.
- Monitoring on an on-going basis SEAI Budgets and expenditure, including key non-financial data as appropriate.
- Monitoring the relationship with the Comptroller and Auditor General (C&AG), to ensure that there are no restrictions on the scope of the audit and to review the activities, findings, conclusions and recommendations of the external auditor. This includes reviewing the audit opinion and management letter from the C&AG, following completion of the audit, together with management's response to any issues raised by the C&AG in the course of the Audit and advising the Board accordingly.
- Reviewing the manner in which management ensures there is an adequate and effective system of internal financial, operational and compliance controls.
- Within the resources available, reviewing as appropriate to determine whether financial controls, including the delegation structure, enables the organisation to achieve its objectives on a value for money basis,
- Making recommendations to the Board on the appointment, re-appointment and removal of the SEAI Internal Auditors who shall have unrestricted access to the Chair of the Committee.
- Approving and reviewing the planned programme of work of the Internal Auditor, which should be submitted to the SEAI Board annually for approval.
- Reviewing all internal audit reports and findings and monitoring the implementation by management of significant recommendations.
- Monitoring and reviewing, at least annually, the effectiveness of the internal audit function and advising on the necessary level of resources and seeking to ensure that it is independent and free from management or other restrictions.
- Reviewing and approving the processes for managing risk, including the Risk Appetite Framework, approved by the Board, within SEAI. This shall include a high-level review of the SEAI Risk Register, on a biannual basis, and the overall SEAI control arrangements to mitigate these risks. It will also include systems established by management to identify, assess, manage and monitor key risks, both financial and non-financial, which might have significant implications for SEAI. The Committee should report to the Board accordingly on the outcome of this review. The Committee should also submit their review of the SEAI Risk Register to the Board, on an annual basis, for consideration.
- Overseeing the fraud risk policy and management process and the activities of the SEAI Programme Compliance Committee, including a review of the Annual SEAI Programme Compliance Committee report before submission to the SEAI Board.
- Ensuring there are appropriate procurement procedures in place and being implemented within SEAI.

- Examining SEAI Programmes, as required, in the context of the application of the Public Spending Code.
- Reviewing the effectiveness of the Committee on a regular basis, including the effectiveness of the relationship between the internal and external auditors.

### **Meetings**

- The Audit and Risk Committee shall meet at least four times each year and report on its activities to the Board.
- The quorum will be three.
- The Chief Executive Officer, other executives and representatives of the Comptroller and Auditor General may be in attendance at meetings of the Audit and Risk Committee for selected agenda items, at the request of the Chair.
- The Secretary to the Audit and Risk Committee shall maintain a written record of the proceedings of the Audit and Risk Committee.
- At the outset of each Committee meeting, the Chair should establish if Committee members have any real or perceived conflicts of interest in relation to Agenda items and enquire from the Committee if they wish to raise any issues under "Any Other Business".

### **Reporting**

- The Chair of the Audit and Risk Committee, or in his/her absence, a Committee member shall give an oral report on the proceedings of each Committee meeting at the next meeting of the Board.
- The approved minutes of each Audit and Risk Committee meeting shall be distributed to the members of the Board.
- An annual report from the Committee should be submitted to the Board. This should be compiled in accordance with the checklist for the effectiveness of Audit Committees as set out in the revised Code of Practice for the Governance of State Bodies issued in August 2016.

## **SEAI Performance Management and Remuneration Committee**

**Terms of Reference - as approved by SEAI Board on 28 September 2022 and reviewed by the Board in February 2025 as part of the review of this Code of Governance Framework.**

### ***Introduction***

The Performance Management and Remuneration Committee has been established in order to assess the overall performance of the CEO of SEAI, in the context of the Sustainable Energy Act (2002), the Oversight/Performance Delivery Agreement (PDA) between SEAI and the Department of Communications Climate Action and Environment (DECC) and the outputs achieved in the context of goals and objectives agreed by the SEAI Board on an annual basis. The Committee will also consider and approve remuneration, as appropriate, where applicable and in compliance with the revised Code of Practice for the Governance of State Bodies issued by the Minister for Public Expenditure and Reform in August 2016. The Committee also takes a high-level view, in consultation with the CEO, on the collective performance of senior management.

### ***Establishment***

The Performance Management and Remuneration Committee is a sub-committee of the Board of the Sustainable Energy Authority Ireland, established by formal resolution and comprises at least three non-executive members of the Board appointed by the Board.

The membership will rotate between members over time on the basis of one each year after an initial two-year period. The Chair will be a permanent member of the Committee.

### ***Responsibilities and Role***

The Performance Management and Remuneration Committee shall be responsible for:

- Recommending to the Board the Terms and Conditions (including remuneration, following consultation with DECC and the Department of Finance/Public Expenditure and Reform) upon which the Chief Executive Officer shall hold office, within the guidelines established from time to time by the Government;
- Reviewing and assessing the performance of the CEO on an annual basis in the context of agreed goals and objectives, and the Performance Delivery Agreement (PDA) between SEAI and the Department of the Environment Climate and Communications (DECC).
- Providing appropriate feedback to the CEO on the assessment and reporting to the SEAI Board on the outcome.
- Reviewing annually, on a high-level basis the collective overall performance of the senior management team in SEAI on the basis of feedback from CEO.
- Approving, following acceptance by DECC, the Authority's Action Plan in respect of any Public Sector Agreements, where applicable.

### ***Meetings and Reporting Structures***

The Performance Management and Remuneration Committee will be chaired by the Chair of the Board.

The quorum will be two.

The Committee will meet as required and report on its activities to the Board.

The Secretary to the Board will keep a decision record of the Committee's proceedings.

## **Business and Public Sector Committee**

**Terms of Reference - Approved by the SEAI Board on 26 May 2021 and reviewed by the Board in February 2025 as part of the review of this Code of Governance Framework.**

### ***Establishment:***

The SEAI Board Committee on the Business and Public Sector (BPSC) is established as a Committee of SEAI under Section 13 of the Sustainable Energy Act 2002 to perform the functions specified below.

### ***Membership:***

The Chairperson and members of the BPSC Committee shall be appointed by the Board.

The membership of the Committee shall consist of a Chairperson and three members. The Chairperson shall be a non-executive member of the Board. The members of the Committee shall comprise three other members of the SEAI Board.

If considered necessary, in due course, the Chair of the Committee may, in consultation with the Board Chair, seek Board approval for the appointment of an appropriate additional external expert member.

The Chair and the SEAI Board members shall be appointed for an initial period of two years (or the unexpired term of appointment to the SEAI Board, if shorter).

Other Board members, SEAI personnel or further external experts may be invited by the Chairperson, in consultation with the CEO, to attend and participate in meetings where they have expertise relevant to the work of the committee. In addition, the Committee may engage/liase with external business and Public Sector group/representative bodies as appropriate.

### ***Meetings:***

The BPSC Committee shall be convened by the Chairperson as is required to carry out its business. The schedule of meetings will be agreed with the Committee.

Members may attend in person, by teleconference or by videoconference. Members may also approve decisions by email in accordance with procedures agreed by the Committee.

A Quorum shall be **three** members participating in the meeting. Members approving decisions by email shall be present for the purposes of arriving at a quorum.

### ***Functions:***

The functions of the Committee are as follows:

- Ensuring appropriate oversight and monitoring of developments/outputs in relation to the SEAI Business and Public Sector Programme and also the Support Scheme for Renewable Heat.
- Developing, in consultation with the Executive, a co-ordinated and holistic approach to the funding of industry/business and in particular the approach to funding/ assisting SMEs.
- Supporting the Executive in the efforts to encourage wider Public Sector participation in Energy Efficiency Programmes, including those operated by SEAI.

- Making recommendations to the Board on any issues/topics considered desirable, in the context of the wider Business and Public Sector area.
- Overseeing recommended decisions by SEAI, in the context of the Memorandum of Understanding (MOU) on the SSRH between SEAI and the Minister for the Environment Climate and Communications before submission to the Board.
- Reviewing existing delegated authority levels approved by the Board and make recommendation to the Board for any changes considered necessary in relation to the BPSC/SSRH. The BPS Committee will operate in accordance with such delegated authority levels as agreed by the Board.
- Ensuring appropriate interaction and engagement with the other established SEAI Board Committees in relation to any crossover issues.

***Reporting:***

The Chair of the Committee shall brief the Board on the work of the Committee.

In addition, the Secretary shall compile reports of all meetings of the Committee, and these shall be submitted to the Board for information.

A formal annual Report on the SSRH Scheme, shall be compiled by the Executive, reviewed by the Committee, and submitted to the Board for approval before submission to the Department of the Environment Climate and Communications.

The Committee shall submit a written Annual Report to the Board on its work over the previous year, in order to provide clarity and transparency to the Board on its activities.

## National Retrofit Delivery Body

**Terms of Reference-- Approved by the SEAI Board on 28 September 2022 and reviewed by the Board in February 2025 as part of the review of this Code of Governance Framework.**

### **Establishment:**

The SEAI Board Committee on the National Retrofit Delivery Body (NRDB) is established as a Committee of SEAI under Section 13 of the Sustainable Energy Act 2002 to perform the functions specified below.

### **Membership:**

The Chairperson and members of the NRDB Committee shall be appointed by the Board.

The membership of the Committee shall consist of a Chairperson and three members. The Chairperson shall be a non-executive member of the Board. The members of the Committee shall comprise three other members of the Board.

If considered necessary, in due course, the Chair of the Committee may, in consultation with the Board Chair, seek Board approval for the appointment of an appropriate additional external expert member.

The Chair and the SEAI Board members shall be appointed for an initial period of two years (or the unexpired term of appointment to the SEAI Board, if shorter).

Other Board members, SEAI personnel or further external experts may be invited by the Chairperson, in consultation with the CEO, to attend and participate in meetings where they have expertise relevant to the work of the committee.

### **Meetings:**

The NRDB Committee shall be convened by the Chairperson as is required to carry out its business. The schedule of meetings will be agreed with the Committee.

Members may attend in person, by teleconference or by videoconference. Members may also approve decisions by email in accordance with procedures agreed by the Committee.

A Quorum shall be **three** members participating in the meeting. Members approving decisions by email shall be present for the purposes of arriving at a quorum.

### **Functions:**

The functions of the Committee are as follows:

- Ensure that an appropriate legal basis is put in place for SEAI to carry out the role of the NRDB and in this regard make recommendations, if considered necessary, to the Board regarding any changes required to the Sustainable Energy Act 2002.
- Oversee and monitor developments, at a strategic level, in relation to the establishment and operation of the NRDB within SEAI. This will include approval of an NRDB Implementation Plan and monitoring overall compliance with governance requirements.



- Monitor and review the outputs from the NRDB in the context of achieving the annual SEAI Business Plans objectives and alignment with the SEAI Strategy for the period 2021-2025.
- Ensure that there is an ongoing risk analysis on the NRDB including an update of the SEAI Risk Register to reflect new emerging risks in this context.
- Support, advise and propose on areas that the Committee feel should be considered by the NRDB.
- Making recommendations to the Board on any issues/topics considered desirable, in the context of the NRDB.
- Ensuring appropriate interaction and engagement with the other established SEAI Board Committees in relation to any crossover issues.

**Reporting:**

The Chair of the Committee shall brief and update the Board on the work of the Committee.

In addition, the Secretary shall compile reports of all meetings of the Committee, and these shall be submitted to the Board for information.

The Committee shall submit a written Annual Report to the Board on its work over the previous year, in order to provide clarity and transparency to the Board on its activities.

Delegation of Authority (TBC by Board in context of wider Delegation of Authority levels for Board Committees and the Executive).

## Research and Policy Insights Committee

**Terms of Reference – Approved by the Board on 28 September 2022 and reviewed by the Board in February 2025 as part of the review of this Code of Governance Framework.**

### **Establishment:**

The SEAI Board Committee on Research Policy and Insights (RPIC) is established as a Committee of SEAI under Section 13 of the Sustainable Energy Act 2002 to perform the functions specified below.

### **Membership:**

The Chairperson and members of the RPIC shall be appointed by the Board.

The membership of the Committee shall consist of a Chairperson and three members. The Chairperson shall be a non-executive member of the Board. The members of the Committee shall comprise three other members of the Board.

If considered necessary, in due course, the Chair of the Committee may, in consultation with the Board Chair, seek Board approval for the appointment of an appropriate additional external expert member.

The Chair and the SEAI Board members shall be appointed for an initial period of two years (or the unexpired term of appointment to the SEAI Board, if shorter).

Other Board members, SEAI personnel or further external experts may be invited by the Chairperson, in consultation with the CEO, to attend and participate in meetings where they have expertise relevant to the work of the committee.

### **Meetings:**

The RPIC Committee shall be convened by the Chairperson as is required to carry out its business. The schedule of meetings will be agreed with the Committee.

Members may attend in person, by teleconference or by videoconference. Members may also approve decisions by email in accordance with procedures agreed by the Committee.

A Quorum shall be **three** members participating in the meeting. Members approving decisions by email shall be present for the purposes of arriving at a quorum.

### **Functions:**

The functions of the Committee are as follows:

- Oversee the development of strategic plans and engagement approaches to enhance SEAI's impact and 'authoritative voice' and dissemination of insights across the energy ecosystem.
- Oversee the provision of strategic energy policy insight and advice to DECC and other Government Departments.
- Oversee the delivery of SEAI's statutory functions relating to Energy Statistics, Energy Modelling, and the National Energy Modelling Framework.
- Oversee SEAI's Research and Development (R&D) activities, including strategic partnerships with other bodies.

- Oversee SEAI's support services activities, including the District Heating Centre of Excellence, Single Point of Contact for Renewables Consenting and Permitting, and supports to sustainable energy communities and education.
- Support, advise and monitor the CEO and the Director of Research and Policy Insight in carrying out the work of the Directorate.
- Making recommendations to the Board on any issues/topics considered desirable, in the context of the RPIC.
- Ensuring appropriate interaction and engagement with the other established SEAI Board Committees in relation to any crossover issues.

**Reporting:**

The Chair of the Committee shall brief and update the Board on the work of the Committee.

In addition, the Secretary shall compile reports of all meetings of the Committee, and these shall be submitted to the Board for information.

The Committee shall submit a written Annual Report to the Board on its work over the previous year, in order to provide clarity and transparency to the Board on its activities.

## Appendix 5 - Policy for Dealing with Conflicts of Interest

### 1. Introduction

This policy sets out principles for the management of conflicts of interest, and potential conflicts of interest, arising in relation to Board members. It is designed to:

***so far as possible, prevent conflicts of interest from arising; ensure that any conflicts of interest that do arise are managed in such a way that the independence and integrity of the decisions of the Board are neither compromised nor perceived as being compromised.***

While this policy expressly addresses those conflicts of interest that can be readily anticipated, it is not possible to provide a comprehensive list of all of the conflicts of interest that might arise. Therefore:

- this procedure must be interpreted with regard to its spirit and purpose.
- Board members must comply with this procedure in spirit as well as in letter; and
- if there is any doubt as to whether a matter amounts to a conflict of interest, it should be presumed to be a conflict of interest ***until a decision is made to the contrary by an appropriate person.***

### 2. Scope

This policy applies to Board members and staff members as appropriate.

Some parts of this policy require Board members to ensure certain conduct by, or to make declarations in relation to, their spouses, parents, siblings or children or other connected persons or bodies corporate as set out in the Act and in the revised Code of Practice for the Governance of State Bodies, issued in August 2016, and as may be amended from time to time.

### 3. Objectives of the policy

The objectives of this policy are to:

- protect the Board corporately and each Board member individually against the breach of any law, including, for example, the breach of any of the provisions of the Ethics in Public Office Acts, 1995 and 2001.
- protect the Board corporately and each Board member individually against impropriety or the appearance of impropriety, including risk to its and their reputations; and
- protect the Board against any conflicts of interest that may be detrimental to the exercise of its functions.
- ensure, in so far as possible, that Board members make decisions free from any external influences, whether personal or financial, whilst recognising that it is precisely their position and expertise external to the Board that enables some of the Board members to make valuable contributions to its work.

while adhering to the principle that Board members should not make a personal profit as a result of their membership of the Board, other than the remuneration determined by the Minister for the Environment Climate and Communications.

### 4. Register of interests

- The Secretary to the Board shall maintain a register to be known as the register of Board Members' registrable interests (the "Register") in accordance with the provisions of the Ethics in Public Office

Acts, 1995 and 2001 and in order to comply with the requirements of the Code of Practice for the Governance of State Bodies.

- The Register shall be confidential and shall be updated on an annual basis. Changes in the interim should be notified to the Secretary as soon as possible. Only the Chairperson, Secretary and CEO shall have access to the Register.
- The purpose of the Register is to ensure transparency in relation to any interests of Board members, or of their spouses, parents, siblings or children or other connected persons or bodies corporate as set out in Code of Practice for the Governance of State Bodies, as may be amended from time to time.
- The Register must contain, in relation to each Board member, details of any of the following held or carried on by that Board member or any persons or bodies connected with a Board member, **where they give rise to a conflict of interest, as** more particularly set out in the Second Schedule of the Ethics in Public Office Act, 1995:
  - Occupational income, etc., other than that as office holder or member;
  - Shares, etc.;
  - Directorships;
  - Land and buildings;
  - Gifts;
  - Supplies of property or services
  - Travel facilities, etc.;
  - Remunerated position as a lobbyist, etc.; and
  - Contracts with the State.
- It is the duty of each Board member to declare to the Secretary any matter relating to him or her that is required to be included on the Register.
- If a Board member is in doubt as to whether a particular matter should be declared, he or she should declare it, and the Secretary (in consultation with the Chairperson (if appropriate) shall decide whether it is a matter that is required to be included on the Register.
- A Board member shall make a signed declaration of his or her interest for the purposes of the Register immediately on taking up appointment as a Board member and shall subsequently declare any new matter that is required to be included on the Register as soon as possible after it arises.
- Board members may be required at any time to confirm to the Secretary to the Board that their current entries on the Register are accurate and up to date, and the Secretary shall ask them to do so at least once in each year.

## **5. Board meetings**

Board members must comply with the procedure for the disclosure of conflicts of interest arising at Board Meetings, as set out in this Code of Governance.

## **Appendix 6 - Procedure for Dealing with Conflicts of Interest**

### **1. Introduction**

Given the diversity of the functions of the Authority, and the calibre of the Board members and staff employed by it, it is essential that an effective and robust policy and procedure exists to manage the actual or potential conflict of interest for any Board member or employee of the Authority.

This procedure outlines the steps that the Authority will undertake if, and when, situations arise where there is, or has the potential to be, a conflict of interest for a Board member or senior manager of the Authority. This procedure should be considered with, and is complementary to, the Policy for Dealing with Conflicts of Interest.

### **2. Managing Potential or Actual Conflict of Interest**

Before any item is discussed at a Board meeting, each Board member must disclose any conflict of interest that he or she believes may arise in relation to that item. If a Board member is in doubt as to whether a particular matter amounts to a conflict of interest and should be disclosed, he or she should disclose it.

The Chairperson (or, in his or her absence the Senior Independent Board Member) in his or her discretion will decide whether any matter disclosed by a Board member (other than the Chairperson or in his or her absence, the Acting Chairperson) amounts to a conflict of interest that should prevent that Board member from participating in the discussion of the relevant item.

Board members will elect an Acting Chairperson from amongst their numbers and decide whether any matter disclosed by the Chairperson amounts to a conflict of interest that should preclude the Chairperson from participating in the discussion at the relevant item. Should the Acting Chairperson be chairing the meeting, the Board members, will decide by taking a vote.

The decisions as to whether to disclose any matter and whether that matter amounts to a conflict of interest should be made having regard to the terms, and the spirit and purpose, of the policy for conflicts of interest.

Where the Chairperson decides that any Board member does have a conflict of interest in relation to any item that Board member may not participate in any discussion relating to that item or in any vote taken in relation to it. If requested to do so by the Chairperson, the Board member must also absent himself or herself from any discussion of the item.

In the event that a Board Member, Authority employee or Committee member receives any written paper in relation to any matter on which he or she believes that a conflict of interest may arise, they must disclose that conflict of interest to the Chairperson, or CEO as appropriate, at the earliest opportunity.

Should a Board Member (or staff member) receive an approach from a member of the public or organisation to intervene on their behalf and exert influence for the purpose of gaining advantage in accessing a service or any benefit, it is Board policy that no such intervention should be taken.

The Board, or a sub Committee may, at any time discontinue an investigation into a Board members' interests if it takes the view that the complaint concerned is frivolous or vexatious.

## **Appendix 7 – SEAI Internal Audit Charter**

(Approved by the Audit and Risk Committee on 4 December 2024)

### **1. Purpose of the Internal Audit Charter**

The purpose of the Internal Audit Charter is to define the role, purpose, authority, and responsibility of the Internal Audit Function in delivering outsourced Internal Audit Services to the Sustainable Energy Authority of Ireland ("the Authority").

The role of Internal Audit within the Authority is currently outsourced to Forvis Mazars.

### **2. Board Policy Statement**

The Board recognises the significant contribution to good governance and effective internal control made by an efficient and effective Internal Audit function. It pledges its full support to the Internal Audit function and to the Audit and Risk Committee ("ARC") in discharging the authorities and responsibilities contained in this Charter. Further, it respects the independence of the ARC and undertakes to provide adequate, competent and skilled resources to Internal Audit to properly discharge its function.

### **3. Purpose of Internal Audit**

Internal Auditing is an independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve the operations of the SEAI. It assists SEAI in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of governance, risk management and internal control processes within the SEAI.

The purpose of the internal audit function is to provide the Audit and Risk Committee ("ARC") and senior management with independent, risk-based, and objective assurance, advice, insight, and foresight.

#### *Commitment to adhering to the Global Internal Audit Standards*

Internal Audit will adhere to the mandatory elements of the Institute of Internal Auditors Global Internal Audit Standards ("the Standards") and topical requirements. Internal Audit will report periodically to the ARC and senior management regarding the internal audit function's conformance with the Standards, which will be assessed through a Quality Assurance and Improvement Program ("QAIP").

### **4. Internal Audit Mandate**

#### *Authority*

Internal Audit derives its authority from the Board through the ARC and is authorised to have:

- Unrestricted access to all SEAI functions, data records, information, property and personnel pertinent to carrying out internal audit responsibilities, including those controlled by subsidiaries and associates, if any. Internal auditors are accountable for confidentiality and safeguarding records and information.
- Full and free access to the ARC (including private meetings without management present), the Chief Executive Officer, the Director of Corporate Services, the Secretary to the Board and the Chairperson of the Board.
- Freedom to allocate resources, set frequencies, select subjects, determine scope of work and apply the techniques required to accomplish function's objectives.

- the necessary assistance and cooperation of personnel in units where audits are performed, other specialized services from within or outside the Authority.

Internal Audit will continuously review for conflicts of interest in the delivery of the internal audit plan and perform annual checks to confirm that no conflicts have arisen. Without prejudice to this objective, it may selectively review systems under development and advise on standards of control before implementation.

#### Independence, Organisational Position, and Reporting Relationships

- The Internal Audit Partner (from Forvis Mazars) will report functionally to the ARC and administratively to the Director of Corporate Services. The Internal Audit Partner will communicate and interact directly with the ARC, including in executive sessions and between ARC meetings as appropriate. This positioning provides the organisational authority and status to bring matters directly to senior management and escalate matters to the ARC, when necessary, without interference and supports the internal auditors' ability to maintain objectivity.
- The Internal Audit Function will remain free from interference by the Authority management team and any stakeholders to permit maintenance of a necessary independent and objective mental attitude. Matters of audit selection, scope, procedures, frequency, timing, or report content is subject to discussion with the ARC.
- The Internal Audit Partner will confirm to the ARC, at least annually, the organisational independence of the Internal Audit Function and any interference internal auditors encounter related to the scope, performance, or communication of internal audit work and results. The disclosure will include communicating the implications of such interference on the Internal Audit function's effectiveness and ability to fulfil its mandate.

### **5. Audit Committee Oversight**

- To establish, maintain, and ensure that the Authority's Internal Audit function has sufficient authority to fulfil its duties, the ARC will:
- Be responsible for the appointment of the outsourced Internal Audit Function and the oversight and evaluation of the adequacy, performance, and effectiveness of internal audit activity.
- Ensure that the Internal Audit Function is independent and has adequate resources to fulfil their duties, including implementation of the Annual Audit Plan
- Ensure the Internal Audit Function has unrestricted access to and communicates and interacts directly with the ARC, including in private meetings without senior management present.
- Approve the Internal Audit Charter, which includes the Internal Audit mandate and the scope and types of internal audit services.
- Approve the risk-based Internal Audit plan.
- Approve the Internal Audit function's budget.
- Make appropriate inquiries of management to determine whether there is inappropriate scope or resource limitations.
- Consider, at least every five years, if the Internal Audit Function should be subject to an external quality assessment.
- Approve all decisions regarding the performance evaluation, appointment, or removal of the outsourced Internal Audit Partner.

#### Changes to the Mandate and Charter

The Internal Audit Partner will obtain approval from the ARC, for any changes in the Internal Audit mandate and Charter.



## **6. Scope of Activities**

The scope of internal audit services covers the entire breadth of the organisation, including all activities, assets, and personnel and all identified auditable processes in the internal audit universe. The scope of internal audit activities also encompasses but is not limited to objective examinations of evidence to provide independent assurance and advisory services to the ARC and management on the adequacy and effectiveness of governance, risk management, and control processes for the Authority. The nature and scope of advisory services may be agreed with the party requesting the service, provided the Internal Audit function does not assume management responsibility and independence and objectivity is not impaired.

In planning, executing and reporting its work, the Internal Audit function should ensure that value-for-money auditing receives adequate attention. A partnership approach should be developed that ensures open communications, the delivery of meaningful services, and a cost-efficient system of internal controls.

Internal audit engagements may include:

- Evaluating the financial, operational, strategic and regulatory risks to ensure that these are appropriately identified, monitored, and managed, including assessments of the second line functions.
- Evaluating risk exposure relating to achievement of the organisation's strategic objectives.
- Evaluating the reliability and integrity of information and the means used to identify, measure, classify, and report such information.
- Evaluating operations or programmes to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.
- Assessing the actions of the Authority's directors, employees, and contractors in compliance with policies, procedures, and applicable laws, regulations, and governance standards.
- Reviewing that controls are adequately designed and operate effectively.
- Evaluating governance processes.
- Evaluating the effectiveness of the organisation's risk management processes.
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws and regulations which could have a significant impact on the organisation.
- Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets.
- Verifying if the resources and assets are acquired economically, used efficiently, and protected adequately.
- Evaluating specific operations assisting in the investigation of activities (including fraudulent) at the request of the ARC, the Board or senior management, as appropriate.
- Performing consulting and advisory services related to governance, risk management and control as appropriate for the organisation.

## **7. Internal Audit's Roles and Responsibilities**

Internal Audit is an independent appraisal function established within the Authority to examine and evaluate its activities as a service to the Board and management.

The scope of the Internal Audit Function's work encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the Authority's governance, risk management, and internal control processes in relation to the Authority's defined goals and objectives.

### Ethics and Professionalism

The Internal Audit Function will be undertaken in conformance with the Institute of Internal Auditors' ("IIA") Global Internal Audit Standards, including the principles of integrity, objectivity, competency, due professional care, and confidentiality. This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit activity's performance.

### Objectivity

Internal auditors must exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors must make a balanced assessment of all the relevant circumstances and remain free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner. Internal Auditors must not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance. If the Internal Audit Partner determines that objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to appropriate parties.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair the internal auditor's judgment.

### Managing the Internal Audit Function

Internal Audit has responsibility to:

- Develop and maintain an internal audit universe and strategic risk-based Internal Audit plan covering a rolling three-year period using appropriate risk assessment tools and submit that plan to the Audit Committee for review and approval, including changes thereafter.
- Develop annual audit plans, in consultation with the ARC and Senior Management, based on significant exposures identified in the strategic audit plan and submit such annual plans to the Audit and Risk Committee for approval.
- Develop the scope for each specific review for consideration of, and approval by the Audit and Risk Committee. In so doing the Internal Auditor will draw attention to matters which are specifically proposed to be out of scope.
- Implement the audit plans as approved, including any special projects assigned by the ARC, or requested by senior management subject to approval by the ARC.
- Review and adjust the Internal Audit plan, as necessary, in response to changes in the Authority's business, risks, operations, programmes, systems, and controls.
- Ensure each engagement on the Internal Audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
- Follow up on engagement findings and corrective actions, and report periodically to senior management and the ARC any corrective actions not effectively implemented.
- Issue reports to the ARC addressing the results of audits conducted, summarising observations and recommendations made, and management responses to the audit findings.
- Ensure adherence to the Authority's relevant policies and procedures unless such policies and procedures conflict with the Internal Audit Charter or the Global Internal Audit Standards. Any such conflicts will be resolved or documented and communicated to the ARC and senior management.

- Ensure that Internal Audit Function collectively possesses or obtain the knowledge, skills, and other competencies and qualifications needed to meet the requirements of the Internal Audit Charter, Global Internal Audit Standards.
- Considering the scope of work, in consultation with the Audit and Risk Committee, and liaising with external auditors for the purpose of providing optimal audit coverage;
- Reporting periodically on the internal audit activity's purpose, authority, responsibility, performance metrics (see Appendix I) and performance relative to its plan.
- Reporting significant risk exposures and control issues relating to the processes for controlling the activities of the Authority, including fraud risks, governance issues, and other matters needed or requested by the ARC, the Board or senior management, as appropriate.
- Maintaining a professional audit service staffed with sufficient knowledge, experience and skills to meet the requirements of this charter; and
- Ensuring that confidentiality is maintained over all information and records obtained in carrying out its audits.
- Internal Audit has responsibility to ensure that the audit programme and methodology take due account of the possibility of fraud.
- As considered necessary, bring to the attention of the Committee Chair, any issues identified during the audit review, which is deemed to be outside the scope of the audit, but which, in the opinion of the Internal auditor, should be referenced in the audit report. The ARC may deem it necessary to amend the scope of the audit following consideration.

The Management and the ARC of the Authority has responsibility to:

- Keep Internal Audit informed of all material changes within the organisation.
- Report all material risk incidents and events to Internal Audit in a timely manner.

## **8. Management's Responsibilities**

Management responsibilities include but are not limited to:

- Managing risk, maintaining effective controls and implementing internal audit (and external audit) recommendations in an appropriate manner.
- Proactively interacting with the Internal Audit function, responding promptly to draft reports and agree actions and timescales to rectify control weaknesses identified.
- Following up on the implementation of agreed audit actions and reporting progress to the ARC on a bi-annual basis.
- Management also has primary responsibility for the prevention of fraud and for detecting and resolving any fraud that may occur.

## **9. Reporting**

A written report will be prepared and issued by the Internal Audit Function following the conclusion of each internal audit engagement to the ARC. The internal audit report will include Management's response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management's response, whether included within the original audit report or provided shortly thereafter, should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The Internal Audit Function will be periodically responsible for independent, appropriate follow-up on the findings and recommendation noted in the internal audit reports, as agreed via the rolling 3-year Internal Audit Plan. All findings should remain in an open issues file maintained by Management until cleared.

On a quarterly basis (or as required by ARC), a quarterly report will be issued to communicate to the ARC the progress in accordance with the internal audit plan including other matters (see Appendix I).

The Internal Audit Function will prepare an annual report for the ARC to report on and confirm matters noted in this Charter, including confirmation of organisational independence and conformance with the Global Internal Audit Standards, as well as reporting on the purpose of the internal audit activity authority and responsibility, as well as performance relative to its internal audit plan. Reporting will also include significant risk exposures and control issues, including fraud risks, governance issues and other matters needed or requested by senior management, the Audit and Risk Committee and the Board.

## **10. Quality Assurance and Improvement Programme**

The Internal Audit Partner will develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the Internal Audit Function. Annually, the Internal Audit Partner will communicate with the Audit & Risk Committee and senior management about the Internal Audit Function's quality assurance and improvement program, including the results of internal assessments (ongoing monitoring and periodic self-assessments).

The Audit & Risk Committee will consider, at least once every five years, if an external quality assessment of the Internal Audit Function or a self-assessment with independent validation should be carried out. The Internal Audit Partner will participate in any such assessment, initiated by the Audit Committee. Any external assessment must be conducted by a qualified, independent assessor or assessment team and qualifications must include at least one assessor holding an active Certified Internal Auditor credential.

## **11. Review of this Charter**

In accordance with the Standards, this Charter will be reviewed annually and approved by the Internal Audit Function and the Audit and Risk Committee.

## Appendix I: Internal Audit Performance Metrics Reporting to Audit Committee

	Performance Metric	Description	Timing	Remarks	Rating
1	Internal Audit Plan and Universe	Develop and maintain an Internal Audit Universe and strategic risk-based Internal Audit plan on a rolling three-year period using appropriate risk assessment tools and submit that plan to the ARC for review and approval.	Annual		Met / Not Met
2	Formalised scope for each audit	Develop a formalised scope (e.g., Terms of Reference) per audit area which must be agreed with management prior to the start of audit fieldwork	Per occurrence		Met / Not Met
3	Progress report to ARC	Completion of approved audit plan update report, including any ad hoc audits assigned / requested by the AC and/or management	Quarterly		Met / Not Met
4	Attend ARC meetings	Internal Audit Partner attends ARC meetings quarterly and presents updates to audit plan and completed reports.	Per occurrence		Met / Not Met

## **Appendix 8 - Procedure for Board Members to obtain Independent Professional Advice**

### **Principle**

Board members may, in the furtherance of their duties, take independent professional advice, if necessary, at the reasonable expense of the Sustainable Energy Authority of Ireland.

### **Rationale**

The Board should be supplied in a timely manner with information in a form and of a quality appropriate to enable it to discharge its duties.

### **Procedure**

If a Board member decides to seek independent legal advice through SEAI, he or she shall put his or her request in writing to the Secretary to the Board.

The Board Secretary shall notify the Chair of the Board and/or the Chair of the Audit and Risk Committee of the request and the estimated costs and seek the approval for the procurement of the advice.

The advice supplied to the Board member shall be provided to all members of the Board. In the event that a request for advice is declined, this decision shall be notified to the full Board.

## **Appendix 9 - Principles of a Quality Customer Service for Customers and Clients of the Public Service (1997)**

SEAI has published a statement that outlines the nature and quality of service which customers can expect, and it is available on the SEAI website. It consists of a Customer Service Charter, Customer Action Plan and Feedback, Complaints and Appeals process.

### **Customer Service Charter**

---

Our vision is to be a leading authority driving Ireland's sustainable energy transformation for the benefit of society.

#### **Who are we and what do we do?**

SEAI is Ireland's national sustainable energy authority. We work with householders, businesses, communities, and the government to create a cleaner energy future.

Our mission is to be at the heart of delivering Ireland's energy revolution. You can find out more about the SEAI Values here (Insert link to [Our Values | About Us | SEAI](#))

#### **Our commitment to you**

We will:

- Deliver our services to all our customers in a timely, effective, and professional manner.
- Conduct our business in a fair, open, and transparent manner.
- Respect your privacy and confidentiality in accordance with GDPR guidelines.
- Strive for excellence in the development and delivery of programmes and services through consultation and continuous improvement.
- Provide choice in the delivery of our services, while endeavouring to accommodate diversity and physical access needs.
- Provide expert, authoritative, and independent advice and information in a form that best suits your needs.

### **Customer Action Plan**

SEAI commits to delivering our services to all customers in a timely, effective and professional manner. This will be done in accordance with our values and our commitment to Quality Customer Service.

#### **How to submit feedback, an appeal or complaint**

We value your opinion (compliments, comments and complaints).

SEAI aims to deliver an efficient and effective service to our customers. We listen to you and use the information we gain from feedback, complaints and appeals to improve our services. We will deal with complaints and appeals in a fair and sympathetic manner and respond based on the timelines below:

## How to contact us

- Phone – **01-8082100**
- Email – [info@seai.ie](mailto:info@seai.ie)
- Post – **SEAI, PO Box 119, Cahersiveen, Co. Kerry**
- Webchat on [www.seai.ie](http://www.seai.ie)

## Customer Action Plan

SEAI commits to delivering our services to all customers in a timely, effective and professional manner. This will be done in accordance with our values and our commitment to Quality Customer Service.

## Our commitment to Quality Customer Service

We align with the Government's 12 principles of quality customer service <https://enterprise.gov.ie/en/who-we-are/customer-service/12-principles-of-quality-customer-service/>

## Contacting SEAI

SEAI commits to providing maximum choice and access in the delivery of our services. We will aim to accommodate diversity and physical needs by making it easier and more convenient to do business with us.

### Customers can contact us via:

- Phone - **018082100**
- Email – [info@seai.ie](mailto:info@seai.ie)
- Post – **SEAI, PO Box 119, Cahersiveen, Co. Kerry**
- Webchat at [www.seai.ie](http://www.seai.ie)
- Online forms

### We will assist with accessibility by:

- Ensuring that all publications are available online
- Continuing to ensure our website is accessible to the visually impaired
- Ensuring our offices comply with occupational and safety standards
- Accommodating the diverse needs of our stakeholders in an appropriate manner
- Recognising and respecting all stakeholders in an equitable manner regarding service delivery
- Complying with the Official Languages Act 2003- Acht na dTeangacha Oifigiúla 2003

### We commit to:

- Answering calls promptly during business hours
- Acknowledging receipt of all correspondence promptly
- Logging all details in a central database (CRM) capturing, name, address and description of query
- Being helpful and courteous
- Ensuring that all replies carry contact details
- Applying quality assurance checks via call calibration

**We will commit to respecting the environment in the delivery of our services. We demonstrate this by:**



- Adhering to sustainability values such as
  - Providing video conferencing facilities to reduce travel
  - Working toward paperless work practices

**We commit to the following work practices:**

- We aim to conduct our business in a fair open and transparent manner. We have processes and systems designed to comply with GDPR regulations.
- We strive for excellence in the development, delivery, and improvement of programmes with the customer and stakeholder at the heart of them.
- We provide accurate, trusted and independent advice and information in a form that suits the customer's needs.
- We aim to resolve complaints and appeals efficiently and effectively in line with our complaints and appeals procedure.

**Consultation:**

We strive to continuously improve our services and offerings.

This is done by carrying out regular consultations and surveys and supplying an accessible feedback mechanism for customers.

**Evaluation:**

To measure our success in achieving the above we will:

- Perform a regular review of the Customer Action Plan
- Seek feedback from internal and external customers on the quality of our service
- Review service feedback through our online feedback form and act accordingly
- Investigate appropriate externally recognised customer service standards and seek to attain such standards.

**Reporting:**

- We will report our performance in relation to complaints and appeals in the Annual Report.

**Review**

- Our Customer Action Plan will be reviewed every three years.

**Customer Responsibility - How can you help us?**

Please bear in mind the following points to help us serve you better:

- Treat our staff courteously
- Provide feedback so that we can improve our service
- Provide accurate information, including any relevant reference numbers, when dealing with us
- Provide your contact details (name, daytime phone number, email)

## Feedback, Complaints and Appeals Policy

### We value your opinion (compliments, comments and complaints)

SEAI aims to deliver an efficient and effective service to our customers. We listen to you and use the information we gain from feedback, complaints and appeals to improve our services. We will deal with complaints and appeals in a fair and sympathetic manner and respond based on the timelines below.

#### Feedback

Your feedback, both positive and negative, is important to SEAI. We will use this information to make improvements in our programmes.

What can I provide feedback or express dissatisfaction about?

- Eligibility for schemes which are based on set rules
- Waiting lists for SEAI-contracted works
- Availability of certain measures e.g. windows and doors
- SEAI-registered contractors/assessors/installers etc
- General feedback on SEAI ways of working
- General feedback on SEAI services

This list is not exhaustive and other expressions of dissatisfaction can be directed through the Feedback channel.

How can I submit feedback?

You can submit your feedback via email at [info@seai.ie](mailto:info@seai.ie) or by post to SEAI, PO Box 119, Cahersiveen, Co. Kerry

## Complaints and Appeals

### What can I submit a complaint or appeal about?

**A complaint** is a written expression of dissatisfaction where a person believes we did not meet service standards or meet their expectations regarding an SEAI grant or service.

Customers can submit a complaint related to errors, delays and unsatisfactory service received.

**An appeal** is a request for review of a decision under any SEAI grant programme.

Customers can appeal a decision regarding grants, for example:

- If a grant application was rejected and you believe you were in compliance with all the scheme criteria.
- If costs claimed for were deemed ineligible.

Contractors may appeal inspection results in accordance with the Guide to Inspections

*Note: A contractor or BER Assessor who has been directly engaged by a customer cannot be dealt with under a complaint or appeal. Any issues an individual may have with a contractor or BER Assessor should be raised directly with them and not SEAI.*

### What issues are not covered under Complaints and Appeals?

There are some situations which are not covered by this policy, such as:

- A routine first-time request for a service.

- Criteria for eligibility for grants.
- Issues with customer-appointed contractors or BER assessors
- Matters which are the subject of litigation.
- A request under Freedom of Information, Access to Information on the Environment, or data protection legislation.
- A request for information or an explanation of policy or practice.
- An attempt to reopen a complaint or appeal previously concluded under this policy or to have a complaint or appeal reconsidered where we have already given our final decision following an investigation. If you are still not satisfied, you can ask the Office of the Ombudsman for an independent review of the complaint or appeal.
- Actions of staff which are not related to their role in SEAI.
- A complaint or an appeal will not be dealt with if it is considered on initial examination to be trivial or frivolous. Should this be the case, SEAI will advise you of our views in respect of this and will not deal any further with the complaint or appeal.

If a complaint or appeal is considered to be vexatious, SEAI may choose to limit or cease correspondence with you. This decision will be recorded as part of the record of complaint or appeal.

Unreasonable, vexatious or abusive complainants, along with threats or abuse of staff will not be tolerated and, where appropriate, will be referred to An Garda Síochána.

If other procedures or rights of appeal can help you resolve your concerns, we will give information and advice to help you.

### **How to submit a Complaint or Appeal**

Complete the online form By Post to **SEAI, PO Box 119, Cahersiveen, Co. Kerry**

Please provide the following information in your submission:

- Name
- Contact details (phone and email where possible)
- Grant Application name and/or Reference Number
- Documents to support your complaint.

This will enable us to investigate your complaint promptly and respond to you as soon as possible. If you are making a complaint on behalf of another person, please submit their written agreement for you to represent them.

### **Complaint and Appeals Procedure**

We have a standard procedure in place to handle complaints and appeals in a fair and thorough manner. Upon receiving your complaint or appeal:

- SEAI will acknowledge receipt of your complaint or appeal within 5 working days.
- We will investigate your complaint or appeal and respond to you within 20 working days from receipt.

### **Requesting an Escalation**

If you feel our response did not address your concern adequately and you have **additional information or new points** that were not previously considered, you can request an escalation of your complaint or appeal.

In this case, you must include the following in your request:

- A clear and concise reason for escalation
  - Additional information or new points that were not previously considered for an escalation
- Your request must be submitted in writing or by email to SEAI within **20 working** days of receiving the original decision.

A response and remedy proposal, if applicable, will be issued within 20 working days of receipt by SEAI.

It is important to note that the decision outcome of the review will constitute SEAI's final position on the matter.

If, for some reason it is not possible for SEAI to respond within the stated timeframes, SEAI will notify you in advance and provide an explanation for the delay. The maximum extension allowed will be 20 working days after the original deadline.

### **Option to Refer your Complaint or Appeal to the Ombudsman**

If you remain unhappy with our response to your complaint or appeal, then you can refer it to the Office of the Ombudsman.

The Ombudsman is fair, independent, and free to use. The Ombudsman will ask you for details of your complaint and a copy of our final response to your complaint.

The best way to contact the Ombudsman is by:

- Clicking on the 'Make A Complaint' link at [www.ombudsman.ie](http://www.ombudsman.ie)
- Write to the Ombudsman at: 6 Earlsfort Terrace, Dublin 2, D02 W773

### **How to contact us**

Phone - 01 808 2100

Email – [info@seai.ie](mailto:info@seai.ie)

Post – SEAI, PO Box 119, Cahersiveen, Co. Kerry

Webchat - [www.seai.ie](http://www.seai.ie)

## Appendix 10 - SEAI Protected Disclosures (Whistle Blowing) Policy and Procedure, Disclosures Policy

(Policies approved by the Board on 27 March 2024).

# PROTECTED DISCLOSURES (WHISTLE-BLOWING) POLICY AND PROCEDURE

## 1. Introduction

The Sustainable Energy Authority of Ireland (SEAI) is committed to providing workers with a confidential and secure pathway for reporting concerns about wrongdoing in the workplace and also to protecting workers against penalisation for having reported those concerns.

The Protected Disclosures Act 2014 (as amended) ("the **Act**") protects workers who report certain workplace wrongdoings (known as relevant wrongdoings). A formal channel for reporting such concerns has been established in accordance with the Act.

This document sets out: how to make a report; the types of wrongdoing that constitute a protected disclosure; what happens when a report is received; and the protections that are available against penalisation for reporting a concern about wrongdoing.

SEAI will:

- Keep the identity of the reporting person and any person named in a report confidential, in so far as possible;
- Not tolerate any penalisation or threat of penalisation of the reporting person or persons associated with the reporting person;
- Acknowledge all reports within seven days;
- Follow-up diligently on all reports of relevant wrongdoing;
- Endeavour to provide feedback to the reporting person within three months of acknowledgement; and
- Provide further feedback at three-month intervals on written request.

SEAI's Director of Corporate Services has overall responsibility for the Procedures set out in this policy.

SEAI's Director of Corporate Services, Head of Governance and Senior Information Compliance Officers are the Designated Persons with day-to-day responsibility for the handling of reports.

**Please read this document carefully before making a report. It is solely your responsibility to ensure you meet the criteria for protection under the Act.** If you have any queries about this policy, please contact: [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie).

## 2. WHO THIS POLICY APPLIES TO

This policy applies to all "workers". A "worker" is an individual in a work-related relationship with SEAI who acquires information on relevant wrongdoings in a work-related context and who is or was:

- (a) an employee;
- (b) an independent contractor;
- (c) an agency worker;
- (d) a trainee;
- (e) a shareholder of an undertaking;
- (f) a member of the administrative, management or supervisory body of an undertaking including non-executive members;
- (g) a volunteer;
- (h) an individual who acquired information on a relevant wrongdoing during a recruitment process; or an individual who acquired information on a relevant wrongdoing during pre-contractual negotiations (other than a recruitment process).

### **3. What is a protected disclosure?**

Making a report in accordance with the Protected Disclosures Act is referred to as “making a protected disclosure”. A “protected disclosure” means a disclosure of “relevant information” made by a “worker” in the manner specified in the Act. The relevant information must, in the reasonable belief of the worker, tend to show one or more relevant wrongdoings and have come to the attention of the worker in a work-related context. These requirements are explained in more detail below.

### **4. What is relevant information?**

Relevant information is information which in the reasonable belief of the worker tends to show one or more relevant wrongdoings and it came to the attention of the worker in a work-related context.

The information should disclose facts about someone or something, rather than a general allegation that is not founded on any facts.

Workers should not investigate allegations of wrongdoing. The Designated Person is responsible for the appropriate follow up of all reports.

#### **4.1 What is a reasonable belief?**

The worker’s belief must be based on reasonable grounds, but it is not a requirement that the worker is ultimately correct. Workers are not expected to prove the truth of an allegation.

No disciplinary or other action will be taken against a worker who reasonably believes the information they have reported tends to show a wrongdoing, even if the concern raised turns out to be unfounded.

The motivation of the worker in making a report is irrelevant as to whether or not it is a protected disclosure. The worker will be afforded the protections of the Act if they reasonably believe, when making the report, that the information disclosed tended to show a relevant wrongdoing. A report made in the absence of a reasonable belief is not a protected disclosure and may result in disciplinary action. It is a criminal offence to make a report that contains any information the reporting person knows to be false. A person who suffers damage resulting from the making of a known to be false report has a right to take legal action against the reporting person.

#### **4.2 What are relevant wrongdoings?**

To qualify as a protected disclosure, the matter reported must be a “relevant wrongdoing”. The following are relevant wrongdoings:

- (a) that an offence has been, is being or is likely to be committed
- (b) that a person has failed, is failing or is likely to fail to comply with any legal obligation, other than one arising under the worker's contract of employment or other contract whereby the worker undertakes to do or perform personally any work or services;
- (c) that a miscarriage of justice has occurred, is occurring or is likely to occur;
- (d) that the health or safety of any individual has been, is being or is likely to be endangered;
- (e) that the environment has been, is being or is likely to be damaged;
- (f) that an unlawful or otherwise improper use of funds or resources of a public body, or of other public money, has occurred, is occurring or is likely to occur;
- (g) that an act or omission by or on behalf of a public body is oppressive, discriminatory or grossly negligent or constitutes gross mismanagement;
- (h) that a breach of EU law as set out in the Act, has occurred, is occurring or is likely to occur; or that information tending to show any matter falling within any of the preceding paragraphs has been, is being or is likely to be concealed or destroyed or an attempt has been, is being or is likely to be made to conceal or destroy such information.

It does not matter whether a relevant wrongdoing occurred, occurs or would occur in Ireland or elsewhere and whether the law applying to it is that of Ireland or that of any other country or territory.

Workers may be subject to mandatory reporting obligations relevant to their role or profession. Such reports may or may not amount to protected disclosures under the Protected Disclosures Act depending on whether the requirements of the Act are met. Legislation other than and in addition to the Protected Disclosures Act may provide for making reports. Workers should ensure that they are aware of what protections, if any, such other legislation and/or the Protected Disclosures Act makes available to them and seek legal advice if necessary.

#### **4.3 MATTERS THAT ARE NOT RELEVANT WRONGDOINGS**

A matter is not a relevant wrongdoing which it is the function of the worker or the worker's employer to detect, investigate or prosecute and does not consist of or involve an act or omission on the part of the employer.

A matter concerning employment grievances exclusively affecting a worker is not a relevant wrongdoing and will not be dealt with under this procedure. Such matters are dealt with under SEAI's Grievance Policy or other appropriate SEAI policy.

Failure to comply with a legal obligation that arises solely under the worker's contract of employment or other contract where the worker undertakes to do or perform personally any work or services is not a relevant wrongdoing. Such matters are dealt with under SEAI's existing policies which can be found on the SEAI Human Resources SharePoint page. Protected disclosures can only be made by workers and be made in a work-related context (see next section). Reports of wrongdoing that do not fulfil this criteria may be dealt with under SEAI's Disclosures Policy or SEAI's Customer Charter.

#### **4.4 WHAT IS A WORK-RELATED CONTEXT?**

"Work-related context" means current or past work activities through which, irrespective of the nature of those activities, persons acquire information concerning a relevant wrongdoing and within which those persons could suffer penalisation if they reported such information.

### **5. HOW TO MAKE A REPORT**

Reports should be made to the Designated Persons at [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie) who receive reports under this policy. Reports can be made in writing or orally.

Reports can be made as follows:

- By email to: [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie)
- By telephone to: 01 8551640
- By post (marked *Strictly Private and Confidential*) to:

**SEAI Protected Disclosures Designated Person**

Sustainable Energy Authority of Ireland 3 Park  
Place  
Hatch Street Dublin  
2 D02 FX65

Reports should contain at least the information set out in Appendix A.

## **6. ANONYMOUS REPORTS**

Reports can be made anonymously. Persons who choose to report anonymously and whose report meets the requirements of the Act remain entitled to all of the protections of the Act. Anonymous reports will be followed-up to the greatest extent possible. However, it may not be possible to fully assess and follow-up on an anonymous report.

In addition, implementing certain elements of this policy – such as seeking further information, maintaining communication and protecting the reporting person’s identity or protecting them from penalisation – may not be possible.

## **7. PROCESS FOLLOWING RECEIPT OF A REPORT**

This process shall apply to all reports made in the manner specified in section 4 of this policy. This process may not apply if a report or other communication is made in a manner other than that specified in section 4.

### **7.1 ACKNOWLEDGEMENT**

All reports received in accordance with section 4 shall be acknowledged within seven days of receipt.

The acknowledgement shall include access to the relevant procedures.

### **7.2 ASSESSMENT**

The Designated Person shall assess if there is *prima facie* evidence that a relevant wrongdoing might have occurred.

The Designated Person may, if required, make contact with the reporting person, in confidence, in order to seek further information or clarification regarding the matter(s) reported.

It may be necessary to differentiate the information contained in the report. It may be the case that not all of the matters reported fall within the scope of this policy or the Protected Disclosures Act. Different parts of a report may need to be approached separately, and some matters may be directed to another, more appropriate, policy or procedure (e.g. personal grievances).



The Designated Person may decide that there is no *prima facie* evidence of a relevant wrongdoing and either close the procedure or refer the matter to another relevant procedure. If this occurs, the Designated Person will notify the reporting person in writing of this decision and the reasons for it.

If the Designated Person decides that there is *prima facie* evidence of a relevant wrongdoing, the report may be referred to another appropriate person or persons to review the matter and, where appropriate, necessary action will be taken to address the wrongdoing, having regard to the nature and seriousness of the matter.

An informal process may be used to address a disclosure where the alleged relevant wrongdoing is relatively straightforward or not very serious or does not require consideration of the making of adverse findings about any individual.

If a decision to close the matter or refer it to another process is made, a party affected by this decision may request a review of this decision, by emailing [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie) within 14 days of the original decision.

### **7.3 INVESTIGATION**

The Designated Person shall decide whether or not an investigation is required.

If an investigation is required, the Designated Person shall decide how the matter should be investigated.

The nature and seriousness of the matter reported will inform whether the matter can or should be investigated internally. In some circumstances it may be more appropriate for an investigation to be carried out by external experts, or a statutory body, or for the matter to be reported to An Garda Síochána or other body.

Investigations will be undertaken in accordance with the general principles of natural justice and fair procedures and any other relevant procedures of SEAI as appropriate.

Responsibility for investigating and addressing allegations of wrongdoing lies with SEAI and not the reporting person. Reporting persons should not attempt to investigate wrongdoing themselves.

A review of a decision not to investigate can be requested by emailing [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie) within 14 days of the original decision.

### **7.4 FEEDBACK**

Feedback will be provided to the reporting person within a reasonable time period and no later than three months after the initial acknowledgement of the report.

A reporting person can request the Designated Person, in writing, provide further feedback at three-month intervals until the process of follow-up is completed.

Any feedback is provided in confidence and should not be disclosed by the reporting person other than:

- (a) as part of the process of seeking legal advice in relation to their report from a solicitor or a barrister or a trade union official; or

- (b) if required in order to make a further report through this or another reporting channel provided for under the Act (see next section).

Feedback may include information on the action taken or envisaged to be taken as follow-up to that report or may confirm that the investigation is ongoing.

Feedback will not include any information that could prejudice the outcome of an investigation or any other action that might follow.

Feedback will not include any information relating to an identified or identifiable third party. In particular, feedback will not include any information on any disciplinary process involving another worker. Such information is confidential between the employer and the worker concerned.

If the follow-up process determines that no relevant wrongdoing has occurred, the reporting person will be informed of this in writing, which may include the reasons for this decision. A review of this decision may be requested by emailing [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie) within 14 days of the original decision.

The final outcome of the process triggered by the report will be communicated to the reporting person, subject to any legal restrictions concerning confidentiality, legal privilege, privacy and data protection or any other legal obligation.

## **8. OTHER REPORTING CHANNELS**

The aim of this policy is to provide a means by which workers can safely and securely raise concerns about relevant wrongdoing and to give certainty that all such concerns will be dealt with appropriately. SEAI is confident that issues can be dealt with internally and strongly encourages workers to report such concerns internally in accordance with this policy.

There may, however, be circumstances where a worker may not wish to raise their concern internally or if they have grounds to believe that an internal report they have made has not been followed-up properly.

The Protected Disclosures Act sets out a number of alternative external channels for workers to raise concerns. Information regarding these channels is set out in Appendix B of this policy.

It is important to note, however, that if a worker is considering making a disclosure using these other channels, different and potentially more onerous conditions may apply. Workers are advised to seek professional advice before reporting externally. Information on where to seek independent, confidential advice in this regard can be found at section 13 of this policy.

## **9. PROTECTION FROM PENALISATION**

SEAI is committed to protecting workers from penalisation or a threat of penalisation because the worker made a protected disclosure. Acts of penalisation will not be tolerated.

If a worker is penalised or threatened with penalisation this can be reported to Head of Human Resources in SEAI and the report will be followed-up in accordance with relevant procedures. Penalisation is any direct or indirect act or omission that occurs in a work-related context, which is prompted by the making of a protected disclosure and causes or may cause unjustified detriment to a worker.

Penalisation includes, but is not limited to:

- (a) Suspension, layoff or dismissal;
- (b) Demotion, loss of opportunity for promotion or withholding promotion;
- (c) Transfer of duties, change of location of place of work, reduction in wages or change in working hours;
- (d) The imposition or administering of any discipline, reprimand or other penalty (including a financial penalty);
- (e) Coercion, intimidation, harassment or ostracism;
- (f) Discrimination, disadvantage or unfair treatment;
- (g) Injury, damage or loss;
- (h) Threat of reprisal;
- (i) Withholding of training;
- (j) A negative performance assessment or employment reference;
- (k) Failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment;
- (l) Failure to renew or early termination of a temporary employment contract;
- (m) Harm, including to the worker's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- (n) Blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- (o) Early termination or cancellation of a contract for goods or services;
- (p) Cancellation of a licence or permit; and
- (q) Psychiatric or medical referrals.

Appropriate action, which may include disciplinary action, will be taken against a worker who penalises a reporting person or other individual due to the making of a protected disclosure.

The normal management of a worker who has made a protected disclosure is not penalisation.

If a protected disclosure is made during an investigation or disciplinary process to which the reporting person is subject, it will not automatically follow that the making of the report will affect the investigation or disciplinary process. Separate processes unconnected with the disclosure will ordinarily continue to proceed.

Disclosure of an alleged wrongdoing does not confer any protection or immunity on a worker in relation to any involvement they may have had in that alleged wrongdoing.

The Protected Disclosures Act provides that a worker who suffers penalisation as a result of making a protected disclosure can make a claim for redress through either the Workplace Relations Commission or the courts, as appropriate.

A claim concerning penalisation or dismissal must be brought to the Workplace Relations Commission within 6 months of the date of the act of penalisation or the date of dismissal to which the claim relates.

A claim for interim relief pending proceedings at the Workplace Relations Commission or the courts must be made to the Circuit Court within 21 days of the last date of penalisation or date of dismissal.

It is a criminal offence to penalise or threaten penalisation or permit any other person to penalise or threaten penalisation against any of the following:

- The reporting person;
- A facilitator (a person who assists the reporting person in the reporting process);

- A person connected to the reporting person, such as a colleague or a relative; or
- An entity the reporting person owns, works for or is otherwise connected with in a work- related context.

## **10. PROTECTION FROM LEGAL LIABILITY**

Section 14 of the Act refers to a person's *Immunity from civil liability* with regards to the making of a protected disclosure, and provides as follows:

**14 (1)** *No cause of action in civil proceedings, other than a defamation action (within the meaning of the [Defamation Act 2009](#)), shall lie against a person in respect of the making of a protected disclosure.*

## **11. CONFIDENTIALITY AND PROTECTION OF IDENTITY**

SEAI is committed, in so far as possible, to protecting the confidentiality of the identity of both workers who raise a concern under these procedures and any third party mentioned in a report and to treating the information disclosed in confidence.

SEAI's Information Compliance Office maintains reports with restricted access.

SEAI's Disclosures log is maintained in an anonymous format, further protecting the identity of reporting persons.

Subject to the exceptions below, the identity of the reporting person or any information from which their identity may be directly or indirectly deduced will not be shared with anyone other than persons authorised to receive, handle or follow-up on reports made under this policy without the explicit consent of the reporting person.

The Protected Disclosures Act provides for certain exceptions where a reporting person's identity or information that could identify the reporting person can be disclosed without the reporting person's consent. These are:

- (a) Where the disclosure is a necessary and proportionate obligation imposed by EU or national law in the context of investigations or judicial proceedings, including safeguarding the rights of defence of persons connected with the alleged wrongdoing;
- (b) Where the person to whom the report was made or shared shows, they took all reasonable steps to avoid disclosing the identity of the reporting person or any information that could identify the reporting person;
- (c) Where the person to whom the report was made or shared reasonably believes disclosing the identity of the reporting person or information that could identify the reporting person is necessary for the prevention of serious risk to the security of the State, public health, public safety or the environment; and
- (d) Where the disclosure is otherwise required by law.

Where a reporting person's identity or information that could identify a reporting person is to be disclosed under exceptions (a) to (d), above, the reporting person will be notified in writing in advance, unless such notification would jeopardise:

- The effective investigation of the relevant wrongdoing reported;

- The prevention of serious risk to the security of the State, public health, public safety or the environment; or
- The prevention of crime or the prosecution of a criminal offence.

A reporting person may request a review of a decision to disclose their identity by emailing [whistleblowing@seai.ie](mailto:whistleblowing@seai.ie).

Circumstances may arise where protection of identity is difficult or impossible – e.g. if the nature of the information disclosed means the reporting person is easily identifiable. If this occurs, the risks and potential actions that could be taken to mitigate against them will be outlined and discussed with the reporting person.

Other employees must not attempt to identify reporting persons. Attempts to do so may result in disciplinary action.

If you believe your identity has been disclosed, you have the right to complain in the first instance to a Designated Person.

Records will be kept of all reports, including anonymous reports, in accordance with applicable policies concerning record keeping, data protection and freedom of information as set out further in this policy.

## **12. RELATED POLICIES AND PROCEDURES**

When considering making a report of wrongdoing, a worker should consider its employer's own policies and procedures relating to its staff and whether the report would be more suitably dealt with thereunder, for example grievance, disciplinary, bullying/harassment, anti-fraud, disclosure or other suitable policies or procedures.

## **13. SUPPORTS AND INFORMATION**

Transparency International Ireland operates a free Speak-Up Helpline that offers support and advice (including legal advice) for workers who have reported or plan to report wrongdoing. The helpline can be contacted by Freephone 1800 844 866 (+353 1 554 3965). For more information, see [www.speakup.ie](http://www.speakup.ie).

For workers who are members of a trade union, many unions offer free legal advice services on employment-related matters, including protected disclosures.

SEAI staff have access to the Employee Assistance Programme (EAP). This is a confidential and free service that provides support and assistance for a range of work, health and personal issues. Further information is available on the Intranet or from Human Resources.

Information in relation to making a complaint of penalisation to the Workplace Relations Commission can be found at: <https://www.workplacerelations.ie/en/>

Further information regarding the Act is available from Citizens Information at: <https://www.citizensinformation.ie/en/employment/enforcement-and-redress/protection-for-whistleblowers/>

## **14. DATA PROTECTION**

All personal data will be processed in accordance with applicable data protection law, including the General Data Protection Regulation (GDPR).

It is important to note that section 16B of the Protected Disclosures Act imposes certain restrictions on data subject rights, as allowed under Article 23 of the GDPR.

Where the exercise of a right under GDPR would require the disclosure of information that might identify the reporting person or persons concerned, or prejudice the effective follow up of a report, exercise of that right may be restricted.

Rights may also be restricted to the extent, and as long as, necessary to prevent and address attempts to hinder reporting or to impede, frustrate or slow down follow-up, in particular investigations, or attempts to find out the identity of reporting persons or persons concerned.

If a right under GDPR is restricted, the data subject will be given the reasons for the restriction, unless the giving of such reasons would identify the reporting person or persons concerned, or prejudice the effective follow up of a report, or prejudice the achievement of any important objectives of general public interest as set out in the Act.

A person whose data subject rights are restricted can make a complaint to the Data Protection Commissioner or seek a judicial remedy in respect of the restriction.

## **15. RECORD KEEPING**

A record / log of all reports – including all anonymous reports – will be maintained.

Where a report is made via telephone to the designated telephone number set out at section 4, a recording of the call will be retained.

Records will be retained in line with SEAL's Records Management Policy and Records Retention Schedule.

## **16. FREEDOM OF INFORMATION**

The Freedom of Information Act 2014 does not apply to any records relating to disclosures made in accordance with the Protected Disclosures Act, irrespective of when it was made.

## **17. REVIEW OF THIS POLICY**

This policy will be reviewed biennially

## **APPENDIX A – WHAT TO INCLUDE IN A DISCLOSURE**

Reports should contain at least the following information:

- a. that the report is a protected disclosure and is being made under the procedures set out in this Policy;
- b. the reporting person's name, position in the organisation, place of work and confidential contact details;
- c. the date of the alleged wrongdoing (if known) or the date the alleged wrongdoing commenced or was identified;
- d. whether or not the alleged wrongdoing is still ongoing;
- e. whether the alleged wrongdoing has already been disclosed and if so, to whom, when, and what action was taken;
- f. information in respect of the alleged wrongdoing (what is occurring / has occurred and how) and any supporting information;
- g. the name of any person(s) allegedly involved in the alleged wrongdoing (if any name is known and the worker considers that naming an individual is necessary to report the wrongdoing disclosed); and any other relevant information.

## **APPENDIX B – OTHER DISCLOSURE CHANNELS**

### **B.1 OVERVIEW**

The Protected Disclosures Act sets out a number of alternative external channels for workers to raise concerns. Information regarding these channels is set out below.

Workers should note that different and potentially more onerous conditions may apply when using these channels. Workers are advised to seek professional advice before reporting externally. Information on where to seek independent, confidential advice in this regard can be found at section 13 of this policy.

**The information set out in this Appendix gives a general overview of the other disclosure channels available under the Act. It does not purport to be legal advice or a legal interpretation of the Protected Disclosures Act. It is entirely a matter for each worker to satisfy themselves that they are reporting in accordance with the Act.**

### **B.2 REPORTING TO A PRESCRIBED PERSON**

The conditions applying to reporting to a prescribed person are set out in section 7 of the Protected Disclosures Act.

Prescribed persons are designated by the Minister for Public Expenditure, NDP Delivery and Reform to receive reports of wrongdoing in respect of matters they regulate or supervise.

If a worker wishes to make a report to a prescribed person, in addition to having a reasonable belief that the information they report tends to show a relevant wrongdoing, they must also reasonably believe the information they report is substantially true and that the relevant wrongdoing they wish to report falls within the description of matters for which the person is prescribed.

Prescribed persons are required to have formal channels to receive reports to them under the Act and to acknowledge, follow-up and give feedback on all reports received.

If a worker decides to report to a prescribed person, they must make sure that they choose the right person or body for their issue. For example, if they are reporting a breach of data protection law, they should contact the Data Protection Commission. A full list of prescribed persons and a description of the matter for which they have been prescribed can be found at: [www.gov.ie/prescribed-persons/](http://www.gov.ie/prescribed-persons/).

### **B.3 REPORTING TO THE PROTECTED DISCLOSURES COMMISSIONER**

The conditions applying to reporting to the Protected Disclosures Commissioner are set out in section 7 of the Protected Disclosures Act.

The Protected Disclosures Commissioner is an alternative means by which a worker can make a report under section 7 of the Act. In particular, the Commissioner can assist where the worker is uncertain as to which prescribed person to report to. The Commissioner will transmit the report to the correct prescribed person or to another person the Commissioner considers suitable to follow-up on the report. In exceptional circumstances (e.g. if no prescribed person or suitable person can be found) the Commissioner will follow-up directly on a report.

If a worker wishes to make a report to the Commissioner, in addition to having a reasonable belief that the information they report tends to show a relevant wrongdoing, they must also reasonably believe the information they report, and any allegation contained in it is substantially true.

The Commissioner has established formal channels for workers to make reports under the Act. Information on how to report to the Commissioner is available at: <https://www.opdc.ie/>.

### **B.4 REPORTING TO INSTITUTIONS OF THE EU**

The conditions applying to reporting to institutions of the EU is set out in section 7B of the Act.

If the relevant wrongdoing a worker wishes to report concerns a breach of European Union (EU) law, as set out EU Directive 2019/1937 on the protection of persons who report breaches of Union law, they can report to a relevant institution, body, office or agency of the EU, provided:

- the worker believes the information they wish to report is true at the time of reporting; and
- the information falls within the scope of EU Directive 2019/1937.

A number of these EU institutions have formal channels for receiving reports from workers. A worker wishing to make such a report should contact the institution concerned for information in this regard.



## **B.5 REPORTING TO A MINISTER**

The conditions applying to reporting to a Minister are set out in section 8 of the Protected Disclosures Act.

A worker who is or was employed by a public body can make a report to the Minister or Minister of State responsible for the public body concerned, provided one or more of the following conditions is met:

- the worker has previously made a report of substantially the same information to their employer or other responsible person; or to a prescribed person; or the Protected Disclosures Commissioner; or to a relevant Minister but no feedback has been provided to the worker in response to the report within the specified feedback period, or, where feedback has been provided, the worker reasonably believes that there has been no follow-up or that there has been inadequate follow-up;
- the worker reasonably believes the head of the public body concerned is complicit in the relevant wrongdoing concerned;
- the worker reasonably believes that the relevant wrongdoing concerned may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage.

In the case of SEAI, the relevant Minister is the Minister for Climate, Environment and Communications.

Protected disclosures may be made to the Minister or Minister of State of the Department of the Environment, Climate and Communications, by post marked confidential to:

- Minister / Minister of State for the Department of the Environment, Climate and Communications, 29-31 Adelaide Road, Dublin 2, D02 X285.
- or by email to [ministerprotecteddisclosures@decc.gov.ie](mailto:ministerprotecteddisclosures@decc.gov.ie)
- If a report is made to the Minister, it will within 10 days of receipt, be transmitted, without consideration, directly to the Protected Disclosures Commissioner.

## **B.6 REPORTING TO A LEGAL ADVISER**

The conditions for reporting to a legal adviser are set out in section 9 of the Act.

A worker can disclose information concerning a relevant wrongdoing to a barrister, a solicitor or a trade union official (or an official of an excepted body under section 6 of the Trade Union Act 1941) in the course of obtaining legal advice, including advice in relation to the operation of the Protected Disclosures Act.

## **B.7 REPORTING TO OTHER THIRD PARTIES**

There are specific – and more onerous – conditions that must be met for a worker to be protected if they make a disclosure to any person other than their employer or other responsible person, a prescribed person, the Protected Disclosures Commissioner or a relevant Minister. These are set out in section 10 of the Protected Disclosures Act.

The worker must reasonably believe that the information disclosed in the report, and any allegation contained in it, is substantially true, and that at least one of the following conditions is met:

- the worker previously made a disclosure of substantially the same information to their employer or other responsible person; to a prescribed person; to the Protected Disclosures Commissioner, or to a relevant Minister, but no appropriate action was taken in response to the report within the specified feedback period; or
- the worker reasonably believes that the relevant wrongdoing concerned may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage, or
- the worker reasonably believes that if he or she were to make a report to a prescribed person, the Protected Disclosures Commissioner or a relevant Minister that there is a risk of penalisation, or
- the worker reasonably believes that if he or she were to make a report to a prescribed person, the Protected Disclosures Commissioner or a relevant Minister that there is a low prospect of the relevant wrongdoing being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where a prescribed person may be in collusion with the perpetrator of the wrongdoing or involved in the wrongdoing.

#### **B.8 REPORTING OF MATTERS RELATED TO LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE**

Section 17 of the Protected Disclosures Act sets out certain special conditions that apply to the reporting of matters relating to law enforcement and the administration of justice. A full definition of what constitutes such matters is set out in section 17(1) of the Act.

In general, reports concerning law enforcement, and the administration of justice can only be made:

- To the workers employer in accordance with this policy; or
- To a prescribed person, if a person has been prescribed in respect of the matter the worker wishes to report; or
- To the Comptroller and Auditor General, if the report contains taxpayer information.

A worker can also disclose information concerning a relevant wrongdoing in this area to a legal adviser or a trade union official (or an official of an excepted body under section 6 of the Trade Union Act 1941) in the context of seeking legal advice regarding their disclosure.

A report on matters concerning law enforcement and the administration of justice can in certain circumstances be made to a member of Dáil Éireann or Seanad Éireann. Section 17 sets out the specific conditions that apply in this case. Workers should familiarise themselves with these conditions and seek legal advice if required.

No other form of disclosure of these matters is permitted under the Protected Disclosures Act.

## **B.9 REPORTING OF MATTERS RELATED TO SECURITY, DEFENCE, INTERNATIONAL RELATIONS AND INTELLIGENCE**

Section 18 of the Protected Disclosures Act sets out certain special conditions that apply to the reporting of matters relating to security, defence, international relations and intelligence. A full definition of what constitutes such matters is set out in sections 18(1) and 18(2) of the Act. Reports concerning matters relating to these areas can only be made:

- To the worker's employer, in accordance with this policy;
- To a relevant Minister in accordance with section 8 of the Protected Disclosures Act;
- To the Disclosures Recipient in accordance with section 10 of the Protected Disclosures Act.

A worker can also disclose information concerning a relevant wrongdoing in these areas to a legal adviser or a trade union official (or an official of an excepted body under section 6 of the Trade Union Act 1941) in the context of seeking legal advice regarding their disclosure.

No other form of disclosure of these matters is permitted under the Protected Disclosures Act.

## **Sustainable Energy Authority of Ireland**

### **Disclosures Policy**

#### **SEAI Disclosures Policy**

This SEAI Disclosures Policy is published on [www.seai.ie](http://www.seai.ie) and is distinct from SEAI's Protected Disclosures (Whistle-Blowing) Policy and SEAI's Protected Disclosures (Whistle-Blowing) Procedure (which is contained in SEAI's Code of Governance document on SEAI's website) which provide Workers (as defined therein) with certain statutory protections in relation to particular reports of wrongdoing in a work related context.

#### **About this policy**

The aim of this policy is to encourage individuals who may have concerns about possible improprieties (such as those outlined below), in connection with programmes administered by SEAI or other functions performed by SEAI, to contact SEAI. This invitation applies equally to members of the public, homeowners, beneficiaries, applicants, grantees, nominated project contacts or applicant representatives, project co-ordinators, contractors or any other competent person, BER assessors, special advisors or independent consultants, stakeholders, or anyone otherwise involved in or familiar with a programme delivered by SEAI.

The successful delivery of all programmes managed and administered by SEAI relies upon the honest and reasonable participation of all parties involved.

All registered contractors, installers, BER assessors or any other competent persons, special advisors or independent consultants and any other parties involved in a programme should undertake their duties in a competent, professional and honest manner.

#### **What is a concern / disclosure?**

Examples of concerns that may warrant disclosure include, but are not limited to, suspected instances of:

- Unlawful or improper use of funds, and/or resources of a public body or any other financial malpractice, impropriety or suspected fraud, bribery or corruption;
- Improper conduct or unethical behaviour;
- Failure to comply with or breach of the operating rules and/or guidelines of a programme or any attempt to encourage a breach of same or a breach of the terms of contractor/assessor registration;
- Failure to comply with any legal obligations or statutes;
- Danger to the health and safety of an individual;
- Damage to the environment;
- Criminal activity or the commission or committing of an offence; and
- Attempts to deliberately conceal any of the above matters or attempts to induce others to facilitate such actions.

#### **What happens when a disclosure is made?**

##### **Our actions may include:**

- Consideration of all disclosures which fall within our remit;

- If SEAI deems it to be appropriate, a thorough investigation of the disclosure, to the extent that the information provided/available allows;
- Fully or partially withholding grant payments;
- Imposing sanctions in accordance with our programme rules; and
- Referring a matter to An Garda Síochána in appropriate circumstances.

You will be asked to provide as much detail as possible including the details of names and addresses of all persons and/or properties involved and specifics of the allegations of malpractice or impropriety.

SEAI will consider what steps may be appropriate to take in the circumstances, including whether it is appropriate to investigate any suspected improper conduct. SEAI will provide appropriate training to staff to ensure disclosures of relevant concerns are addressed in accordance with this policy.

The person making the disclosure is not generally a party to the process of reviewing the disclosure. As such, the person making such a disclosure will not generally be briefed on the outcome of SEAI's review, other than in circumstances where it is considered that there is a particular reason to do so.

Note: Where an SEAI worker raises a concern or discloses information regarding potentially relevant wrongdoing within SEAI that has come to their attention through their work, they may refer to the SEAI Protected Disclosures (Whistle-blowing) Policy and associated Procedure for further guidance. For the purposes of the SEAI Protected Disclosures (Whistle-blowing) Policy and associated SEAI Protected Disclosures (Whistle-Blowing) Procedure, "workers" include employees, officers, consultants, independent contractors, interns, trainees, casual workers, agency workers, members of administrative, management or supervisory bodies of SEAI, shareholders, job applicants, individuals who acquire information during pre-contractual negotiations (other than those associated with recruitment) and volunteers.

This Disclosures Policy does not apply to SEAI investigations of complaints or appeals. A complaint is regarded as a written expression of dissatisfaction about SEAI or any third party acting on SEAI's behalf. An appeal is regarded as a request for review of a decision under any SEAI grant programme. If you have a complaint or appeal, please refer to the SEAI Customer Charter for the SEAI Feedback, Complaints and Appeals Policy (published on [www.seai.ie](http://www.seai.ie)).

### **Raising a concern**

If you wish to raise a concern relevant to this Policy, please contact SEAI directly by:

- writing to us at Disclosures, SEAI, 3 Park Place, Hatch Street Upper, Dublin 2;
- calling us at 01 8082100; or
- emailing us at [disclosures@seai.ie](mailto:disclosures@seai.ie)

A concern may be received as a disclosure under this Disclosures Policy or in another way, for example, a relevant concern about possible improprieties (such as those outlined above) may be raised by an individual by contacting their usual contact within SEAI. If appropriate, this will be dealt with as a disclosure under this Disclosures Policy.

SEAI recognises that the decision to report a concern about suspected instances of impropriety (such as those outlined above) may be difficult. SEAI will make all reasonable efforts to treat concerns raised as confidentially as possible, including to keep the identity of a disclosing individual confidential, however, this needs to be commensurate with a fair investigation (should SEAI deem it appropriate to investigate the disclosure).

## **The process**

1. To facilitate tracking, when a relevant concern is received outside of the channels outlined in this Disclosures Policy, staff members are requested to forward such correspondence or send details of a concern raised with them to [disclosures@seai.ie](mailto:disclosures@seai.ie);
2. Details of the disclosure or concern are reviewed by the Information Compliance Officer who will acknowledge receipt of the concern and assign it to the appropriate team within SEAI for investigation, if SEAI deems it to be appropriate, in accordance with their normal procedures;
3. The actions taken by SEAI will be appropriate to the circumstances. However, SEAI will endeavour to ensure that the following steps are followed and documented in a file in any investigation by SEAI:
  - Establish credibility of the concern;
  - Identify specifically the conduct that is allegedly or actually contrary to law, SEAI's rules or terms and conditions or any applicable code of practice or regulation or any other binding rules;
  - If the concern is credible and improper conduct is identified, consider whether it is appropriate to seek a response on same from the third party in question<sup>[1]</sup>; and
  - SEAI will consider the third party's response, if any, together with the file of information collated, and determine the appropriateness of imposing sanctions or penalties on the third party or reporting the matter to the appropriate enforcement agency.

## **SEAI Register of Disclosures**

Disclosures and concerns are tracked on the SEAI Register of Disclosures, which will be maintained by the Information Compliance Officer.

## **SEAI Records relating to Disclosures**

The Information Compliance team will create a folder and provide access to the appropriate team within SEAI if such team is assigned to investigate the disclosure. The investigating team will keep a copy of all records relevant to their investigation in this folder.

## **Internal Access to SEAI Records relating to Disclosures**

Access to disclosure folder(s) will be managed by the Information Compliance Officer. Except for as outlined above, access shall only be provided upon receipt of a written access request from a member of SEAI's Senior Management Team. Members of SEAI's Senior Management Team will only request access where there are justifiable grounds for that request.

SEAI reserves the right to withdraw or amend this Disclosures Policy at any time.

<sup>[1]</sup> In circumstances of suspected criminal activity or where obliged by law or otherwise to do so, SEAI may decide that it is not appropriate to seek a response from the third party in question and report the matter directly to An Garda Síochána and/or other regulatory bodies.

## Appendix 11 – SEAI Anti-Fraud, Bribery & Corruption Policy

(Approved by the Board on 11 December 2024)

### ***Sustainable Energy Authority of Ireland Anti-Fraud, Bribery & Corruption Policy***

<b>Document Reference</b>	Anti-Fraud, Bribery & Corruption Policy
<b>Document Status</b>	Approved by Board
<b>Document Version</b>	3
<b>Approval Date</b>	11/12/2024
<b>Document Owner</b>	Chief Risk Officer
<b>Document Type</b>	Policy

## ***Table of Contents***

1. INTRODUCTION.....	3
2. POLICY .....	3
3. SCOPE.....	3
4. DEFINITION OF FRAUD, BRIBERY & CORRUPTION.....	3
5. RISK FACTORS.....	4
6. SEAI RESPONSIBILITIES .....	4
7. BOARD RESPONSIBILITIES .....	5
8. SENIOR MANAGEMENT TEAM RESPONSIBILITIES .....	5
9. EMPLOYEE RESPONSIBILITIES .....	5
10. INTERNAL AUDIT RESPONSIBILITIES .....	6
11. HR RESPONSIBILITIES .....	7
12. REPORTING AND INVESTIGATION .....	7
13. IMPLICATIONS OF NON-COMPLIANCE WITH THIS POLICY .....	7
14. DO'S AND DON'TS .....	8
15. DOCUMENT CONTROL .....	8
Appendix 1 .....	10



## **1. INTRODUCTION**

SEAI is committed to the prevention of fraud, bribery and corruption and to the promotion of an anti- fraud, anti-bribery and anti-corruption culture. SEAI aims to manage and control operations, processes, projects and systems in such a way that the risk of fraud, bribery and corruption is minimised. It is committed to investigating thoroughly all cases of suspected fraud, corruption and related offences and to recover any money and /or property, including intellectual property, lost through fraud, bribery or corruption. SEAI will also, when necessary, pursue prosecution through the Courts.

## **2. POLICY**

It is the policy of SEAI to adopt best practice corporate governance based on openness, transparency and accountability; effective anti-fraud, bribery and corruption controls based upon risk management reviews; and regular monitoring of activities and functions. SEAI believes this creates the right culture and environment to prevent and deter fraud, bribery or corruption.

The purpose of this document is to set out key responsibilities with regard to fraud, bribery and corruption prevention and detection, what to do if fraud, corruption, bribery and related offences are suspected and the action that will be taken where these offences have been reported.

This policy is one of a suite of related policies, including the Protected Disclosures (Whistle-blowing) Policy, Disclosures Policy, Code of Conduct, Corporate Gifts Policy and Delegated Authority Framework (the "Policies").

Disciplinary action, up to and including suspension and dismissal, will be taken against staff members involved in fraud, bribery or corruption and related offences and action may also be taken against staff members whose negligence, through lack of supervision and control or otherwise, or other actions may have facilitated the event. Fraud, bribery or corruption are offences which carry criminal sanctions if successfully prosecuted. It is SEAI's policy to co-operate with criminal investigations where requested to do so.

## **3. SCOPE**

The Anti-Fraud, Bribery and Corruption Policy applies to any fraud, or suspected fraud, bribery, corruption, or suspected corruption involving employees, agency/contract workers, Board Members or Board Committee Members.

## **4. DEFINITION OF FRAUD, BRIBERY & CORRUPTION**

### **FRAUD**

Fraud generally means deceitful misrepresentation of facts to commit or conceal a crime. It may be defined as "the theft, misappropriation or unauthorised use of SEAI time, funds, property or other assets, which may or may not also involve misstatement of financial documents or records to conceal the theft or misuse". It usually involves the obtaining of money or services to which a person is not entitled. False and/or forged documents are often used in these types of activities.

Fraud could be carried out by an individual or a group of individuals colluding with each other either within or outside of SEAI.

#### **BRIBERY**

Bribery is offering, promising, giving, accepting or agreeing to accept any financial or other advantage to someone in business or government in order to obtain or retain a commercial advantage, or to influence another person to act improperly in carrying out their duties or to reward another person for acting improperly. Bribery also includes “facilitation payments” (see below).

An advantage includes money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or anything else of value.

A bribe whether offered or received is a corrupt payment. Bribes are often monetary in nature but can also take the form of other benefits or advantage. Bribes include but are not limited to the inappropriate provision of:

- monetary benefits or use of services;
- gifts or hospitality that are disproportionate, secretive, frequent or given during business negotiations or tender processes with the intention or perceived intention of influencing the outcome of negotiations and/or tenders and are not reasonable and bona fide;
- product discounts or credits that are disproportionate and not readily available to other customers;
- non-bona fide employment or investment opportunities.

Bribery can also exist where the payment is offered/given by or through a third-party agent or representative.

Facilitation Payments – typically small, unofficial, undocumented payments made to secure or expedite a routine governmental action by a government official. Facilitation payments are not permitted.

#### **CORRUPTION**

Corruption can be broadly defined as the abuse of entrusted power for private gain. Corrupt activity can be engaged in by private individuals, public officials and businesses. Corruption (or acting corruptly) includes acting with an improper purpose personally or by influencing another person, whether by means of making a false or misleading statement, by means of withholding, concealing, altering or destroying a document or other information, or by any other means. Corruption can take many forms including conflicts of interest, undue influence and the giving and taking of bribes.

## **5. RISK FACTORS**

Particular care should be taken where:

- there are any close family, personal or business ties that a third party or partner has with officials;
- a request has been made for a cash payment;
- an unusual payment arrangement has been requested such as a payment to be made in a third country or to a third party;
- a request has been made to pay an expense which is unusual or vague;
- invoices are disproportionate or non-standard;

- there is evidence of overriding controls;
- there are 'cosy' relationships with suppliers, customers or partners;
- key documents are missing (e.g invoices, contracts); documentation is lacking essential information, missing official records;
- there is unusual employee behaviour;
- a request has been made for a payment or an advantage in relation to a service which does not attract a fee.

## **6. SEAI RESPONSIBILITIES**

The board of SEAI, and its subcommittee the Audit and Risk Committee are responsible for oversight of the Anti-Fraud, Bribery and Corruption policy. The role of management is to develop and monitor a risk management framework in the organisation to reduce the likelihood of fraud, corruption and related offences and to ensure that the policy is effective. It is the responsibility of SEAI to:

- Ensure that it is operating an effective system of governance and internal control;
- Ensure it has suitable policies, procedures and controls in place to safeguard itself against fraud, bribery and corruption;
- Ensure that it clearly communicates its policy on fraud, bribery and corruption to all staff members;
- Ensure that this policy is publicly available on [www.seai.ie](http://www.seai.ie);
- Ensure appropriate segregation of duties across SEAI and delegated approval authority across a range of personnel;
- Promote a culture of transparency including the application of procedures in accordance with the Protected Disclosures Policy for those reporting allegations of fraud or corruption;
- Ensure that appropriate management resources and structures are in place across SEAI to detect any incidence of fraud or corruption;
- Ensure that an annual report on fraud, bribery and corruption is prepared for the consideration of the Audit and Risk Committee and the Board;
- Carry out investigations if fraud, bribery, or corruption is suspected;
- Ensure fair treatment of all personnel who become the subject of a fraud, bribery, or corruption allegation;
- Take appropriate legal and/or disciplinary action against perpetrators of fraud, bribery, or corruption; and
- Take appropriate action against staff members where their failures have contributed to the commissioning of fraud, bribery or corruption.
- Treat suspicions or allegations of potential fraud, bribery or corruption as confidential to the extent possible in accordance with the Policies, in particular the Protected Disclosures Policy, or as required by law or until such time as the information comes into the public domain.

The Chief Executive Officer of SEAI carries overall responsibility for the prevention of fraud, bribery and corruption.

## **7. BOARD RESPONSIBILITIES**

It is the responsibility of the Board of SEAI to ensure that an appropriate Anti-Fraud, Bribery & Corruption Policy is in place and with the support of the Audit and Risk Committee, to monitor its implementation through periodic reports from the executive. Board Members have a responsibility also to ensure they adhere to the provisions of this policy.

## **8. SENIOR MANAGEMENT TEAM RESPONSIBILITIES**

The Senior Management Team is responsible for overseeing and embedding appropriate operational procedures and controls to prevent and detect any improper activity and to be familiar with the types of fraud, bribery or corruption that might occur in their area of responsibility. This includes:

- Identifying the risks to which systems, operations and procedures are exposed;
- Developing and maintaining effective controls to prevent and detect fraud, bribery and corruption;
- Ensuring that controls are being complied with;
- Providing induction and regular training for staff members involved in internal control systems to ensure that their responsibilities are regularly highlighted and reinforced;
- Ensuring persons reporting to them are made aware of and understand this policy;
- Ensuring the rotation of staff members where possible and appropriate / necessary;
- Reporting all incidents and any suspected cases of, bribery, corruption or fraud in accordance with reporting procedures.

On an annual basis, each Head of Department will be asked to confirm that they have taken steps to ensure staff are aware of this policy and appropriate controls have been implemented.

## **9. EMPLOYEE RESPONSIBILITIES**

It is the responsibility of members of staff to be familiar with the types of fraud, bribery or corruption that might occur in their area of responsibility and to be alert for any indication of suspected or actual improper activity, misappropriation, or dishonest activity that is or was in existence, and to put in place controls to prevent such occurrences.

Every employee has a responsibility to:

- Read and be familiar with the contents of this policy and other applicable policies, including the Policies;
- Be alert to the possibility of bribery, corruption or fraud and take special care where unusual events or transactions occur;
- To report any suspected cases of fraud, bribery or corruption to your line manager and/or in line with SEAI's Protected Disclosures (Whistle-blowing) Policy;
- Ensure that public funds/assets entrusted to them are safeguarded;
- Comply with the Code of Business Conduct for Staff Members as set from time to time by SEAI;
- Inform the Human Resources Department and respective Head of Department in writing of gifts or hospitality which may give the appearance of a past, present or future conflict of interest and ensure they are in line with the SEAI Corporate Gifts Policy;
- Inform the Head of Department in writing of any outside interests that may conflict or impinge on their duties;
- Alert the Head of Department in writing to perceived weaknesses in the control system or in any SEAI system;
- Co-operate fully with any internal checks, reviews or investigation of suspected instances of bribery, corruption or fraud;
- Assist in any investigation that may arise in respect of fraud, bribery corruption or associated offences.

Every employee must not:

- Offer, give, promise, provide, solicit, request, accept or agree to receive anything of value, whether cash or in any other form (directly or indirectly), intentionally or otherwise to or

from any person or entity wherever located for the purpose of:

- Gaining any commercial, contractual, or regulatory advantage for SEAI in any way which is unfair or unethical.
- Gaining (or engaging in conduct that could be viewed as gaining) any personal advantage, pecuniary or otherwise, for you or anyone in which you have a relationship or close links with.
- Improperly offer, promise or transfer anything of value (directly or indirectly) to a public official wherever located in order to:
  - Influence the public official in the exercise of their public functions.
  - Obtain or retain business for SEAI.
  - Secure advantage for SEAI, its employees or any other entity, person, including anyone with whom you have a relationship or close links.

Please refer to the Employee Handbook for full details of employee obligations.

Employees should be aware that their rights as whistleblowers are protected under the Protected Disclosures Act 2014 and the Protected Disclosures (Amendment) Act 2022. Please refer to the SEAI Protected Disclosures (Whistle-blowing) Policy as set out in Appendix 10 of the SEAI Code of Conduct and as available on the HR Department SharePoint site and on the SEAI website.

## **10. INTERNAL AUDIT RESPONSIBILITIES**

Internal audit provides reasonable assurance to SEAI management that the organisation's significant risks are being appropriately managed with an emphasis on internal controls and governance processes. SEAI's Internal Audit function is outsourced however it is supported by an internal Audit & Risk team. The following processes are managed by the Internal Audit teams cooperatively:

- Promoting procedure manuals which identify controls which should be in place;
- Providing clear recommendations where control weaknesses have been identified;
- Ensuring risk management and systems of controls are continually being monitored by departments in response to a constantly changing environment;
- Ensuring audit work takes account of the possibility of fraud, bribery, corruption and related offences.
- Assisting in fraud, bribery, corruption and related offences investigations as and when is required.

The audits undertaken by Internal Audit will be prioritised to reflect the levels of potential risks to the organisation and the frequency of reviews will be dependent on resources available to the audit unit. An annual internal audit is carried out on internal financial controls to support the Board's Statement of Internal Financial Control.

## **11. HR RESPONSIBILITIES**

A key preventative measure to deter fraud, bribery and corruption is to take effective steps at the recruitment stage to establish, insofar as possible, the previous record of potential new employees. Human Resources responsibilities are as follows:

- Ensure references of all new resources have been secured and are satisfactory;
- To request confirmation from line manager of satisfactory completion of probationary periods for their staff;
- To issue appropriate rules of conduct on appointment;

- To ensure employment policies, including those regarding fraud, bribery, corruption, and related offences are included in induction programmes for staff members at all levels;
- To monitor turnover and leave patterns of staff members;
- To provide updates on an annual basis on this and other relevant employment policies.

## 12. REPORTING AND INVESTIGATION

All reports of fraud, bribery and corruption must be taken seriously. The following plans must be enacted to allow for decisive action should an incident of actual or suspected fraud/bribery/corruption come to light:-

**Where the report is internal to SEAI and relates to fraud, bribery or corruption within SEAI:**

- Staff members shall report any case of actual or suspected fraud, bribery, corruption or related offences, or irregularities to their line manager and/or in line with the SEAI Protected Disclosures (Whistle-blowing) Policy and associated Procedure.
- It is imperative that SEAI resources act quickly to minimise any losses and to increase the chances of a successful investigation (the first 24-48 hours are critical in this respect). The investigation will be carried out, professionally and fairly but bearing in mind that it is only an allegation until the outcome of investigation is known.
- The staff member making the report should be aware that SEAI will use all reasonable endeavours to keep their identity confidential, but that in the interests of fair procedure and natural justice, the release of their identity may be required to properly investigate the allegation.
- Evidence must be preserved and moved to a secure location where practicable. Documentary evidence must be preserved in its original state and no additions or notes made thereon. Hard copy documents should be placed in a clear plastic envelope and labelled noting where it was stored and under whose control. It should also be recorded on the label the time and date any such document was passed to another person and their identity. Soft copy documents should be stored in a secure location with restricted access. Documents should not be deleted or destroyed.

## 13. IMPLICATIONS OF NON-COMPLIANCE WITH THIS POLICY

Actions of bribery, corruption and fraud are subject to criminal sanction and there are serious penalties for anyone found guilty of breaching the law in this area including fines and/or imprisonment. SEAI may be required to report incidents or suspected incidents of bribery, corruption or fraud to An Garda Síochána or other regulatory authorities. Breaches of this policy by staff can result in the organisation taking disciplinary action up to and including dismissal.

## 14. DO'S AND DON'TS

DO ...	
... report your suspicions or any disclosures promptly	Report any suspected cases of fraud, bribery, corruption or related offences to your line manager and/or in line with SEAI's Protected Disclosures (Whistle-blowing) Policy;

<b>... retain any evidence you may have</b>	The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation.
<b>DON'T</b>	
<b>... approach the person you suspect or try to investigate the matter yourself</b>	There are special rules relating to the gathering of evidence for use in investigations. Any attempt to gather evidence by persons who are unfamiliar with these rules may compromise the investigation.
<b>... be afraid of raising your concerns</b>	The law provides protection for staff that raise reasonably held concerns about irregularities in their workplace through the appropriate channels.
<b>... convey your concerns to anyone other than authorised persons</b>	There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons. Where the case is well founded, information shared could prejudice or compromise investigations. Vexatious claims will be dealt with under SEAL's grievance policy or otherwise.

## 15. DOCUMENT CONTROL

The Anti-Fraud, Bribery and Corruption Policy will come into effect immediately upon approval by the Audit and Risk Committee and the Board and will be reviewed biennially.

## Appendix 1

**Further guidance on matters which may constitute acts of fraud, bribery or corruption.**  
**Please note the examples provided are not exhaustive.**

### FRAUD

Fraud occurs in a variety of ways. Typically, fraud can include (but is not limited to):

- Banking and credit-card fraud;
- Bogus, invalid and unsolicited invoices paid by an organisation;
- Theft, misappropriation or unauthorised use of SEAI time, funds, property or other assets;
- Paying of excessive prices or fees to third parties with the aim of personal gain;
- Advanced fee fraud where fees are paid before work is satisfactorily completed;
- Where works being claimed for have not been carried out at all;
- Collusion with SEAI contractors, suppliers or other third parties to falsify records
- Deliberate misrepresentation of identification and/ or qualifications;
- Fictitious applications for grants;
- Knowingly submitting fraudulent or duplicate receipts or falsifying an expense report;
- Forgery or alteration of documents;
- Destruction or removal of records;
- Accepting or offering kickbacks or bribes for preferential treatment, for example in the supplier selection or work allocation process;
- Using or disclosing commercial or customer-related data without appropriate authorisation. This includes disclosing confidential information to external parties;
- Employees seeking or accepting cash, gifts or other benefits from third parties in exchange for preferment of the third parties in their dealings with the Authority;
- Any corrupt activities e.g., bribery;
- Cyber fraud or cybercrime.

Fraud can also take the form of computer fraud. This is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud.

### BRIBERY AND CORRUPTION

Some common bribery and corruption indicators are:

- Giving or receiving any gift and/or hospitality which is not reasonable, not proportionate and not justifiable and where the intention of giving or receiving the gift and/or hospitality is to influence a person corruptly or improperly in the exercise of their duty
- Giving or receiving gifts and/or hospitality immediately prior to, during or immediately after your involvement in a tender or contracting/negotiation process.
- Giving or receiving any gift, benefit, entertainment or other personal favour or assistance which goes beyond accepted industry practice.
- A third party insists on receiving a commission or fee payment before committing to sign up to a contract with us or carrying out a government function or process with us.
- A third-party requests payment in cash and/or refuses to sign a fee agreement, or to provide an invoice or receipt for a payment made.
- A third-party request that payment is made to a country or geographic location



different from where the third party resides or conducts business where we suspect those places are a tax haven or where those places have a reputation for money laundering.

- A third party requests an unexpected additional fee or commission to “facilitate” a service
- A third party demands entertainment or gifts before commencing or continuing contractual negotiations or provision of services.
- We become aware that a third party engages in, or has been accused of engaging in, improper business practices.
- We learn that a third party has a reputation for paying bribes, or requiring that bribes are paid to them.
- A third-party request that a payment is made to “overlook” potential legal violations.
- A third-party request that you provide employment or some other advantage to a friend or relative
- We receive an invoice from a third party that appears to be non-standard or customised.
- A third-party refuses to put terms agreed in writing.
- We are offered an unusually generous gift or offered lavish hospitality by a third party not in accordance with our industry standards and/or general commercial practice.

Context is important when identifying whether an incident constitutes bribery, corruption or fraud. In terms of gifts and hospitality, the test to be applied is whether in all the circumstances the gift or hospitality is reasonable, proportionate and justifiable. It can never be given with the intention of influencing, inducing or rewarding improper performance. Further guidance regarding gifts, hospitality and expenses is set out in the Corporate Gifts Policy.

## Appendix 2 Controls

**Further guidance on the types of controls to implement and maintain to prevent, deter and detect fraud, bribery, corruption and related offences. Please note the examples provided are not exhaustive.**

- Ensuring that appropriate segregation of duties are in place so that all work is organised in such a way that no one individual has responsibility for all aspects of a process. For example, there is segregation of employees responsible for checking eligibility and recommending payments from those responsible for authorising and making payments.
- Authorised signatory lists for payments.
- Authorisation approval limits for staff members.
- Ensuring that Procedures Manuals are in place and updated regularly.
- Systems of review (e.g. certification checks, verification checks, internal audit, risk assessment and management).
- Periodic internal audits take place in relation to fraud prevention and detection.
- Ensuring that appropriate due diligence is undertaken of suppliers.
- Carrying out HR vetting of staff.
- Ensuring that grants awarded for works are inspected in accordance with the grant scheme rules.
- Provide appropriate fraud, bribery and corruption awareness training.
- Regular financial review and reporting of financial position up the management chain.
- Regular review by senior management that the systems of control are adequate and effective.
- Applying relevant external (e.g., Department of Finance, EU Regulation) and internal guidelines and procedures.
- Proper, efficient and prompt collection, receipt, and accounting for and monitoring of monies.
- Checks to ensure SEAI is complying with its legislative requirements within its statutory remit.
- When systems and/or procedures for SEAI are being designed, managed and used, fraud, bribery and corruption prevention must be taken into consideration. All systems should be designed not just to meet the requirements of legislation, be it national or European, but also to include checks and controls which prevent fraud, bribery and corruption.

Appendix 12 - Business Continuity Policy

Business Continuity Policy

(Approved by the Board 11 December 2024)

Document Reference	Business Continuity Policy
Document Status	Approved by Board
Document Version	3.1
Approval Date	11/12/2024
Document Owner	Risk Manager
Document Type	Management Policy

Distribution:  
This document does not have restricted access and is available to staff and interested parties as required.

## Table of Contents

<b>Business Continuity Policy Statement .....</b>	<b>3</b>
<b>1.0 Introduction .....</b>	<b>4</b>
<b>1.1 Objective .....</b>	<b>4</b>
<b>1.2 Ownership &amp; Review .....</b>	<b>4</b>
<b>1.3 Context and Scope .....</b>	<b>4</b>
<b>1.4 Documents and Records .....</b>	<b>5</b>
<b>2.0 Governance and Responsibilities .....</b>	<b>5</b>
<b>3.0 SEAI Business Continuity Management Framework.....</b>	<b>6</b>
<b>3.1 Policy &amp; Programme Management .....</b>	<b>6</b>
<b>3.2 Analysis.....</b>	<b>7</b>
<b>3.3 Design (Recovery Solutions) .....</b>	<b>7</b>
<b>3.4 Implementation (Response Planning).....</b>	<b>8</b>
<b>3.5 Validation (Testing and Review) .....</b>	<b>8</b>
<b>3.6 Embedding Business Continuity .....</b>	<b>9</b>
<b>Appendix 1: Terms and Definitions .....</b>	<b>10</b>
<b>Document Control.....</b>	<b>13</b>



## **Business Continuity Policy Statement**

The mission of the Sustainable Energy Authority of Ireland (SEAI) is to play a leading role in transforming Ireland into a society based on sustainable energy structures, technologies and practices. Our key objectives are implementing strong energy efficiency actions, accelerating the development and adoption of technologies to exploit renewable energy sources, supporting innovation and enterprise for our low-carbon future and supporting evidence-based response that engage all actors.

We are committed to maintaining a high level of service to our stakeholders including the citizen, clients, service partners, employees, suppliers, regulators, government departments and policy-makers during periods of disruption. We aim to react effectively to disruptive incidents and protect our employees, core business assets and ensure the continuity of SEAI's quality service to our clients to the extent possible in the circumstances.

SEAI has developed its Business Continuity Management System aligned to International Standard ISO22301:2019 (Security and Resilience – Business continuity management systems – Requirements)). The SEAI Business Continuity Policy provides the framework within which stakeholder commitments, expectations and needs will be determined and on how business continuity is implemented and maintained across the organisation. Each programme and function will maintain their business continuity capabilities and plans reflecting their ongoing business requirements, including legal and regulatory requirements, while operating within the framework presented in this policy. The Policy encompasses business supporting processes including Health & Safety, IT Systems, Security & Service Continuity, Risk Management and complies with all other obligations to that we may subscribe.

Business continuity objectives will be established annually and will be approved by the Director of Corporate Services. These objectives will form the basis of the business continuity programme, to deliver continuous improvement in performance and to enhance organisational resilience.

All SEAI staff are collectively responsible for embedding business continuity principles in processes and for exercising Business Continuity Plans when appropriate. This Policy will be communicated within the organisation and will be available to interested parties.

Signature

Chief Executive Officer

## **1.0 Introduction**

### **1.0 Objective**

The purpose of the SEAI Business Continuity Policy (the Policy) is to provide a clear statement of SEAI's commitment to business continuity and a framework for its Business Continuity Management System ('BCMS'). The purpose of SEAI's BCMS is to facilitate the protection of SEAI's priority services in the event of serious disruption from adverse circumstances/emergencies or other constraints that may be placed on the business operations.

The objectives of the Policy are as follows:

- To provide the context for and scope of SEAI's BCMS
- To outline the SEAI Business Continuity and Crisis Management frameworks
- To detail the Governance structure including roles, responsibilities and management oversight

### **1.1 Ownership & Review**

The Policy is managed by the Business Continuity Manager, implemented by the Senior Leadership Team (SLT) and approved by the Audit and Risk Committee.

The Policy will be reviewed biennially or following significant organisational changes (such as a fundamental change to services, operating model or legal or regulatory requirements). All relevant personnel will be informed of changes through policy updates.

### **1.2 Context and Scope**

SEAI has developed its Business Continuity Management System aligned to International Standard ISO22301:2019 (Security and Resilience – Business continuity management systems – Requirements)). The SEAI Business Continuity Policy provides the framework within which stakeholder commitments, expectations and needs will be determined and how business continuity is implemented and maintained across the organisation. Each programme and function will maintain their business continuity capabilities and plans reflecting their ongoing business requirements, including legal and regulatory requirements, while operating within the framework presented in this policy. The Policy encompasses business supporting processes including Health & Safety, IT Systems, Security & Service Continuity, Risk Management and complies with all other obligations to that we may subscribe.

The Policy applies to all SEAI locations, staff, business programmes, functions and business process outsource (BPO) dependencies, with a prioritised focus on time-critical business continuity. The organisational scope is outlined in the SEAI Services Chart set out in the BCP Procedure.

All incidents that have a significant impact on SEAI's ability to maintain its critical or important functions and activities and / or any incidents that immediately threaten our core business assets (including personnel, facilities, IT, data, reputation and brand) can be considered a business continuity related incident. The nature of business disruption addressed by the Policy is restricted to operational capability including activities such as facilities, personnel, IT and suppliers as well as sudden and unexpected emerging situations that require a rapid response to contain (e.g. regulatory breach, reputational damage, industrial relations, cyber-attack, internal sabotage).

The basis on which our business continuity plans expect to be able to contain disruption is limited to credible worst-case scenarios involving the loss of a location, utilities, personnel, IT, data and/or key supplier(s). Our response plans focus on the early continuity stages following an incident and the long-term recovery to pre- incident levels is not detailed.

### **1.3 Documents and Records**

The Business Continuity Management System (BCMS) includes the following main documents:

- I. Business Continuity Policy
- II. Crisis Management Plan
- III. Business Impact Analysis Management Report
- IV. Services (Department) Response Plans
  - Priority Service Impact Assessment
  - Services Business Impact Analysis
- V. BCMS Operating Procedure – SEAI Services Chart
- VI. Business Continuity Exercise Programme

All records (including forms, templates, test reports, management reviews and action plans) created for the implementation and maintenance of the BCMS will be retained for at least three years. The Business Continuity Manager is responsible for the maintenance of the documentation system.

The Policy will be available to staff via the SEAI Intranet and provided to interested parties as required.

## **2.0 Governance and Responsibilities**

SEAI is committed to maintaining an acceptable level of service to its stakeholders including clients, partners, employees, suppliers, regulators, government departments and policymakers. It takes reasonable steps to ensure continuity in the performance of priority activities and employs appropriate and proportionate systems, resources and procedures to ensure same.

The Policy is reviewed biennially, ensuring alignment with risk appetite and other relevant risk management policies. Policy revisions are submitted to the Audit and Risk Committee for approval and notified to the Board. The CEO is accountable for the BCMS and for ensuring that effective continuity arrangements are in place. The Director of Corporate Services, supported by the Business Continuity Manager, is responsible for setting, overseeing, and reporting on the achievement of business continuity objectives. The Senior Management Team is responsible for ensuring that BCMS requirements are integrated into business processes. The Executive Leadership team, supported by the Senior Management Team and Business Continuity Manager, is responsible for leading crisis management response.

## 2.0 SEAI Business Continuity Management Framework

SEAI has adopted the principles outlined in ISO22301:2019 (Security and Resilience – Business continuity management systems – Requirements) and the Business Continuity Institute (BCI) Good Practice Guidelines 2018 as the framework for how business continuity is applied across the organisation. They are illustrated in Figure 1 below.

**Figure 1: Business Continuity Management Framework (Ref: BCI Good Practice Guidelines 2018)**



The framework of the Business Continuity Management System has six key elements;

- **Policy & Programme Management;** governance, performance management and BCMS project implementation
- **Analysis;** understanding the organisation's business, i.e. defining the time-critical programmes and functions of the organisation, recovery timeline, minimum resource requirements, IT service alignment and risk assessment
- **Design;** development of the recovery strategies and the incident / crisis management structure
- **Implementation;** plan development and documentation including crisis management, business continuity and IT Disaster Recovery plans
- **Validation;** BCMS operating and maintenance procedure, exercise and testing and ongoing review activities
- **Embedding Business Continuity;** awareness, training, integrating business continuity into day-to-day processes and culture

The minimum requirements for how business continuity should be applied across the organization is detailed in this section of the Policy.



### **3.1 Policy & Programme Management:**

Appropriate and proportionate contingency planning will be applied depending on the nature and criticality of the service provided. At a minimum, all priority programmes and functions must have documented response plans, which are up to date and subject to periodic exercise/test.

The development of new Programmes or where implementing major change to existing programmes will incorporate business continuity planning and/or review.

The Director of Corporate Services and Business Continuity Manager will review effectiveness of the BCMS annually. Annual objectives will be set for the BCMS by the Business Continuity Manager and approved by the Director of Corporate Services. Performance indicators will be defined, and targets established as required. The BCMS implementation, maintenance and improvement plan will be managed and controlled by the Business Continuity Manager. An annual programme of activities with assigned responsibilities will be defined for the BCMS and included in an operational procedure.

### **3.2 Analysis:**

#### *Business Impact Analysis (BIA)*

Time-critical programmes and functions are identified through assessing the impact of disruption over time on the business if the service is not available. Each programme / function determines (qualitatively) the potential financial, legal, and reputational and other consequences if the service is unavailable and identify the maximum acceptable downtime (Maximum Tolerable Period of Disruption) for the service. The output will be reviewed annually.

The processes, activities and resources required to support and deliver the time-critical services are determined by the departmental BIA analysis and are captured in the Department Response Plans using the SEAI pre-defined methodology. The analysis captures the recovery period and minimum resources required to deliver an acceptable service. In addition, critical suppliers and service providers are identified.

BIA's are reviewed and amended where necessary but at least annually or sooner if there is a major service development. The Business Continuity Manager coordinates BIA activity across the organisation to ensure a consistent and acceptable standard of analysis.

Close alignment is maintained between IT DR capabilities and business application requirements. An input into this process is the IT Risk Management Framework which is reviewed on a quarterly basis.

#### *Business Continuity Risk Assessment*

Through the *SEAI Risk Management Framework*, each programme / function identifies plausible disruption scenarios that may lead to short, medium and long-term disruptions to critical business functions and assesses the likelihood of these scenarios occurring. Risk mitigation actions are identified, assessed and implemented where necessary.

### **3.3 Design (Recovery Solutions):**

Practical and cost-effective recovery solutions are required to address facility, personnel, IT, BPO and other critical supplier disruption. Key programmes and functions consider recovery solutions based on the needs of the business and on the results of the BIA. These solutions are appropriate and proportionate and are subjected to cost/benefit analysis where necessary. The Executive Leadership Team (ELT) is responsible for ensuring that resources and budgetary provision is proportionate for implementation of the SEAI BCMS objectives. Any associated risk as a consequence of inadequacy is captured on the Risk Register. SEAI

vendor management process will require a periodic assessment of business continuity planning within BPO and other critical suppliers having impact on SEAI resilience.

### **3.4 Implementation (Response Planning):**

#### *Business Continuity Planning*

Priority programmes / functions within each department maintain at all times a written Service (Department) Response Plan (DRP). The DRP refers to the documented procedures and information that enable the functions to respond to a disruption, recover and resume critical business functions and return to a minimum level of service in an orderly fashion.

An 'all-hazards' methodology is applied to business continuity response planning at SEAI. The focus of the DRP is on the early continuity stages following an incident. The long-term recovery to pre-incident levels is not detailed.

Each department has ownership of their respective DRP and appoints a plan owner who is responsible for reviewing, amending and updating the plan at least annually.

#### *IT Disaster Recovery Planning*

The SEAI IT function maintains an IT Disaster Recovery Plan supported by detailed system recovery procedures as required.

#### *Crisis Management Planning*

A written account of how to deal with a serious incident (crisis), called the SEAI Crisis Management Plan (CMP), is maintained and tested at regular intervals in a simulated environment to ensure that it can be implemented in emergency situations. The Crisis Management Team (CMT), made up of representatives of the ELT with additional support personnel such as IT, Legal, Human Resources, Corporate Communications and Service Functions as required, directs the business during a crisis.

Managers and key employees with designated responsibilities in terms of the CMP keep off-site copies of the plan to be readily available in the event of an incident. The CMP and copies of department response plans will be held in hardcopy, securely, in appropriate locations.

Additionally, as SEAI are utilising cloud services through Microsoft Office365, all CMP documents are accessible from any location online from any location or premises, provided SEAI systems are available.

### **3.5 Validation (Testing and Review):**

#### *Exercise and Testing*

A series of exercises and tests is carried out periodically to challenge the effectiveness of the response plan, in accordance with an Exercise & Test Master Schedule. Exercise and test results are reviewed by the respective manager, corrective actions identified where necessary and reported to the Business Continuity Manager.

#### *BCMS Review and Maintenance*

The performance of the BCMS will be reviewed at regular intervals and updated to reflect significant organisational and operational changes. The BCMS Operating Procedure details the annual programme of activities required to maintain the system. All BCPs are reviewed at least annually to ensure that the response capability

remains fit-for-purpose and up-to-date. Periodic internal audits, assessed against good practice and in alignment with ISO22301, supports the review and continuous improvement process.

Non-conformances or corrective actions are addressed in a timely manner and any required changes reflected in the appropriate documentation.

### **3.6 Embedding Business Continuity:**

Regular communication of the BCP programme is conducted across the organisation to support and maintain general awareness. Specific and targeted training requirements are identified for staff tasked with business continuity duties and responsibilities. The training schedule is coordinated by the Business Continuity Manager and is reviewed on an annual basis in line with a requirements analysis and the available training budget. Training records are maintained.

Each business function / programme is responsible for ensuring that relevant staff are adequately trained on their respective BCP and associated duties.

Business continuity considerations are incorporated into processes such as the SEAI Business Planning process, risk management, supplier management, service level performance reviews, change control and during the development of new services.

## Appendix 1: Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

<b>Activity</b>	Process or set of processes undertaken by an organisation (or on its behalf) that produces or supports one or more products and services.
<b>Audit</b>	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
<b>Business Continuity</b>	Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident (ISO22301)
<b>Business Continuity Management</b>	Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities (ISO22301).
<b>Business Continuity Management System (BCMS)</b>	Part of the overall management system that establishes implements, operates, monitors, reviews, maintains and improves business continuity.
<b>Business Continuity Plan (BCP)</b>	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
<b>Business Continuity Programme</b>	Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
<b>Business Impact Analysis (BIA)</b>	Process of analysing activities and the effect that a business disruption might have upon them.
<b>Crisis</b>	A critical event, which, if not handled in an appropriate manner, may dramatically affect an organization's profitability, reputation, or ability to operate. Abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability.
<b>Crisis Management</b>	The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate.
<b>Crisis Management Plan (CMP)</b>	A written account to support, coordinate and guide the management response to a crisis
<b>Service (Department) Response Plan (DRP)</b>	Documented procedures that guide a specific function to respond, recover, resume, and restore to a pre-defined level of operation following disruption
<b>Event</b>	Occurrence or change of a particular set of circumstances. <ul style="list-style-type: none"> <li>An event can sometimes be referred to as an "incident" or "accident".</li> <li>An event without consequences may also be referred to as a "near miss", "incident", "near hit", "close call".</li> </ul>

<b>Executive Leadership Team (ELT)</b>	Group of managers who direct and control the organisation at the highest (executive) level.
<b>Exercise</b>	Process to train for, assess, practice, and improve performance in an organisation. A test is a unique and particular type of exercise which incorporates an expectation of a pass or fail element within the goals or objectives of the exercise being planned
<b>Incident</b>	Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
<b>Infrastructure</b>	System of facilities, equipment and services needed for the operation of an organisation.
<b>Invocation</b>	Act of declaring that an organisation's business continuity arrangements need to be put into effect in order to continue delivery of key products or services.
<b>Maximum Acceptable Downtime (MAD)</b>	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. (See also Maximum Tolerable Period of Disruption)
<b>Maximum Tolerable Period of Disruption (MTPD)</b>	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. (See also Maximum Acceptable Outage)
<b>Outsource (verb)</b>	Make an arrangement where an external organization performs part of an organisation's function or process. <ul style="list-style-type: none"> <li>An external organisation is outside the scope of the management system, although the outsourced function or process is within the scope.</li> </ul>
<b>Policy</b>	Intentions and direction of an organisation as formally expressed by its management.
<b>Prioritised Activities</b>	Activities to which priority must be given following an incident in order to mitigate impacts. <ul style="list-style-type: none"> <li>Terms in common use to describe activities within this group include: critical, essential, vital, urgent and key.</li> </ul>
<b>Resources</b>	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organisation has to have available to use, when needed, in order to operate and meet its objective.

<b>Risk</b>	Effect of uncertainty on objectives.
<b>Risk Appetite</b>	Amount and type of risk that an organisation is willing to pursue or retain.
<b>Risk Assessment</b>	Overall process of risk identification, risk analysis and risk evaluation.
<b>Risk Management</b>	Coordinated activities to direct and control an organisation with regard to risk.
<b>Senior Leadership Team (SLT)</b>	Group of managers who direct and control the organisation at the senior (executive and department head) level.
<b>Testing</b>	Procedure for evaluation; a means of determining the presence, quality, or veracity of something.
<b>Verification</b>	Confirmation, through the provision of evidence, that specified requirements have been fulfilled.
<b>Work Environment</b>	Set of conditions under which work is performed. <ul style="list-style-type: none"> <li>• Conditions include physical, social, psychological and environmental factors (such as temperature, recognition schemes, ergonomics and atmospheric composition).</li> </ul>

## Appendix 13 - Risk Management Policy

### Risk Management Policy & Operational Framework

(Approved by the Board 11 December 2024)

<b>Document Reference</b>	Risk Management Policy
<b>Document Status</b>	Approved by Board
<b>Document Version</b>	3.4
<b>Approval Date</b>	11/12/2024
<b>Document Owner</b>	Chief Risk Officer
<b>Document Type</b>	Risk Management Policy

## Contents

1. Introduction .....	1
1.1 Policy Scope .....	1
1.2 Policy Scope (personnel affected) .....	1
1.3 Guiding Principles and Objectives .....	1
1.4 Policy Owner .....	1
1.5 Key Terminology .....	2
2. Risk Management Methodology .....	5
2.1 Overview .....	5
2.2 Risk Identification .....	5
2.3 Risk Assessment .....	8
2.4 Risk Treatment .....	9
2.5 Ongoing Monitoring .....	9
2.6 Risk Reporting .....	10
2.7 Embedding Risk .....	11
2.8 Fraud Risk Management .....	11
2.9 ISMS IT Risk Register .....	11
3. Risk Appetite .....	12
3.1 Appetite levels .....	12
3.2 Appetite areas .....	13
3.3 Escalation .....	13
3.4 Changes and Variations to Risk Appetite .....	13
4. Risk Management Governance Structure .....	14
4.1 Overview .....	14
4.2 Internal Control Environment .....	15
4.3 Key Roles and Responsibilities .....	16
<b>Appendix A – Risk Notification Template .....</b>	<b>19</b>
<b>Appendix B Maximum Risk Appetite Framework Heat Map on a page .....</b>	<b>21</b>
<b>Appendix C Level 2 Risk Taxonomy Definitions .....</b>	<b>22</b>



## 1. Introduction

### 1.1 Policy Scope

In line with requirements outlined in “Section 8.1 - Code of Practice for The Governance of State Bodies”, Sustainable Energy Authority of Ireland (SEAI) has implemented a defined and structured process by which risks are identified, assessed, managed and controlled.

The scope of this policy is to establish a framework to identify potential events that may expose SEAI to risk, to control and manage this risk within the Board’s risk appetite, and to provide reasonable assurance regarding the achievement of SEAI’s objectives.

### 1.2 Policy Scope (personnel affected)

All personnel at SEAI have a responsibility to engage in good risk management practices and contribute to the identification, management and reporting of risks, risk events and known/potential control deficiencies. Further, all personnel are expected to actively anticipate and manage risks and take advantage of opportunities within defined risk appetites. The external and internal risks being faced by SEAI are changing constantly and personnel are expected to proactively:

- Utilise experience through knowledge sharing;
- Deal with ambiguity, uncertainty and increasing complexity;
- Prioritise, make decisions and implement solutions on a timely basis;
- Recognise and act on opportunities as they occur;
- Participate in achievement of business objectives despite a changing business environment.

### 1.3 Guiding Principles and Objectives

SEAI’s Vision for Risk Management:

*SEAI seeks to adopt best practice in the identification, assessment and control of risks to ensure that they are eliminated or reduced to a level acceptable to the Board in the achievement of its objectives.*

The following six guiding principles and objectives outline SEAI’s approach to risk management in- order to achieve this vision:

- I. All members of SEAI have a responsibility to contribute to the ongoing management and identification of risk
- II. Risks are recorded, assessed and reported upon in a consistent and transparent manner
- III. Risks are managed in line with the Risk Appetite communicated by the Board (and where this is unknown or unclear, personnel should seek clarity from their direct manager)
- IV. Risk events are reported and investigated promptly and in an appropriate manner
- V. Consideration of risk should inform all decision making (including development of business plans)
- VI. Where preventative or remediation action is required, management will respond promptly and proactively selecting the risk treatment that best meets the needs of the organisation

### 1.4 Policy Owner

The Board has overall responsibility for risk management within SEAI including approving changes to Risk Management policies and procedures.

Enquiries about this policy or other related risk management issues should be directed to the Internal Audit & Risk Manager, Head of Governance & Procurement, or the Chief Risk Officer.

## 1.5 Key Terminology

TERM	DEFINITION
<b><i>Risk</i></b>	<p>An event, that may or may not occur, that has the potential to affect SEAI's ability to achieve its strategic objectives.</p> <p>Note(s):</p> <ul style="list-style-type: none"> <li>Risks are characterised by uncertainty or a lack of information, which may relate to the nature of the event itself or its likelihood or impact.</li> <li>ISO31000:2018 Risk Management Standard extends the definition of risk to also include potential events that could have a positive impact on the achievement of strategic objectives. (SEAI defines these events as opportunities which are addressed in Department/Unit business plans).</li> </ul>
<b><i>Enterprise Risk Management</i></b>	A process which has been designed to identify potential events that might mitigate against SEAI's ability to achieve the policy objectives in its Strategic Plan. The process seeks to control these risks in order to provide reasonable assurance regarding the achievement of the agency's objectives.
<b><i>Risk Policy</i></b>	SEAI's position with regard to the standards for identification, assessment, tolerance, mitigation, monitoring and reporting of risk.
<b><i>Risk Identification</i></b>	The process of determining what risks might happen and under what circumstances they may occur. This involves ongoing scanning of SEAI's internal and external operating environment to identify new and emerging organisational, legislative, financial, technological and other factors that could impact the organisation's ability to achieve its Strategic objectives.
<b><i>Risk Assessment</i></b>	Categorization of risks, based on Likelihood and Impact, to assist management with prioritizing risk remediation and monitoring activities, and determine which risks require Senior Management and Board input and/or intervention.
<b><i>Impact</i></b>	A measure of the damage/harm arising from the adverse consequence suffered by the organisation in the event a risk occurs i.e. a risk event. The Impact of Risks is measured on a scale of 1 – 5 (see Methodology)
<b><i>Likelihood</i></b>	A measure of the degree of possibility of a risk occurring in an organisation taking into account the strengths and weaknesses of the organisation's controls and known instances where the risk has occurred. The Likelihood of Risks is measured on a scale of 1-5 (see Methodology).
<b><i>Risk Appetite</i></b>	Level of risk that the Board of SEAI is prepared to accept in order for the organisation to achieve its strategic objectives.
<b><i>Risk Event</i></b>	The occurrence of a known or unforeseen risk.

	<p>Note(s):</p> <ul style="list-style-type: none"> <li>• A risk event may occur due to a breakdown in the controls framework or some other unforeseen factor.</li> <li>• Risk events must be reported upon and investigated as per the Board's requirements (which may vary depending upon the nature and materiality of the risk event.)</li> <li>• Events assessed to have the potential to re-occur again in the future, or whose likelihood of reoccurring is unclear, should be communicated to SEAI's Internal Audit &amp; Risk Manager, Head of Governance &amp; Procurement and Chief Risk Officer for inclusion in the appropriate Departmental Risk Register or Organisation Risk Register (as appropriate).</li> </ul>
<b>Issue</b>	<p>A current problem impacting on the achievement of SEAI's objectives, requiring action to be taken to remediate the situation. The main difference between an issue and a risk is that an issue refers to a situation which has already occurred, whereas a risk may or may not occur in the future. An issue may result in multiple risk events and vice versa. For example, an IT system outage is an issue, whereas the possibility of a currently working IT system failing in the future is a risk.</p>
<b>Emerging Risk</b>	<p>A risk that is new, or a familiar risk in a new or unfamiliar context or under new context conditions (re-emerging)<sup>1</sup>. Such risks are often evolving in areas and ways where the body of available knowledge is weak, which makes risk assessment challenging<sup>2</sup>.</p>
<b>Near-Miss</b>	<p>A risk event which by chance did not result in any adverse impact on SEAI.</p>
<b>Controls</b>	<p>Checks and safeguards in place to reduce the Likelihood or Impact of a risk to an acceptable level e.g. Segregation of Duties, Physical limitations on access, Passwords, authority limits, approvals etc.</p> <p>Note(s):</p> <ul style="list-style-type: none"> <li>• Controls may be automated e.g. System enforced authority levels, or Manual e.g. Supervisor review.</li> </ul>
<b>Action Plans</b>	<p>Activities undertaken to modify risk levels which can be grouped into four main categories (or "Treatments"):</p> <ul style="list-style-type: none"> <li>• Avoidance (eliminate, withdraw from or not become involved)</li> <li>• Reduction (implement additional or enhanced mitigating controls)</li> <li>• Sharing (transfer the risk via outsourcing or insurance)</li> <li>• Retention (accept the risk at its current level and budget for potential events)</li> </ul>

<sup>1</sup> [Governance of Emerging Risks - IRGC](#)

<sup>2</sup> [how-to-assess-and-treat-emerging-risks-charities-sig-final.pdf \(theirm.org\)](#)

<b>Risk Taxonomy</b>	A risk taxonomy is a comprehensive, common, and stable set of risk categories that is used within an organization <sup>3</sup>
<b>Inherent Risk</b>	Also referred to as <i>raw</i> risk. Level of risk to an entity in the absence of any controls or management actions to alter a risks Likelihood and/or Impact.
<b>Residual Risk</b>	Risk that remains after management's response, including controls, have been applied to reduce the Likelihood and or Impact of a risk. Within SEAI, risk ratings (and other risk related communications and discussions) are based on Residual Risk.
<b>Risk Register</b>	List of known risks and associated information. SEAI tracks details of all key Departmental and Organisational risks in a Risk Management platform (currently Decision Time) which is maintained on an ongoing basis by the Internal Audit & Risk team with support from the Risk Champions and Head of Department. In situations where business areas or projects are maintaining their own risk register and where a risk is escalating to the point that it is becoming a Departmental or Organisational risk, this should be communicated to the Internal Audit & Risk Manager/ Head of Governance and Procurement or Chief Risk Officer for assessment of next steps.

## 2. Risk Management Methodology

### 2.0 Overview

Risk management is an umbrella discipline that cuts across all areas of activity within an organisation, reflecting the fact that risks permeate across all activities and lines of services. To be effective, risk assessment must be integrated into business processes to provide timely and relevant risk information to management. This is a continuous process owned by the business and embedded within the business cycle, starting with risk identification as part of the strategic planning process, carrying through to business process and execution, and ending in evaluation. SEAI seeks to apply best practice principles as outlined in the Code of Practice for the Governance of State Bodies (2016) and ISO 31000: 2018 Risk Management best practices.

The risk management process consists of the following steps:

- Risk Identification
- Risk Assessment
- Risk Treatment, including the identification of suitable controls and ongoing monitoring
- Ongoing Reporting
- Reviewing the Risk Management Framework

### 2.1 Risk Identification

Risks affect all aspects of organisational activity. Documenting risks (in the form of a register) provides a framework for business units, functional areas and projects to track and assess the organisation's exposure to risk. The Risk identification process is conducted biannually.

The Organisation Risk Register submitted for approval to the SEAI Audit and Risk Committee and the SEAI Board is a combination of new and emerging strategic risks derived from input received from the SEAI Executive Team and various other stakeholders involved in the bi-annual risk review process. Managers document their key business objectives and then undertake a process to determine an event (that may or may not occur) that has the potential to affect SEAI's ability to achieve its strategic objectives. These are documented through departmental or programmatic risk registers, which in turn inform the Organisation Risk Register.

The Organisation Risk Register captures the key strategic risks. Other programmatic or departmental specific risks are recorded on Departmental Risk Registers.

There are a number of channels available to assist with the identification of risks including (but not limited to):

- Business Plan Review process
- ongoing scanning of internal and external environments
- group workshops
- international standards and recognised frameworks e.g. ISO 31000
- professional association publications
- known incidents and near misses
- process flowcharts and risk control matrix

Descriptions of risks should be clear, comprehensible and unambiguous. All risks should be allocated a Risk Owner(s). Descriptions should (1) identify an event or set of circumstances (that may or may not occur) and (2) the impact this may have on the ability of the organisation to achieve its organisation and strategic objectives.

For consistency of documentation of risk description, SEAI uses the following format: “**X** happens because of/due to **Y**”. Where the consequence is not immediately evident, the risk will also capture what may be described as “resulting in **Z**”.

### 2.2.1 Risk Taxonomy

To facilitate the capturing and reporting of risks in a consistent manner six broad categories of risks (Level 1 risk categories) have been identified. These are further sub-divided into more granular risk categories (Level 2). This additional categorisation facilitates the identification of risk themes across departments and helps avoid inconsistencies, duplication and/or gaps in the risk register. See Appendix C for definitions. It also enables a consistent method of linking risks on the risk register to SEAI’s risk appetite statements.

<b>Level 1 RISK CATEGORY</b>	<b>Level 1 DESCRIPTION</b>	<b>Level 2 Risk Categories</b>
<b>Strategic</b>	Risks associated with failure to achieve the strategic and business objectives	<ul style="list-style-type: none"> <li>• Strategic Mandate</li> <li>• Strategic Delivery</li> <li>• Erroneous policy or expert advice</li> <li>• Inadequate design or insufficient range of grant schemes.</li> </ul>
<b>Governance and Compliance</b>	Risks relating to failing to comply with statutory/ legal obligations.	<ul style="list-style-type: none"> <li>• Regulatory Compliance</li> <li>• Legal Risk</li> <li>• Regulatory Functions/Delegated Authorities</li> </ul>
<b>Financial and Funding</b>	Failure to maintain effective financial management and accountability arrangements in all activities	<ul style="list-style-type: none"> <li>• Financial Management</li> <li>• Fraud, Bribery and Corruption</li> <li>• Credit Risk</li> <li>• Liquidity Risk</li> </ul>
<b>Brand Reputation and Trust</b>	Potential for negative publicity, public perception or uncontrollable events	<ul style="list-style-type: none"> <li>• Reputational Risk</li> </ul>
<b>Operational</b>	Risks arising from people, processes and systems involved in SEAI’s day to day activities	<ul style="list-style-type: none"> <li>• People Risk</li> <li>• Business Continuity</li> <li>• Outsourcing/Third Party Vendor</li> <li>• Change Management</li> <li>• Stakeholder Experience</li> <li>• IT Systems Risk</li> <li>• Information Security</li> <li>• Data Management</li> <li>• Developing Partnerships</li> <li>• Supply Chain</li> <li>• Customer Experience</li> <li>• Concentration Risk</li> </ul>
<b>Macro-Risks</b>	Macro risks refer to the external risks relating to economic, political, environmental, social factors.	<ul style="list-style-type: none"> <li>• Economic</li> <li>• Socio-Political</li> <li>• Environmental</li> </ul>

### *2.2.2. Employee's role in risk identification*

SEAI encourages a risk culture where individual accountability is encouraged. This means that each employee is empowered to be open and fact-based in discussing issues, making all relevant facts and information available so SEAI can assess the risks associated to the conditions identified by employees. Each employee is accountable for raising and escalating concerns to management about issues that may cause risk or create opportunity.

To ensure that each Department's risk register remains up to date, biannual risk discussions are held at department level, which capture employee feedback on risk and control. Internal and external events affecting the ability to achieve set objectives are identified and discussed. Based on this feedback, Departmental Risk registers are updated to reflect the most up to date risk identification and assessment. Risk update and identification is an agenda item in the Departmental, Executive and Audit and Risk Committee meetings.

### *2.2.3 Procedure for adding, changing or removing risks from the Organisation level risk register*

On a biannual basis, new risks, changes to risk profiles or the removal of risks will be considered as part of the Departmental Risk Register Review and Organisational Risk Register Review process. The outputs of this process will be summarised and discussed by the SMT and the ELT and will form part of the biannual reporting to the Audit and Risk Committee and the Board on the annual risk identification process.

Outside of the biannual risk identification process, any new proposals for adding, changing or removing risks (Appendix A) from the organisation level risk register must be tracked through the use of the Risk notification form and proposed by the relevant Executive level risk owner(s) at a meeting of the Executive Committee.

The Risk notification form is used to capture:

- risk category
- risk description (existing or proposed wording)
- risk owner(s)
- rationale for proposed new risk, risk amendment (for example, changes to risk wording or assessment) or risk removal from the organisation level risk register
- existing controls
- proposed likelihood score (newly proposed or amended)
- proposed impact score (newly proposed or amended)
- planned further actions
- action owners and timelines

The Risk notification form is prepared by the relevant risk owner(s) and sent to the Internal Audit and Risk Manager, Head of Governance and Procurement and Chief Risk Officer. The Chief Risk Officer will assess the Risk notification form and propose any changes to the organisation level risk register to the Executive Committee.

The risk notification form is also maintained as a formal record to track the addition of any new risks, changes to risk assessment or the removal of risks throughout the year.

Where a decision is made to remove a risk from the organisation level risk register, the risk must, where appropriate, be included in the relevant Departmental level risk register(s), which are maintained by Head of Departments, to ensure that the risk continues to be tracked and monitored.

The template "Risk notification" form is included at Appendix A.

## 2.3 Risk Assessment

To assist with determining if the level of risk is within the stated risk appetite, and enable Management to prioritise remediation and corrective actions, risks are assessed based on their Likelihood (probability of the risk occurring) and Impact (harm to the organisation if it does occur) using the following 5-point scale for each.

### 2.3.1 Standard Likelihood & Impact 5 Point Scoring Scale

SCALE	LIKELIHOOD	IMPACT
5	Almost certain to happen (Probability 71% to 100%)	Catastrophic, extremely detrimental (e.g. major compliance breach, unsuccessful litigation, financial loss). Serious effect on performance or reputation in the long term (3yrs+)
4	Likely, will occur in most circumstances (Probability 51% to 70%)	Very significant with significant damage (e.g. scheme failure, compliance breach, inadequate business recovery in a timely basis). Serious effect on performance or reputation in the medium term (1-3yrs)
3	Moderate, may occur (Probability 31% to 50%)	Significant but containable (e.g. control breakdown resulting in material costs, diminished service or relationships). Significant effect on performance or reputation in the short term (up to 1 yr)
2	Unlikely, may occur at some point (Probability 11% to 30%)	Minor significance, with minor impact (e.g. pay-out out for customer error, costs are kept to a minimal, staff turnover)
1	Rare, may occur in exceptional circumstances (Probability less than 10%)	Insignificant, no significant impact (e.g. customer service error, embarrassment with good client, minor control failure)

Please note:

- Unless otherwise indicated, all risk assessments performed within SEAI are based on Residual Risk (i.e. taking into account the impact of existing controls.)
- Risk Owners are encouraged to document key controls linked to the risk to assist with evaluating the effectiveness of controls design and inform those scoring the risk.
- Known risk events should be communicated to those scoring a risk to assist in their evaluation.
- Where more than one person is scoring a risk (e.g. during a workshop), consensus scoring of Likelihood and Impact should be used. Participating individuals should be requested to abstain from scoring risks on subject areas with which they are unfamiliar.

### 2.3.2 Risk Rating

SEAI uses a three-point rating scale (High, Medium & Low) to categorise risks (based on Likelihood and Impact) to assist management with prioritizing risk remediation and monitoring activities, and determine which risks require Senior Management and Board input and/or intervention. A risk's rating



is determined by plotting its Likelihood and Impact against a pre-defined matrix and is categorised as follows:

<i>Rating scale</i>	<i>Likelihood x Impact</i>	<i>Details</i>
<i>High</i>	15-25	Key risks. Critical risks that threaten the achievement of SEAI's strategic objectives. (High impact with limited effective controls to reduce its likelihood).  Review constantly and monitor monthly
<i>Medium</i>	8-14	Secondary risks. Risks that can have a significant adverse effect on the organisation. (Either a high Likelihood or Impact score creating a scenario whereby they may be unlikely to occur but have a high impact or vice versa).  Review and monitor 6-monthly / quarterly / monthly as appropriate depending on relevant risk appetite
<i>Low</i>	1-7	Actions required typically focus on maintaining the current controls and monitoring to determine if a change in classification  Review at least annually

## 2.4 Risk Treatment

Once a risk rating has been determined this should then be compared to the approved Risk within acceptable limits. Where a risk exceeds the risk appetite limit (or where an opportunity to improve the effectiveness or efficiency of internal controls is identified) the Risk Owner should, in consultation with the Head of Department and affected business areas, agree what approach will be taken.

Approaches to modifying risk levels can be grouped into four main categories (or "Treatments"):

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (implement additional or enhanced mitigating controls)
- Sharing (transfer the risk via outsourcing or insurance)
- Retention (accept the risk at its current level and budget for potential events)

Please note:

The approach selected (including agreed upon milestones and activities) should be documented and approved/agreed by relevant stakeholders

Owners of risks listed in the Main Organisation Register are required to provide the Internal Audit and Risk Manager with periodic updates to enable tracking of remediation activities to completion. Owners of risks that are above risk appetite must provide updates at the SMT/ELT meetings.

## 2.5 Ongoing Monitoring

To be effective, Risk Management must be a continuous process, integrated into key business and planning activities. Managers and Risk Owners are responsible for monitoring their respective areas and internal/external environments for the emergence of new risks, or factors that may change the Likelihood or Impact of existing risks. Managers are also responsible for regularly reviewing risk registers maintained by their area.

Changes to risks that are tracked via the Risk Register (or which escalate a risks status to High) should be immediately reported to the Internal Audit and Risk Manager, Head of Governance & Procurement and Chief Risk Officer.

### 2.5.1 Risk Register Reviews

The full Risk Register should be reviewed and updated biannually. Key steps when reviewing the register include:

- Assess risks in the register including how they were identified, monitored and managed
- Consider any new risks proposed for addition to the risk register, including associated controls
- Determine if there are risks which are no longer relevant (and can be “removed” from the register upon proposal by the relevant risk owner)
- Determine progress against previously agreed activities

Develop and agree remediation activities and consider whether control strategies need to be changed. Risk Owners are requested to review the Risk Register, provide the key controls in place and note any mitigating actions required including the action owner and expected completion date.

Risks owners of risks that are above risk appetite should provide periodic updates at Senior Management Team meetings, to note any changes.

An update of the Risk Register is communicated to the Audit and Risk Committee on a biannual basis to review all key risks to determine if corrective action is required and assess progress against agreed upon remediation activities.

The risk register is also subject to biannual review and approval by the Board, and more frequently, where requested by the Chair of the Board. Periodically the Board or its sub-committees may request a risk workshop to consider the risk landscape and consider, in more depth, the risks captured on the Organisational Risk Register.

### 2.6 Risk Reporting

Risk reporting is fundamental to risk management. Reporting provides assurances to management and the Board that risks are being regularly reviewed, effectively managed and helps in creating a risk aware culture. Reporting will include:

- Periodic risk updates on SMT/ELT agenda and consideration of pertinent risks or risks exceeding risk appetite and actions to address.
- Biannual risk reporting by the Chief Risk Officer to the Audit and Risk Committee, including reporting upon risk ratings, risk movements and updates on action plans.
- Biannual risk reporting by the Audit and Risk Committee to the Board, including reporting upon risk ratings and movements in risk(s).
- Standing item on Audit and Risk Committee and Board agendas

As part of the biannual risk management reporting process, all Organisation Risks (including any which are classified as High Impact and Low Probability) are reported upon, including the reporting upon controls activities and any further actions required to help further mitigate the risk. The movement in any such risks is also formally tracked and monitored through the risk register reporting process.

On a biannual basis, risk reporting includes a comparison of individual risks against the stated risk appetite for that category of risk. This facilitates additional focus upon control activities and further actions which are required to mitigate the risk to within risk appetite thresholds. These actions are formally recorded and tracked through the SEAI risk register.

## 2.7 Embedding Risk

Specific and targeted training requirements are identified for staff tasked with risk management duties and responsibilities. The training schedule is coordinated by the Internal Audit and Risk Manager and is reviewed on an annual basis in line with a requirements analysis and the available training budget. Training records are maintained.

Each business function / programme is responsible for ensuring that relevant staff are adequately trained on their respective risk registers and associated duties.

Risk management considerations are incorporated into processes such as the SEAI Business Planning process, change control and during the development of new activities.

## 2.8 Fraud Risk Management

SEAI is committed to the prevention of fraud, bribery and corruption and to the promotion of an anti-fraud, anti-bribery and anti-corruption culture. SEAI aims to manage and control operations, processes, projects and systems in such a way that the risk of fraud, bribery and corruption is minimised. It is committed to investigating thoroughly all cases of suspected fraud, corruption and related offences and to recover any money and /or property, including intellectual property, lost through fraud, bribery or corruption. SEAI will also, when necessary, pursue prosecution through the Courts.

This policy along with the Fraud Risk Assessment Guidelines and the Anti-Fraud, Bribery and Corruption policy form a part of the Fraud Risk Management Framework at SEAI. The Anti-Fraud, Bribery & Corruption Policy sets out the Risk Factors with respect to fraud, bribery and corruption, SEAI responsibilities and provides guidance on matters which may constitute acts of fraud, bribery or corruption.

Fraud Risk Assessments will be carried out on any new schemes or material changes to existing schemes (refer to Standard Programme Design Framework Guidelines). In addition, periodic reviews will be completed on existing schemes. Refer to Fraud Risk Assessment guidelines which sets out how the process should be conducted.

The Risk Management process as covered under this policy including risk identification, risk assessment, risk treatment, risk reporting and risk reviewing is also applicable to Fraud Risk Management.

## 2.9 ISMS IT Risk Register

SEAI's ISO 27001 Information Security Management System (ISMS) follows the SEAI risk management process but has additional details and requirements.

The IT risk register is reviewed quarterly, major IT changes will trigger additional reviews. Reviews are undertaken by SEAI's IT Security Executive, IT Governance Manager, and IT security consultant company. Risks are assessed in terms of confidentiality, integrity, and availability.

For risk treatment, ISO 27001 Annex A controls will be viewed to verify that no standard necessary controls have been omitted.

IT risks, treatments, control implementation and efficacy are monitored in an ongoing plan, check, do, act (PCDA) cycle.

SEAI's entire ISMS including the ISMS IT risk register will be audited internally once a year. An independent external auditor will do a full audit of the ISMS to obtain ISO 27001 certification with surveillance audits to be carried out during the certification cycle of three years. The results of these audits will be shared with SEAI's Corporate Services Director, CIO and Audit and Risk committee.

### 3. Risk Appetite

Risk appetite is defined by ISO 31000, Risk Management, as the 'Amount and type of risk that an organisation is prepared to pursue, retain or take'.

Risk appetite sets the understanding of an organisation's ability to take risk, articulated and quantified in a manner that is meaningful for day-to-day decisions. It is a tool to prepare for the unknown, develop risk maturity to uncover intelligent risk making opportunities, while putting in place risk mitigating measures.

The Board of SEAI ("Board") is responsible for setting the tone for risk management throughout the organisation by clearly articulating and communicating its tolerance for risk ("Risk Appetite") on an ongoing basis. Management (and appointed sub-committees) are in-turn responsible for ensuring SEAI operates in a manner that is consistent with the Board's Risk Appetite (and seeking clarification if this is unclear). In the event a risk exceeds an approved threshold, management is required to perform corrective action to bring it back within the tolerances set by the Board (and where necessary, immediately escalate the risk for Executive Committee and/or Board attention).

#### 3.1 Appetite levels

Risk appetite may be measured on a low to high scale under the terms Averse to Elevated. However, as a Public Body, it is deemed that SEAI should not conduct activity that would be classified under 'Elevated'. As such, it is expected that SEAI's risk appetite will normally range from Averse to Open, along the guidance actions included in table below.

	Averse	Minimal	Moderate	Open	Elevated
Philosophy	Avoidance of risk is a core objective.	Conservative.	Preference for safe delivery.	Will take justified risks greater than normal risks.	Will take aggressive justified risks
Tolerance for uncertainty	Extremely low	Low	Limited	Expect some	High
Preferred risk response approach	Those risks that can not be effectively treated or transferred are avoided	Preference for safe delivery options that have a low degree of inherent risk	Preference for safe delivery taking a balanced approach to risk taking	Preference to accept or reduce risk through internal measures	Risk is accepted
Choice when faced with multiple options	Will select lowest risk option always. Not willing to accept any negative impact in order to pursue strategic sub-objective	Will accept only if essential and limited possibility/extent of failure. Only willing to accept a small negative impact in order to pursue strategic sub-objective	Will accept if limited, and heavily out-weighted by benefits. Potential negative impact and strategic sub-objective completion given equal considerations.	Willing to accept the potential for some negative impact in order to pursue strategic sub-objective.	Will choose option with highest return; accept possibility of failure. Willing to accept a large negative impact in order to pursue strategic sub-objective.
Trade-off against achievement of other objectives	Never	Avoid	Occasionally	Willing under the right conditions	Willing
Residual Risk Score*	0 - 7	8 - 11	12 - 15	16 - 19	20 - 25

\*Risk score calculated using Impact x Probability (5\*5) matrix.

### 3.2 Appetite areas

SEAI's mechanisms to attain organisation goals and objectives include delivering agile and impactful programmes, informing policy, providing expert advice to influence behaviour change, delegated responsibilities, whilst applying the appropriate operational governance procedures to all activities.

SEAI is exposed to a range of inherent risks during the course of organisation delivery, some of which cannot be completely mitigated or reduced to "Low" levels. Hence, on a case-by-case basis, higher tolerance levels may be set by the Board for specific risks (or risk areas), to reflect the organisation's willingness to accept higher levels of risk to achieve its business objectives.

To reflect SEAI's multifaceted functions, SEAI's Statement of Risk Appetite is articulated through a series of statements that describe the levels of risk that the SEAI deem to be acceptable in the pursuit of overall organisational goals.

Appendices B & C detail the 23 Risk Appetite Statements.

### 3.3 Escalation

In the case of business unit or department risk registers, it is the responsibility of the Business Unit or Department Manager to ensure these are communicated to the responsible Head of Department who in turn will liaise with the Internal Audit and Risk Manager and Chief Risk Officer for consideration for inclusion in the Organisation Risk Register. (see 2.2.3)

Any risk exceeding risk appetite threshold will require specific review and remedial action to be tracked. ELT to review and decide if risks assessed as higher than risk appetite are escalated to Board level (included in organisation level risk register).

Where a new or changing risk poses a significant Reputational, Business Disruption, Financial or Health and Safety threat to SEAI, these should be immediately escalated to the Head of Department who in turn will liaise with the Internal Audit and Risk Manager and Chief Risk Officer.

Significant or sudden emerging risks may require immediate escalation to Audit and Risk Committee or Board, as appropriate.

### 3.4 Changes and Variations to Risk Appetite

The Statement of Risk Appetite should be regarded as a 'living document' that reflects the attitudes of the Board towards the risk taking capacity of the organisation at a point in time, and should evolve over time in responses to changes in SEAI strategy and business environment

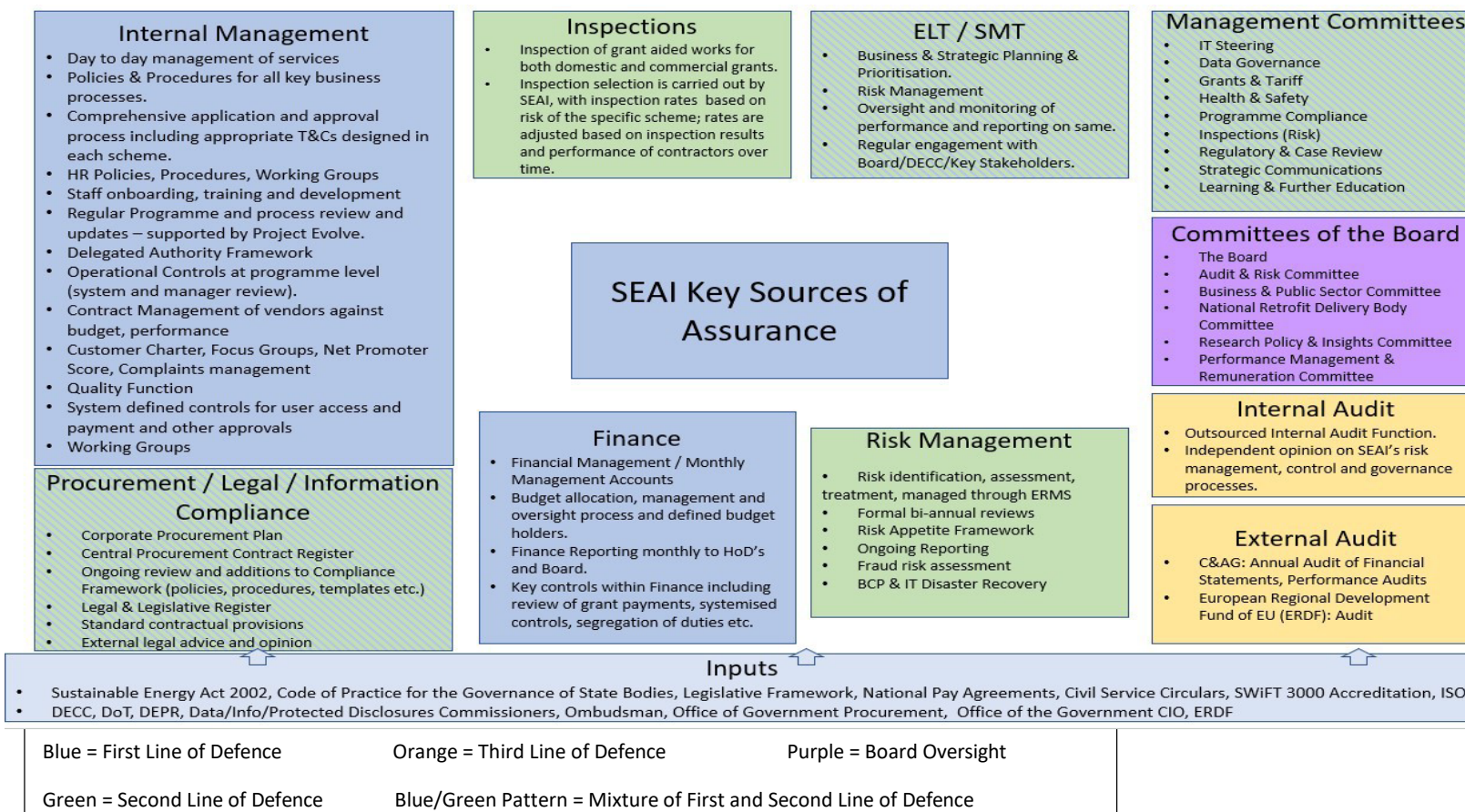
At the Board's discretion, the risk appetite can be changed or modified to reflect the changing needs of the organisation. In addition, the Board may elect to set individual risk appetites (pertaining to a specific activity, functional area, type of risk, impact, client or other criteria) or set appetites based on performance or quantitative metrics to allow for greater flexibility in the management of risk, or ensure sensitive issues are appropriately escalated.



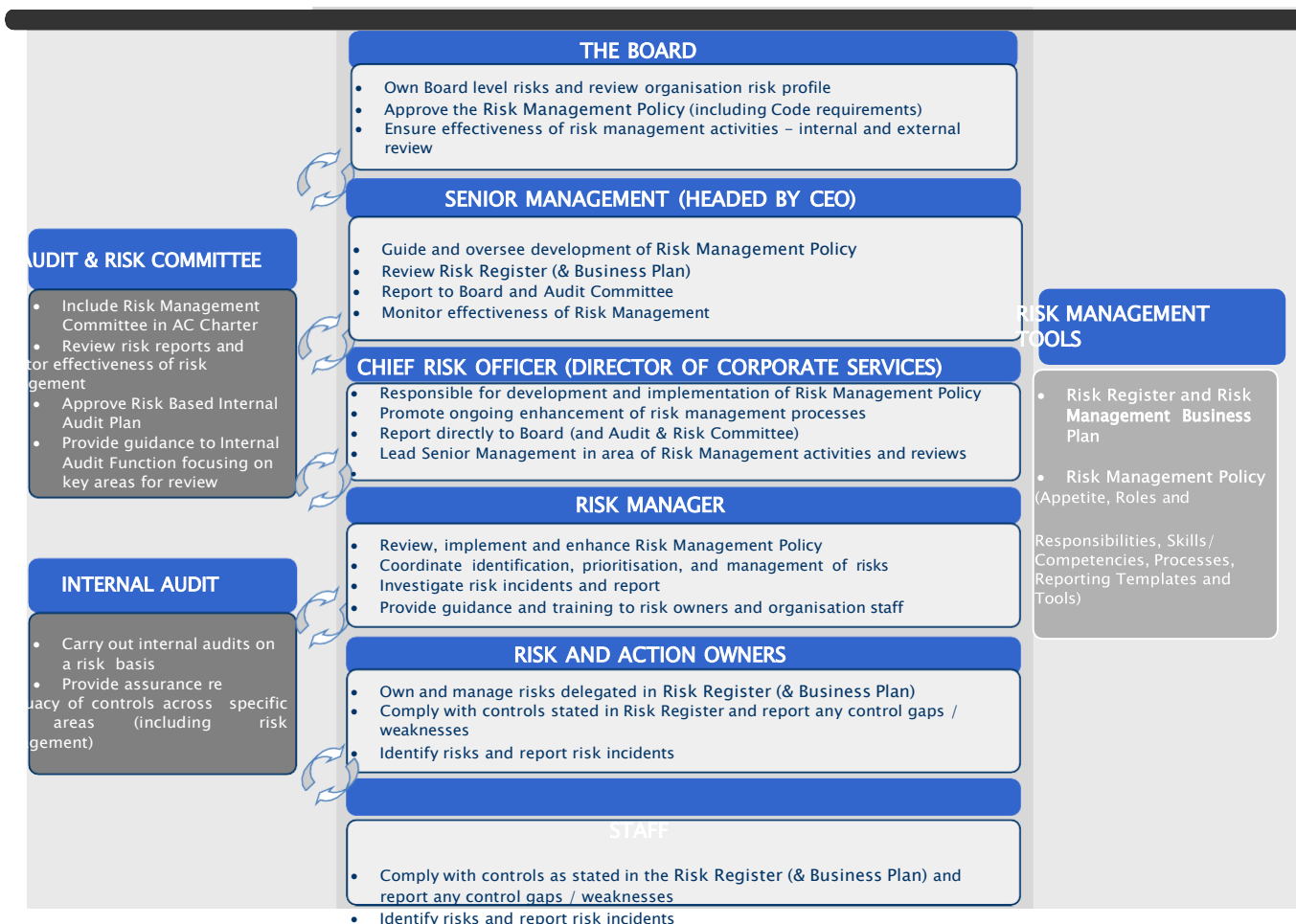
## 4. Risk Management Governance Structure

### 4.4 Overview

The management of risk should be integrated across all levels of the organisation, so that each level supports another. Risk management should be led from the top and operated on the basis of clearly-defined structures and responsibilities. It should be embedded in the normal working routines and activities of the organisation, with all staff conscious of the relevance of risk to achieving their objectives. Risk Assurance is provided across three lines of defence. First line functions own and manage risks as part of their operational activities, second line functions oversee risk management and compliance across the organisation and third line independent assurance is provided through internal and external audits. The key sources of assurance for SEAI across the three lines of defence are listed in the diagram below.



The diagram below presents the high-level risk management framework for SEAI.



## 4.2 Internal Control Environment

The primary objectives of the internal control system within SEAI are:

- To ensure compliance with applicable policies, procedures, laws, regulations and processes
- Delegation of responsibilities to ensure controls are appropriately managed
- To promote effective and efficient use of resources and operations

To support the internal control objectives, the control environment consists of policies, procedures, authority limits, approval processes and other system and manual controls utilised by SEAI to reduce the likelihood and/or impact of a risk to an acceptable level. A key element of SEAI's internal control environment is the delegated authority framework, which consists of the various Board Sub-Committees, Approval & Advisory Committees which have been established for the ongoing monitoring and management of key organisational risks.

### 4.3 Key Roles and Responsibilities

Structure	Responsibilities
<b>The Board</b>	<p>The Board should approve the risk management framework and monitor its effectiveness. The Board should review material risk incidents and note or approve management's actions, as appropriate. Key elements of the Board's oversight of risk management include:</p> <ul style="list-style-type: none"> <li>▪ Assume ownership of Board level risks</li> <li>▪ Hold a Board risk workshop outside of the regular risk reporting cycle periodically (typically every 2 years)</li> <li>▪ Approve the risk management policy, set the risk appetite, and approve the risk register (&amp; business plan) at least annually</li> <li>▪ Include risk management as a standing meeting agenda item</li> <li>▪ Establish a sub-committee of the Board: Audit and Risk Committee, with specific terms of reference, which includes risk management</li> <li>▪ Include risk management experience/expertise in the competencies of at least one Board member. Where composition of the Board does not allow for this, expert advice should be sought externally</li> <li>▪ Appoint a Chief Risk Officer within the executive and provide for a direct reporting line to the Board</li> <li>▪ Delegate risk management to the Executive</li> <li>▪ Review management reporting on risk management, review the risk profile, monitor deviations from risk appetite, and note/approve mitigating actions as appropriate</li> <li>▪ Require external review of effectiveness of risk management framework on a periodic basis.</li> </ul>
<b>Senior Management (headed by CEO)</b>	<p>Primary ownership for organisation risks. Although the management of some risks may be delegated on the risk register, accountability may not be delegated</p> <ul style="list-style-type: none"> <li>▪ Appoint a Chief Risk Officer</li> <li>▪ Promoting Risk Management within SEAI and ensuring that it receives appropriate priority and resourcing</li> <li>▪ The ongoing identification and evaluation of risks and the internal controls environment that might have an impact on SEAI's ability to achieve its Strategic or Organisation plans and objectives</li> <li>▪ Ensuring that Risk Management is effectively implemented and embedded in SEAI's planning and operational processes</li> <li>▪ Promoting and monitoring compliance with approved risk management policies and procedures</li> <li>▪ Providing a framework for risk event reporting and escalation</li> </ul>
<b>Chief Risk Officer –</b>	<p>The Chief Risk Officer will co-ordinate the day-to-day operations of SEAI's Risk Function with responsibility for:</p>



<b>Corporate Services Director</b>	<ul style="list-style-type: none"> <li>▪ Responsible for development and implementation of Risk Management Policy</li> <li>▪ Promotion of best practice in Risk Management within SEAI</li> <li>▪ Lead Senior Management in area of Risk Management activities and reviews</li> <li>▪ Critically reviewing the effectiveness of strategies implemented to ensure that corporate practices appropriately balance risk and operational effectiveness in achieving objectives.</li> <li>▪ Reporting to the Executive Committee, the Audit and Risk Committee and the Board on the operation of risk management processes and procedures</li> <li>▪ Report directly to the Board (and Audit Committee) at least annually</li> <li>▪ Report to Senior Management on an ongoing basis</li> </ul>
<b>Risk Manager</b>	<ul style="list-style-type: none"> <li>▪ Review, implement and enhance Risk Management Policy</li> <li>▪ Promotion of best practice in Risk Management within SEAI</li> <li>▪ Coordinate identification, prioritisation, and management of risks</li> <li>▪ Co-ordinating risk workshops</li> <li>▪ Monitoring the implementation of risk management systems</li> <li>▪ Providing advice, guidance and training to risk owners and management</li> <li>▪ Investigate risk incidents and report</li> <li>▪ Ensuring SEAI Inspection protocols are aligned to risk appetite level according to status of Programme or Scheme, with feedback to programme for correction or improvement.</li> <li>▪ Reporting to the Chief Risk Officer, Executive Committee, the Audit and Risk Committee and the Board on the operation of risk management processes and procedures</li> </ul>
<b>Risk and Action Owners</b>	<p>Risk and Action Owners should:</p> <ul style="list-style-type: none"> <li>▪ Own and manage risks delegated in the risk register (&amp; business plan) on a day to day basis</li> <li>▪ Implement controls as stated in the organisation risk register (&amp; business plan) and report any control gaps / weaknesses, including where internal controls are not aligned to risk appetite (too adverse, or insufficient)</li> <li>▪ Identify new risks and report risk incidents</li> <li>▪ Ensure risks incidents are identified and reported in a timely and effective manner</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Participate in the identification, measurement, prioritisation, and management of risks and controls</li> <li>▪ Be responsible for monitoring controls and implementing actions identified</li> <li>▪ Have performance indicators and early warning systems which allow them to monitor progress, and any deviation from expected outcomes</li> <li>▪ Report systematically and promptly to the chief risk officer any perceived new risks or failures of existing control measures</li> </ul>
<b>Staff</b>	<p>Staff should:</p> <ul style="list-style-type: none"> <li>▪ Provide input into the identification and management of risks as required</li> <li>▪ Understand their accountability for individual risks</li> <li>▪ Comply with all controls pertaining to their area of operation.</li> <li>▪ Take responsibility for carrying out control activities, reporting on control gaps / weaknesses along with any perceived changes in the risk environment as appropriate</li> <li>▪ Update management regarding status of risks and controls as required</li> </ul>
<b>Structure</b>	<b>Responsibilities</b>
<b>Audit and Risk Committee</b>	<p>The Audit Committee should review and agree the processes for managing risk, specifically reviewing the Risk Management Policy and recommending it to the Board for approval. The Committee should have risk management as a standing agenda item at its meetings and should exchange information with the Board, Internal Audit and the Chief Risk Officer regarding the effectiveness of the risk management framework</p> <p>The Audit Committee should:</p> <ul style="list-style-type: none"> <li>▪ Review risk reports and monitor the effectiveness of risk management</li> <li>▪ Approve the Risk Based Internal Audit Plan</li> <li>▪ Provide guidance to the Internal Audit function focusing on key areas for review</li> </ul>
<b>Internal Audit</b>	<p>Internal Audit should:</p> <ul style="list-style-type: none"> <li>▪ Provide objective assurance to the Board on the effectiveness of organisation risk management</li> <li>▪ Help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively</li> </ul>

**Appendix A – Risk Notification Template**

Note(s) for use:

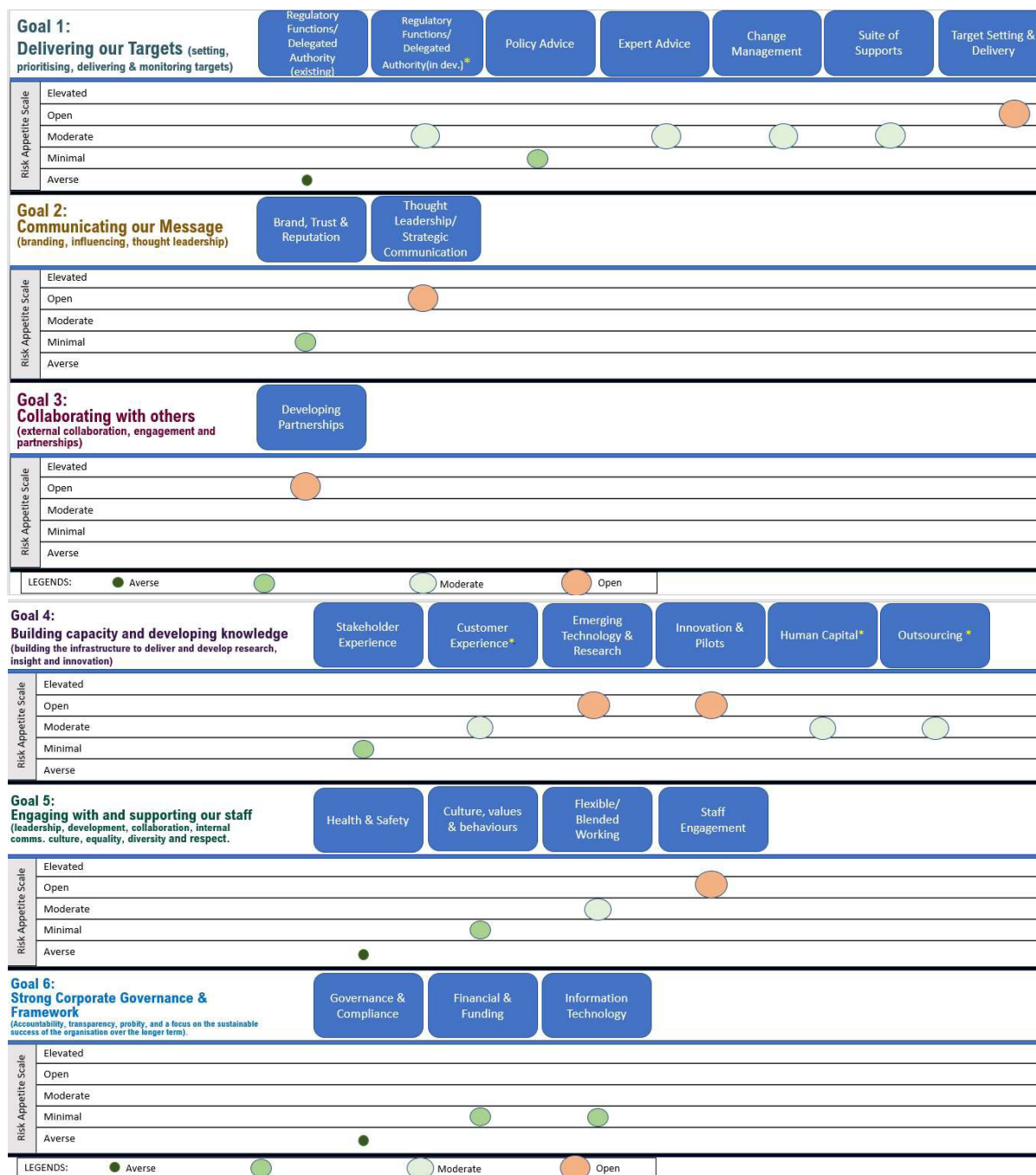
For any proposed new risks or proposed amendments to existing risks, both Table 1 and Table 2 (rationale for new risk/change to existing risk) must be completed in full.

b) For any proposal to remove a risk from the organisation level risk register, please only complete Table 2 and provide the risk number, risk description and rationale for the proposed removal.

Risk Category	Risk description	Risk Owner(s)	Controls	Residual Risk Rating			Actions Required	Action Owner	Deadline for actions
				Score (based on a scale 1-5 Rating Scale).	Score (based on a scale 1-5 Rating Scale).	Each risk is assessed as either Low, Medium or High based on plotting its Likelihood and Impact on the Rating Matrix			
As per the SEAI Risk Framework	Description of risk item using the format:	Nominated SEAI lead responsible that has been given the authority to manage a particular risk and is accountable for doing so.	The controls in place to manage/ minimise the risk.				The remedial actions Nominated SEAI lead responsible for coordinating/ implementing agreed upon remediation activities.		Timeline which the actions are required to be completed by.
X due to Y, resulting in Z.									

Rationale for proposed change (i.e. new risk/risk amendment/risk removal) :

## Appendix B Maximum Risk Appetite Framework Heat Map on a page



## Appendix C - Level 2 Risk Taxonomy Definitions

Level 2 Risk Taxonomy Category	Definition
Strategic - Strategic Mandate	Risk of change in priorities of Govt/DECC, new EU legislative changes, shared/overlapping interests across DECC and DETE.
Strategic - Strategic Delivery Risk	Risk of the inability of SEAI to deliver key capital programmes and responsibilities.
Strategic - Erroneous policy or expert advice	Risk of provision of erroneous policy/expert advice and/or not reaching to SEAI's target group and/or stakeholders, failure to engage or follow through (including risk from incorrect model usage).
Strategic - Inadequate design or insufficient range of grant schemes	Risk of failure to deliver an evolving and comprehensive suite of grant/funding supports for homes/communities/business/industry and the public sector.
Governance & Compliance - Regulatory compliance	Failure to comply with statutory, legal, regulatory, contractual obligations.
Governance & Compliance - Legal risk	Any risk of court action occurring whether domestic, European, or international.
Governance & Compliance – Regulatory Functions/Delegated Authority	<p>Risks arising from SEAI's inability to deliver regulatory functions and delegated functions (listed below) on behalf of Ireland:</p> <ul style="list-style-type: none"> <li>- Regulatory Functions: EPBD, EEOS (article 7), Triple-E, EED (article 8), RED Renewable Installer Register, Public Sector reporting M&amp;R., Biomass Sustainability Certification</li> <li>- Delegated Authority: Market Surveillance for energy labelling regulations and eco-design, EPBD-BER Publications</li> <li>- Delegated Functions (of minister): EEOS (per regs), Single point of contact for renewable energy consenting (including risk from incorrect model usage)</li> </ul>
Financial and Funding - Financial Management	Failure to maintain effective financial management and accountability arrangements in all activities (including inappropriate tracking of the drawdown and inaccurate reporting to DECC or other funders on the drawdowns).
Financial and Funding - Fraud, Bribery and Corruption	Fraud generally means deceitful misrepresentation of facts to commit or conceal a crime. Theft, misappropriation or unauthorised use of SEAI time, funds, property or other assets, which may or may not also involve misstatement of financial documents or records to conceal the theft or misuse". It usually involves the obtaining of money or services to which a person is not entitled. False and/or forged documents are often used in these types of activities.

Level 2 Risk Taxonomy Category	Definition
	<p>Bribery is offering, promising, giving, accepting or agreeing to accept any financial or other advantage to someone in business or government in order to obtain or retain a commercial advantage, or to influence another person to act improperly in carrying out their duties or to reward another person for acting improperly</p> <p>Corruption can be broadly defined as the abuse of entrusted power for private gain. Corrupt activity can be engaged in by private individuals, public officials and businesses.</p> <p>Corruption (or acting corruptly) includes acting with an improper purpose personally or by influencing another person, whether by means of making a false or misleading statement, by means of withholding, concealing, altering or destroying a document or other information, or by any other means. Corruption can take many forms including conflicts of interest, undue influence and the giving and taking of bribes.</p> <p>Refer to the Anti Bribery, Fraud and Corruption policy for details.</p>
Financial and Funding - Credit Risk (includes financial concentration risk)	Counterparty risk refers to the likelihood that a transactor might default on its contractual obligation for e.g., default by energy show partners, BER assessors (registration fees, BER publication fees) or inability to claw back grant amount.
Financial and Funding - Liquidity Risk	The risk of unavailability of, or delays in, letters of allocation from DECC/DoT and/or mismatch between forecasted cash needs and actual cash requirement.
Brand, Reputation & Trust - Reputational risk	Risk of negative publicity, diminished public perception or uncontrollable events.
Operational - People risk	Risk of a gap in achieving the People Strategy Ambitions. This includes conduct risk, risk of having inadequate resources, untrained staff, high attrition rates, inadequate policies and procedures.
Operational - Business continuity	<p>Risk of external crisis that interrupts business delivery excluding IT infrastructure crisis.</p> <p>Business continuity focuses on keeping business operational during a disaster.</p>
Operational - Outsourcing/third party vendor	Risk of failure to deliver SEAI objectives (process, governance, service) in outsourced delivery model as a result of poor-quality management and oversight arrangements of outsourced providers, key service providers going out of business or not commercial arrangement, leading to

<b>Level 2 Risk Taxonomy Category</b>	<b>Definition</b>
	reputational damage and operational exposure. Applies to vendors, BPO, Managing agents etc.
Operational - Change management	Risk of poorly selected, initiated, designed/implemented changes with a negative impact on the achievement of strategic objectives.
Operational - Stakeholder Experience	Risks of failure to understand our Stakeholders requirements (DECC, DoT, Government Depts) including adherence to the PDA with DECC and responding appropriately in a timely manner.
Operational - IT Systems Risk	Risk of failure to provide a stable, fit for purpose, secure, scalable, adequately controlled IT infrastructure, and IT business applications. This risk includes disaster recovery which focuses on restoring data access and IT infrastructure after a disaster.
Operational - Information Security (including Cyber Security)	Risk of unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. Or Threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate.
Operational - Data Management	Risks associated with data processing including the practice of collecting, organising, and accessing data to support productivity, efficiency, and decision-making.
Operational - Developing Partnerships	Risk of not being able to effectively engage with different types of stakeholders.
Operational – Supply Chain	Risk that the supply chain will not be able to scale up sufficiently to meet increasing demand, thus restricting SEAI in the delivery of its strategic objectives and/or higher dependency & SEAI exposure to certain OSS Companies, Contractors and/or Project Co-Ordinators. Risk of capacity constraints in the public sector to engage with SEAI public sector programmes.
Operational - Customer experience	Risk of delivering negative customer experiences.
Operational - Concentration Risk (Contractor/Installer/Customer)	Dependency on a single/small number of contractor(s)/installer(s) to deliver for specific programme(s)
Macro Risks - economic	Macro risks refer to the external risks. Economic risk emanates from changes in Interest rates or exchange rates, recession, inflation, taxes, and changes in demand and supply.



<b>Level 2 Risk Taxonomy Category</b>	<b>Definition</b>
Macro Risks - socio-political	Macro risks refer to the external risks. Socio-political risks might emanate from social unrest, nationalistic rhetoric, riots, demonstrations, or small-scale terrorist movements.
Macro Risks - environmental	Macro risks refer to the external risks. Environmental risks refers to the impact of a changing climate, including more frequent extreme weather events and gradual changes in climate, as well as of environmental degradation, such as air, water and land pollution, water stress, biodiversity loss and deforestation.

## Appendix 14 Data Protection Policy

(Approved by the Board on 27 March 2024)



### DATA PROTECTION POLICY

#### Document Information

<b>Title:</b>	<b>Data Protection Policy</b>
<b>Target Audience:</b>	SEAI data subjects, including SEAI employees, customers, stakeholders and third-party service providers (where relevant)

#### Document Version History

Version No.	Author	Date	Description
v.2	Fiachra Barrett	15/06/2020	Significant policy update (GDPR)
v.3	Mary McDonald	23/02/2024	Policy updates

## Contents

1.	Introduction .....	3
1.1	Personal Data Management .....	3
1.2	Purpose of this Policy .....	3
1.3	Policy Review, Approval and Continuous Improvement.....	4
1.4	Scope and Constraints.....	4
1.5.	DEFINITIONS.....	4
2.	Roles and Responsibilities.....	4
2.1.1	SEAI Board .....	4
3.	How SEAI complies with the Data Protection Principles .....	8
4.	International Transfers.....	12
5.	Individual Rights.....	12
5.2	Data Rectification (Article 16) .....	13
5.3	Data Erasure (“Right to be forgotten”) (Articles 17 & 19) .....	14
5.4	Restriction of Processing (Articles 18 & 19).....	14
5.5	Data Portability (Article 20) .....	15
5.6	Exemptions.....	15
5.7	Right to object to Data Processing.....	16
6	Information and Cyber Security .....	17
6.1	Data Protection by Design and by Default.....	17
6.2	Regular Risk Assessment.....	18
6.3	Data Protection Impact Assessment (DPIA).....	18
7.2	What are SEAI’s requirements in the use of Data Processors and how do we comply with them?.....	19
7.3	Evaluation of processors and pre-processing Agreements.....	20
7.4	What are our requirements as Data Controller and how must we comply with them? .....	20

# 1. Introduction

---

## 1.1 Personal Data Management

In performing its functions and day-to-day activities, SEAI is required to process significant amounts of **"Personal Data"**. Data is essential to the administrative business of SEAI. Data is also necessary for research and analysis purposes. In collecting Personal Data, SEAI has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of the organisation. In striking this balance the necessity and proportionality of the processing activity will be considered.

This Data Protection Policy (the **"Policy"**) sets forth SEAI's commitment to protecting the rights and privacy of individuals in accordance with applicable data protection law.

On 25 May 2018, the General Data Protection Regulation 2016/679 (GDPR) came into effect and replaced the existing data protection regimes in place throughout the European Union (EU), including Ireland. The GDPR is supplemented by the Data Protection Acts 1988 to 2018 (DPA) (together referred to as the "data protection legislation").

For the purposes of the GDPR, SEAI is a "Data Controller" in respect of certain Personal Data relating to its clients, its employees and others as it controls the contents and use of such Personal Data provided to SEAI or requested by SEAI. In other circumstances, SEAI may be a joint Data Controller or a Data Processor.

## 1.2 Purpose of this Policy

This Policy provides a framework for protecting Personal Data, maintaining and improving compliance with data protection requirements and good practice.

The aim of this Policy is to ensure that everyone handling Personal Data is fully aware of the requirements and acts in accordance with data protection procedures.

The purpose of this document is to provide a statement of overall intentions and directions of SEAI for managing compliance with data protection requirements and good practice.

The objectives of the Data Protection Policy are to:

1. enable SEAI to meet its own requirements for the management of Personal Data;
2. ensure SEAI meets applicable statutory, regulatory, contractual and/or professional duties;
3. create a high level of awareness of Personal Data issues, thereby enabling staff to both respect the Personal Data of data subjects and treat this information properly;
4. protect the interests of individuals and other key stakeholders;
5. empower staff to identify the uses of Personal Data and any issues of concern;
6. ensure compliant and best practice data protection operations within SEAI whilst ensuring compliance with the legal and statutory requirements under relevant legislation;
7. support organisational objectives and obligations, and
8. establish appropriate controls in line with SEAI's acceptable level of risk.

This document also highlights key data protection procedures within SEAI.

### 1.3 Policy Review, Approval and Continuous Improvement

In line with best practice, this Policy has been approved by SEAI's Board with a commitment to continually improve SEAI Personal Data practices. This document will be reviewed biennially to ensure its continued relevance to current and planned operations, legal developments, legislative obligations, and Data Protection Commission ("DPC") guidance. Any queries in relation to Data Protection should be directed to [dataprotection@seai.ie](mailto:dataprotection@seai.ie).

### 1.4 Scope and Constraints

This Policy applies to all Personal Data including sensitive personal data (special category data) captured, processed or stored by SEAI, regardless of the media on which the Personal Data is stored (paper-based, electronic or otherwise).

This policy applies to:

- Any person who is employed by SEAI, either directly or indirectly who receives, handles or processes personal data in the course of their employment.
- Any agent, contractor, researcher or individual who receives, handles, or processes personal data for or on behalf of SEAI for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process personal data on behalf of SEAI.

It should be noted that if Personal Data is flowing between SEAI departments, each department will be subject to the same legal and data protection responsibilities. Effectively, departments within SEAI must all comply with standard data protection requirements and adhere to the principles of data protection law if sharing personal data with another department.

### 1.5. Definitions

See Appendix 1 for definitions used in this Policy.

## 2. ROLES AND RESPONSIBILITIES

---

### 2.1.1 SEAI BOARD

The Board is responsible for ensuring that management operate a system of control designed to ensure compliance with GDPR obligations. That responsibility extends to reviewing and approving this policy and any updates to it.

### 2.1.2 Everyone in the Organisation

**Everyone in the organisation** is responsible for ensuring compliance with SEAI's data protection requirements and obligations. It is the responsibility of all employees and contractors of SEAI to ensure that:

1. they familiarise themselves with this Policy and handle Personal Data in accordance with the principles and provisions of data protection legislation and this Policy;
2. they familiarise themselves with and adhere to the requirements of all related SEAI data protection procedures, for example; reporting data breaches, identifying data subject's rights requests etc.;
3. they complete the mandatory data protection training provided;

September 2024 SEAI

4. queries in relation to Personal Data are promptly and courteously dealt with in line with the provisions of this Policy. When an employee receives an enquiry about the handling of Personal Data, they will know what to do, and/or where to refer it.

### **2.1.3 Additional responsibilities of Data Protection Officer**

As SEAI is a public body, it is mandatory that a suitably trained, independent, senior staff member is appointed to the role of Data Protection Officer. This may be performed as a team function provided a single individual is the lead person in charge and roles within the Data Protection Officer team are clearly defined.

Within SEAI, our Data Protection Officer may be contacted at [dataprotection@seai.ie](mailto:dataprotection@seai.ie).

The responsibility of the Data Protection Officer function within SEAI is to:

1. Respond to individuals (Data Subjects) whose data is processed on all issues related to the processing of their data and the exercise of their data protection rights.
2. Cooperate with the Supervisory Authority (Data Protection Commission (DPC)), and act as the organisation's contact point for the DPC on all issues related to the processing of Personal Data in SEAI.
3. Inform and advise SEAI and its employees of their obligations pursuant to data protection legislation and associated privacy legislation.
4. Monitor compliance with the data protection legislation and privacy legislation, in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and any related audits.
5. To provide advice and assistance regarding the requirement to perform Data Protection Impact Assessments and monitor their performance.
6. Arrange annual data protection training sessions for employees.
7. Maintain a log of all data breaches and communication of breaches to all relevant parties when required to do so (Supervisory Authority, controllers, and Data Subjects).
8. Ensure that SEAI maintains relevant Records of Processing Activities (ROPAs).
9. Review and keep this Policy and related policies, procedures and Privacy Notices up to date, including taking cognisance of relevant developments and identifying significant trends.
10. Promote a culture of compliance with data protection legislation and associated privacy legislation.

To allow for the effective performance of the Data Protection Officer's tasks, SEAI will ensure:

1. The Data Protection Officer will be suitably trained and have expert knowledge of Data Protection legislation.
2. SEAI will support the Data Protection Officer in performing the tasks above by providing resources necessary to carry out those tasks. The key to this is to provide sufficient time, finance and staff where appropriate to enable the Data Protection Officer to fulfil their duties.
3. That no tasks and duties result in a conflict of interests for the Data Protection Officer.
4. That SEAI senior management will take steps to ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data and will be in a position to perform their duties and tasks in an independent manner. This includes:

- a. The Data Protection Officer has a dotted reporting line to the CEO and also to the SEAI Board, through the Audit and Risk Committee.
- b. The Data Protection Officer's involvement will be sought where decisions with data protection implications are taken. All relevant information must be passed on to the Data Protection Officer in a timely manner in order to allow him or her to provide adequate advice.
- c. Where appropriate, the Data Protection Officer will be invited to participate in meetings with senior and middle management.
- d. The opinion of the Data Protection Officer will always be given due weight.
- e. The Data Protection Officer will be promptly contacted if a data breach or other data protection incident has occurred.

#### **2.1.4 Additional responsibilities of Human Resources**

SEAI Human Resources (HR) collect and process significant amounts of personal data and special category data on prospective and current employees and, in some instances, may also continue to process personal data of former employees. This personal data can range from basic information such as names, addresses and PPSNs, but can also include more sensitive information on occupational health, sick leave, trade union membership, performance reviews or disciplinary actions. HR personnel must be mindful of their responsibilities, obligations and duties under data protection legislation. Responsibilities of HR include:

1. Ensuring all new members of staff are made aware of this Policy document at induction stage and that Data Protection responsibilities are referenced in staff Terms and Conditions and Role Descriptions.
2. Ensuring that SEAI's data protection management platform is updated on staffing changes. In particular, HR will keep the platform updated with:
  - new staff members joining SEAI
  - staff members leaving SEAI
  - staff members changing jobs or departments within SEAI.
3. Handling all employee-related Personal Data in accordance with this policy, the data protection principles, and data handling rules.
4. Ensuring that any sensitive or special category data is processed in accordance with data protection principles and adequately safeguarded.

#### **2.1.5 Additional responsibilities of Executive Leadership Team (SEAI Chief Executive Officer and Management at Director level)**

The Executive Leadership Team (ELT) is responsible for ensuring SEAI implements appropriate technical and organisational measures to ensure and to be able to demonstrate that any processing of Personal Data is performed in accordance with the GDPR. The ELT also has responsibility for:

1. Ensuring SEAI, as a Public Body, has a Data Protection Officer in place as mandated by the GDPR.
2. Providing leadership on data protection matters for their functional area.
3. Providing oversight and monitoring compliance of data protection issues in their respective areas of responsibility.
4. Allocating resources as necessary to deal with data processing in a compliant manner.
5. Ensuring staff in their functional areas are trained in GDPR obligations.

6. Ensuring systems are in place for managing risks and prompt reporting of data protection breaches in their functional area.

### **2.1.6 Additional responsibilities of Heads of Departments and Programme Managers**

Heads of Departments and Programme Managers have a key role in the implementation of this Policy which includes responsibility for:

1. Ensuring all processing within their department/team is carried out in compliance with the provisions of this Policy.
2. Maintaining the Records of Processing Activities for all Personal Data processed by their department/team.
3. Ensuring that staff in their area are operating in line with this Policy.
4. Ensuring reporting staff complete the mandatory data protection training.
5. Ensuring sufficient resources are available to support the effective implementation of this Policy.
6. Ensuring appropriate technical and organisational security measures are in place in areas for which they are responsible. Specifically, security risk assessments will be undertaken to check that the Personal Data is sufficiently protected in line with SEAI security standards and policies. Where relevant, security risk assessments will be commissioned regularly, and evidence retained for audit purposes. To deal with appropriate technical and organisational security measures, the Head of Department/Programme Manager may delegate security tasks, in full or partially, to another appropriate SEAI representative. This delegation does not exempt the Head of Department/Programme Manager from their responsibility, and they must make sure that the delegated jobs have been carried out correctly.
7. Ensuring data privacy risks are appropriately managed within their function and specifically, to ensure the handling of Personal Data is regularly assessed and evaluated. It is important that if any new projects are being considered then Data Protection needs to be built in at the beginning (Data Protection by design and default).
8. Ensuring that for any project, programme or proposal within their function that will involve the processing of Personal Data, that data protection considerations are assessed and where required, a Data Protection Impact Assessment is carried out (see section 6 for more details on Data Protection Impact Assessment). The SEAI Data Protection Officer must be informed and involved at an early stage.

Ensuring that appropriate systems are in place to respond to Subject Access Requests relating to Personal Data processed within their departments, enabling staff to identify, extract, review and prepare for the release of such information as required.

#### *Additional responsibilities of SEAI Project Managers*

Ensure that data protection principles are applied as part of any changes and managed projects within SEAI. This includes implementation of appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individuals' rights, for example, pseudonymising data to comply with the principle of data minimisation. This is known as Data Protection by design and by default.

### **2.1.7 Data Champions**

SEAI has nominated Data Protection Champions for co-ordinating Data Protection compliance matters for their area. The Data Protection Champions will act as a point of contact for SEAI's Data Protection Officer,



bringing relevant Data Protection matters to the attention of staff in their area and assisting in the maintenance of the Record of Processing Activities related to their area.

## **2.2 Data Security Awareness/Data Protection Training Details**

Data Protection training is mandatory for all SEAI employees and will be arranged by the Data Protection Officer. All SEAI staff are required to complete this training annually and the Data Protection Officer will maintain a record for audit purposes.

IT Security Awareness training is mandatory for all SEAI employees and will be arranged by the IT Manager. All SEAI staff are required to complete this training annually and the IT Manager will maintain a record for audit purposes.

## **3. How SEAI complies with the Data Protection Principles**

---

SEAI is committed to ensuring all Personal Data is processed in line with the principles and good practices set out in GDPR.

SEAI is obliged to comply with the data protection principles set out in the GDPR as outlined below.

### **3.1 “Lawfulness, Fairness and Transparency”**

*Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.*

SEAI is committed to ensuring the lawful, fair and transparent collection of data. Our Records of Processing Activities (RoPAs) record all information processed, including the lawful basis of the types of processing. In addition, our privacy notices provide details to the Data Subject in a concise, transparent, intelligible and easily accessible form including the purposes of processing, the duration of processing, their rights, and lawful basis for the processing. These privacy notices must be provided to Data Subjects **prior to** collecting Personal Data regardless of the collection method (phone, CCTV, forms, interview, website etc.).

To **fairly obtain** data the Data Subject must, at the time the Personal Data is being collected, be made aware of:

- the identity of the persons collecting it;
- the purpose of collecting data;
- the persons or categories of persons to whom the data may be disclosed; and
- any other information which is necessary so that processing may be fair.

**Lawful basis for processing Personal Data:** In order to process Personal Data SEAI must have a lawful basis for doing so. The lawful grounds for processing Personal Data are set out in Article 6 of the GDPR. These are:

- the consent of the individual;
- performance of a contract;
- compliance with a legal obligation;
- necessary to protect the vital interests of a person;
- necessary for the performance of a task carried out in the public interest;
- or in the legitimate interests of the organisation (except where those interests are overridden by the interests or rights and freedoms of the Data Subject).

As a public body, SEAI cannot rely on legitimate interest as a legal basis for processing personal data in the performance of its official tasks.

SEAI will avoid all processing of Special Categories of Personal Data where possible. It is understood that certain business activities within SEAI require the processing of Special Categories of Personal Data (e.g. processing of data concerning health). The *general* processing of Special Categories is prohibited in SEAI, and in the rare instance it is required, Heads of Departments must ensure all processing is defined in the Record of Processing Activities (RoPA), along with an appropriate legal basis (reference 1, Art 6), and derogation (reference 2, Art 9) for processing of such Special Categories recorded within the Record of Processing Activities (RoPA).

### **3.2 Where the lawful basis is “consent”**

Article 7 of the GDPR sets out the conditions needed for consent as a legal basis for data processing to be valid. It is necessary to consider whether consent is freely given, and the Data Subject must have the opportunity to withdraw consent for processing at any time. Consent should not be assumed and must be obtained before data processing begins.

Where the lawful basis of processing is based on consent, SEAI shall incorporate procedures that will ensure that where the consent is withdrawn, that processing based on that consent will cease. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Specifically, where other departmental requirements or legislation require explicit consent (e.g. for marketing), the departments shall have procedures for collecting and managing this consent. The department will monitor all requests for removal or withdrawals of consent, maintain a register of all such requests and ensure that all removals are completed without undue delay.

### **3.3 “Purpose Limitation”**

*Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

SEAI is committed to only collecting and processing information for an explicit purpose.

It is unlawful to collect information about people routinely and indiscriminately, without having a clear and legitimate purpose for so doing. Any individual has the right to question the purpose for which SEAI holds their data and SEAI must be able to identify that purpose.

All information processed, along with the business purpose, is detailed within the Record of Processing Activities (RoPA), which will be reviewed and updated annually or when any significant changes occur in the information processed, where it is processed or with whom it is shared.

Personal Data will only be processed for the defined purpose(s). All requests for changes to the use or processing of Personal Data must be compatible with the original purpose for processing.

Secondary or future uses, which might not be obvious to Data Subjects should be brought to their attention at the time of obtaining Personal Data. Data Subjects should be given the option of saying whether or not they wish their information to be used in these other ways.

Where SEAI holds information about individuals and wish to use it for a new purpose (which was not

disclosed at the time the information was collected and has been assessed as incompatible with the original purpose), then consent will be sought from the Data Subjects on whether or not they wish their information to be used for the new purpose. SEAI will inform data subjects of the new purpose and legal basis and give them the option to withdraw from the processing, if practical. Fairness of the new processing will be a prime consideration. In the absence of prior consent, an assessment of compatibility with the original purpose of processing will be undertaken and documented in advance of further processing of the Personal Data.

SEAI processes Personal Data provided to it only for the purposes of fulfilling its objectives and complying with its statutory obligations.

Note: Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the Regulations, not be considered to be incompatible with the initial purposes ('purpose limitation'). Further processing is subject to the implementation of appropriate technical and organisational measures. Please refer to SEAI Data Protection Officer if you wish to use the data for any of these further processing activities.

### **3.4 "Data Minimisation"**

*Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

SEAI is committed to only collecting and processing appropriate information to the extent needed to fulfil our operational and service needs and to comply with all applicable statutory, regulatory, contractual and/or professional duties.

The Personal Data SEAI keeps should be enough to enable it to achieve its purpose(s), and no more.

SEAI is not entitled to collect or keep Personal Data that it does not need, "just in case" a use can be found for the data in the future.

Data will be minimised and protected through SEAI's Data Protection Impact Assessment (DPIA) procedure, and in line with SEAI's commitment to Data Protection by design and default.

### **3.5 "Accuracy"**

*Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

SEAI is committed to taking all reasonable efforts to ensure the accuracy of our data. This will be enforced through our Data Protection Impact Assessment and Data Protection by Design and Default procedures.

### **3.6 "Storage Limitation"**

*Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.*

SEAI as a Data Controller must be clear about the length of time for which Data will be kept and the reason why the information is being retained. If there is no good reason for retaining Personal Data, then that Data should be routinely deleted. Data should never be kept "just in case" a use can be found for it in the future.

Personal data will only be held for as long as the purpose for which it was collected remains. If that purpose ceases, the Personal Data should be deleted or anonymised to remove any identifying characteristics if it is desired to use the information for another purpose such as research.

SEAI documents the required data retention periods along with justification and action to be taken when the retention period expires in its Records Retention Policy. This document outlines the retention period for all Data retained by SEAI, including Personal Data, and what will occur when the retention period expires. It applies to all Personal Data regardless of the media on which it is stored (paper-based, electronic, audio or otherwise). The Retention Policy helps ensure SEAI is maintaining the necessary Personal Data for an appropriate length of time, based on legal and business requirements and in line with the data protection 'storage limitation' principle. Everyone is responsible for ensuring this Policy is adhered to.

### **3.7 "Integrity and Confidentiality"**

*Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

SEAI is committed to protecting and not disclosing Personal Data, either within or outside of SEAI to any unauthorised recipient. Everyone is responsible for protecting against the accidental loss, destruction of or damage to Personal Data regardless of the media on which it is stored (paper-based, electronic, or otherwise).

SEAI's basic standards of security include:

- Access to information is restricted to authorised staff on a "need-to-know" basis;
- Personal information held in manual files is secured in locked filing cabinets;
- All waste papers, printouts, etc. are disposed of in a careful and secure manner;
- Premises are secure when unoccupied;
- Contracts are put in place with data processors which impose equivalent security obligations on the data processor;
- All reasonable measures have been taken to ensure that all staff are made aware of the IT security measures in place through circulation of SEAI's IT Security policy and training;
- Computer systems are password protected;
- Back-up procedures are in operation for computer held data;
- Information on computer screens and paper files is hidden from callers to offices;
- Personal Data is protected by strong encryption when being stored on portable devices or transferred electronically (including via email);
- Personal Data is not stored on portable devices except in essential circumstances. Where deemed essential, the data must be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements should be in place to fully delete the data on the portable device when it is no longer being used;
- Appropriate facilities are in place for disposal of confidential waste;
- A policy of non-disclosure of personal security passwords to any other individual (including other employees within the organisation);
- Keeping audit logs in relation to read access, changes, additions, deletions on ICT systems;

- Having adequate security measures and policies in place in relation to the use of laptops and other mobile storage devices.
- Strict access controls and permissions such as least privilege are implemented. Least privilege is a concept in which a user is given the minimum levels of access or permissions needed to perform their job.

Refer to SEAI IT / Information Security Team, for further guidance, clarification and consultation in relation to data security.

## 4. INTERNATIONAL TRANSFERS

---

SEAI engages with businesses and service providers in multiple locations for many purposes. The transfer of Personal Data from SEAI to controllers and processors located outside the EU in third countries must not undermine the level of protection of the individuals concerned, with a third country being any country outside the European Economic Area (the "EEA"). Therefore, transfers to third countries or international organisations shall only be done in full compliance with Chapter V of the GDPR, by way of an adequacy decision, having appropriate safeguards in place or by relying on a derogation.

## 5. INDIVIDUAL RIGHTS

---

All SEAI Data Subjects have rights in relation to the Personal Data which SEAI process on their behalf. For information to be Personal Data, it must *relate to* a living individual and allow that individual to be *identified* from it (either on its own or along with other information in, or likely to come into SEAI's possession).

Requests to exercise their rights may be received from any individual, including members of staff, with whom SEAI has had dealings and about whom SEAI holds data. This will include information held both electronically and manually. The Data Subject should be referred to the Data Protection Officer for all requests to exercise their rights.

The rights of individuals with respect to their Personal Data are explained in this section which also sets out what SEAI must do to comply with its duties as a Data Controller.

The following are the applicable Data Subject Rights:

- Data subjects will be able to request to access the data SEAI holds on them through a Subject Access Rights Request (SAR) (Right of Access);
- Data subjects can request to change or correct any inaccurate data (Right to Rectification);
- Data subjects can request to delete data that SEAI holds (Right to Erasure (sometimes referred to as the Right to be Forgotten));
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to have their data moved outside of SEAI if it is in an electronic format (Right to Data Portability);

- Data subjects can object to a decision made by automated processing and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

The following sections provide more information about the rights of data subjects.

## **5.1 Subject Access Requests (Article 15)**

Data Subjects (including employees and the general public) have the right to access Personal Data held about them. This includes factual information, expressions of opinion (other than an expression of opinion about the data subject given in confidence or on the understanding that it would be treated as confidential), irrespective of when the information was recorded.

The Data Subject shall have the right to obtain confirmation from SEAI as to whether or not Personal Data concerning him or her are being processed, and where that is the case, access to the Personal Data and to the following information:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient to whom the Personal Data have been or will be disclosed;
- where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- where the Personal Data are not collected from the Data Subject, any available information as to their source;
- recipients in third countries or international organisations;
- where Personal Data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 25 relating to the transfer.

SEAI shall provide a copy of the Personal Data undergoing processing in accordance with data protection legislation. For any further copies requested by the Data Subject, SEAI may charge a reasonable fee based on administrative costs. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to above shall not adversely affect the rights and freedoms of others.

### *Requests made about or on behalf of other individuals*

A third party, e.g. solicitor, may make a valid Subject Access Request on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individual's consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney, must be provided by the third party.

Where there is a concern around sharing the information with a third party, the response may be sent directly to the Data Subject. The individual may then choose to share the information with the third party after having had a chance to review it.

## **5.2 DATA RECTIFICATION (ARTICLE 16)**

Data Subjects (including employees and the general public) have the right to the rectification of inaccurate Personal Data concerning him or her. This applies if data is inaccurate or misleading to a matter of fact. Data Subjects are also entitled, taking into account the purposes of processing, to have incomplete Personal Data completed.

SEAI must respond to such a request and where necessary take steps to validate the information provided by the Data Subject to ensure that it is accurate before amending it.

This is not an absolute right and restrictions apply. For example, it does not apply to witness statements or opinions of others such as assessors etc. The Data Subject should be referred to the Data Protection Officer for all requests under the "Right to Rectification".

If SEAI has to rectify Personal Data, SEAI must also notify any one to whom it has disclosed such data, unless this would be impossible or involve disproportionate effort.

## **5.3 DATA ERASURE ("RIGHT TO BE FORGOTTEN") (ARTICLES 17 & 19)**

Data Subjects (including employees and the general public) have the right to request from the controller the erasure of Personal Data concerning him or her in specified circumstances including where there is no longer a legal ground for processing of the information. This is also known as the "right to be forgotten".

This is not an absolute right and restrictions apply. The Data Subject should be referred to the Data Protection Officer for all requests under the "Right to Erasure".

Data Subjects have the right under Article 17 of the GDPR to have their data 'erased' in certain specific situations – essentially where processing fails to meet the requirements of GDPR. SEAI must respond to such a request without undue delay and in any event within one month, although this can be extended in certain circumstances.

If SEAI has to erase Personal Data SEAI must also notify any third parties to whom it has disclosed such data unless this would be impossible or involve disproportionate effort.

*Data made available in the public domain*

If SEAI has made Personal Data public, and where it is obliged to erase the data, SEAI must also inform other controllers who are processing the data that the Data Subject has requested erasure of those data.

The obligation is to take reasonable steps and account must be taken of available technology and the cost of implementation.

## **5.4 RESTRICTION OF PROCESSING (ARTICLES 18 & 19)**

Data Subjects (including employees and the general public) have the right to request the restriction of processing, of his or her Personal Data as an alternative to erasure. The Data Subject should be referred to the Data Protection Officer for all requests under the "Right to Restrict Processing".

SEAI is required to ensure it complies with its obligations under Article 18 of the GDPR, and in so doing note that:

- Individuals have a right to 'block' or suppress processing of Personal Data.
- When processing is restricted, you are permitted to store the Personal Data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.

*What is meant by restriction?*

Under GDPR if Personal Data is 'restricted', then SEAI may only store the data. It may not further process the data unless:

- The individual consents; or
- The processing is necessary for establishment or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (Union or Member State) public interest.

If the data have been disclosed to others, then SEAI must notify those recipients about the restricted processing (unless this is impossible or involves disproportionate effort).

## **5.5 DATA PORTABILITY (ARTICLE 20)**

Data Subjects (including employees and the general public) have the right under Article 20 of GDPR to receive Personal Data concerning him or her, in a structured, commonly used and machine-readable format, and to transmit that data to another controller without hindrance from the controller which provided the Personal Data. The right only applies to Personal Data that a Data Subject has provided to SEAI, and where the Personal Data is processed automatically and is processed based on the legal basis of consent or performance of a contract.

SEAI must respond to such a request without undue delay and in any event within one month, although this can be extended in certain circumstances.

There are also limitations to that right. The Data Subject should be referred to the Data Protection Officer for all requests under the "Data Portability Right".

The subject access right provided under the GDPR already gives individuals the right to require their data to be provided in a commonly used electronic form, but Data portability goes beyond this and requires the controller to provide information in a structured, commonly used and machine-readable form so that it may be transferred by the Data Subject to another data controller where it is technically feasible to do so.

## **5.6 EXEMPTIONS**

There are a limited number of exemptions in place in relation to certain Data Subject Rights. It may sometimes be prudent for SEAI to rely on such exemptions and not to adhere to certain individual rights. The Data Protection Officer will consider each request on a case-by-case basis to determine if an exemption applies. Where an exemption does apply, it is likely that such exemptions would not apply to the complete data set and more likely to a restricted and very specific set of Personal Data. For example, SEAI may not be permitted to apply a blanket exemption to the right of access to an entire grant claim file as some elements may be considered privileged.



If SEAI wishes to withhold certain subject rights, this must be referred to the Data Protection Officer who may refer to legal counsel.

#### *GDPR Exceptions to Subject Access Requests*

GDPR allows for Union or Member State law to restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 (Rights of the Data Subject) and Article 34 (Communication of a Personal Data Breach to the Data Subject) , as well as Article 5 (Principles relating to processing of Personal Data) in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.

Article 23, by setting out an exhaustive list of requirements which must be met to lawfully impose a restriction, confirms that any measure used to restrict the rights of a Data Subject must be of limited scope and applied in a strictly necessary, proportionate and specific manner.

### **5.7 RIGHT TO OBJECT TO DATA PROCESSING**

Data Subjects have the right to object to certain types of processing of Personal Data where this processing is carried out in connection with tasks:

- in the public interest,
- under official authority, or
- in the legitimate interests of others.

In all instances where a data subject submits a written objection to their Personal Data being processed by SEAI, these objections are to be referred to the Data Protection Officer. The Data Protection Officer will review and respond to all such objections. SEAI can refuse to comply with a Data Subject's objection to Data Processing where SEAI can prove a strong reason to continue processing their data which overrides their objection.

Data Subjects have a stronger right to object to the processing of their personal data where the processing relates to direct marketing.

## 6 INFORMATION AND CYBER SECURITY

---

The GDPR requires SEAI to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and then to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- a) the pseudonymisation and encryption of Personal Data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

SEAI fulfils these obligations by a number of means, specifically:

1. Deployment of Data Protection by design and by default within our Project Management Lifecycle for all new systems/changes to processing (reference Section 6.1 for further details)
2. Regular Risk Assessments/testing to assess and evaluate the effectiveness of technical and organisational measures on existing processing (reference Section 6.2 for further details)
3. Formalised Data Protection Impact Assessments where processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" and/or "*processing on a large scale of special categories of data*". (reference Section 6.3 for further details)

Records of all of the above activities will be forwarded to the SEAI Data Protection Officer and retained for audit purposes.

### 6.1 DATA PROTECTION BY DESIGN AND BY DEFAULT

SEAI has an obligation under GDPR to consider data privacy throughout all processing activities.

Privacy by Design means that any system, process or project that collects or processes personal data must build privacy into the design at the outset and throughout the entire lifecycle.

Privacy by Default states that the strictest privacy settings should apply by default to any new service or process without requiring the data subject to make any changes.

As part of Data Protection by Design and by Default, a data protection and security design review will be performed during the development stage/part of project management of all new SEAI projects where personal data will be processed. By default, only personal data which are necessary for each specific purpose are processed by SEAI. The review process will include assessing the necessity and proportionality of the processing activities, identifying risks to the rights and freedoms of SEAI data subjects and implementing appropriate controls and recommendations to mitigate any risk.

## 6.2 REGULAR RISK ASSESSMENT

The GDPR requires

*a process for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing.*

SEAI will ensure data privacy risks are appropriate to the processing on existing systems. It is the responsibility of the Head of the Department to ensure appropriate technical and organisational security measures are in place in areas for which they are responsible. Specifically, regular security risk assessments must be commissioned to check that the Personal Data is sufficiently protected, and that processing is in line with security policies based on the level of risk. Security risk assessments will be commissioned regularly, and a record maintained for audit purposes with the output from each area examined. At a minimum, this must evaluate and record the technical and organisational measures identified in the previous section (Section 6.1).

## 6.3 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The GDPR requires that a formalised Data Protection Impact Assessment (DPIA) is performed where processing *"is likely to result in a high risk to the rights and freedoms of natural persons"* and/or in the case of *"processing on a large scale of special categories of data"*.

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed to enable SEAI to evaluate and address the likely impacts of new initiatives and put in place appropriate measures to minimise or reduce the risks (including non-implementation).

Data Protection Impact Assessments are required under GDPR under certain circumstances including:

- When the processing of personal data may result in a high risk to the rights and freedoms of a data subject,
- processing of large amounts of personal data,
- processing of special categories of personal data,
- where there is automatic processing/profiling.

Programme Managers are required to consult with the Data Protection Officer in conducting a Data Protection Impact Assessment (DPIA).

## 7 DATA SHARING – CONTROLLER, PROCESSORS, AND THIRD PARTIES

---

### 7.1 SHARING PERSONAL DATA WITH OTHER PUBLIC BODIES

It should be noted that where Personal Data is flowing between public service organisations, each organisation is a distinct legal entity with its own set of legal and data protection responsibilities. Each public service organisation may, therefore, be a data controller in respect of the Personal Data which it has obtained and for which it is legally responsible, and it is necessary for each data controller to assess whether disclosures of Personal Data to other public service organisation is permissible. In this instance, the other public service organisation may be a processor or controller (independent or joint controller).

Where a request is made for sharing of Personal Data with a public body (or third party), this should be referred to the SEAI Data Protection Officer and SEAI's Data Officer. The Data Sharing and Governance Act, 2019 (DSGA) regulates how and when public bodies can share personal data when providing public services. In some instances, for example, where a public body is not subject to the DSGA, other data sharing arrangements may be put in place between the two bodies.

The Data Protection Officer will consider relevant factors to identify the nature of the data protection relationship between the public bodies, such as the legal basis for sharing the Personal Data and its intended use. This will be documented in writing between the public bodies, in accordance with the requirements of data protection legislation and the DSGA.

## **7.2 WHAT ARE SEAI'S REQUIREMENTS IN THE USE OF DATA PROCESSORS AND HOW DO WE COMPLY WITH THEM?**

Whenever SEAI share Personal Data with a third-party processor, the sharing of the information must be governed by a contract that sets out;

- the subject-matter and duration of the processing,
- the nature and purpose of the processing,
- the type of Personal Data and categories of Data Subjects,
- the obligations and rights of the controller.

This applies to all forms of sharing of information with third parties. Sharing of Personal Data cannot take place for any purpose unless SEAI have put a contract in place describing the nature and purpose of processing, in addition to other specific contractual requirements as detailed in this section.

SEAI will not disclose Personal Data to third parties unless the Data Subject has consented to this disclosure or unless there is a lawful ground for processing (e.g.: disclosure to the third party is required to manage a grant application or employee relationship (and in such circumstances, the third-party processor is bound by similar data protection requirements)).

However, SEAI will disclose Personal Data to third parties if it believes in good faith that it is required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order, or other statutory requirement.

## **7.3 EVALUATION OF PROCESSORS AND PRE-PROCESSING AGREEMENTS**

SEAI must use only use Personal Data processors providing sufficient guarantees to implement and be able to demonstrate appropriate technical and organisational measures taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

## **7.4 WHAT ARE OUR REQUIREMENTS AS DATA CONTROLLER AND HOW MUST WE COMPLY WITH THEM?**

All processing agreements must be governed by a contract that is binding on the processor with regard to the controller.

In accordance with data protection legislation, that contract or other legal act shall stipulate, in particular, that the processor:

1. processes the Personal Data only on documented instructions from SEAI, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest
2. processes all Personal Data within the requirements set by the controller;
3. ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
4. shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including as appropriate:
  - a. the pseudonymisation and encryption of Personal Data;
  - b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
  - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
  - e. the account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed;
5. assist SEAI by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the Data Subject's rights under data protection requirements and good practice;
6. assists SEAI in ensuring compliance with its data protection obligations under Articles 32 - 36 taking into account the nature of processing and the information available to the processor;
7. at the choice of SEAI, deletes or returns all the Personal Data to SEAI after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data;
8. makes available to SEAI all information necessary to demonstrate compliance with our data protection obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by SEAI or another auditor mandated by SEAI.
9. The processor shall immediately inform the controller if, in its opinion, an instruction infringes any data protection regulations, acts or good practices.

Where a processor engages another processor for carrying out specific processing activities on behalf of SEAI, the same data protection obligations as set out in the contract between SEAI and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet SEAI requirements. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to SEAI for the performance of that other processor's obligations.

## APPENDIX 1

### DEFINITIONS

The following key GDPR terms and definitions are provided here for ease of use. For a complete list of definitions refer directly to the Regulation (ref: [Art. 4 GDPR – Definitions - General Data Protection Regulation \(GDPR\) \(gdpr-info.eu\)](#)).

**'Anonymisation'** is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

**'Data controller'** means the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**'Data subject'** any living individual who is the subject of Personal Data. Data subjects within SEAI may include members of the public, clients and customers, claimants, current, past and prospective employees, suppliers (such as sole traders), and other individuals with whom SEAI communicates.

**'Personal Data'** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**'processing'** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'Processor'** means a natural or legal person, public authority, agency or another body which processes Personal Data on behalf of the controller.

**'pseudonymisation'** means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person.

**'Record of Processing Activity (RoPA)'** is a record of an organisation's processing activities involving personal data.

**'Special Categories of Personal Data'** refers to the processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Sensitive Personal Data Sensitive Personal Data (or Special Categories of Personal Data)** relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.

**Supervisory Authority** means an independent public authority which is established by a Member State pursuant to [Article 51](#). In Ireland, the relevant Supervisory Authority is the Data Protection Commission (DPC).

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as in the GDPR.

**Appendix 15 – Data Breach Policy**

**(Approved by the Board on 18 September 2024)**

# SUSTAINABLE ENERGY AUTHORITY IRELAND (SEAI) DATA BREACH POLICY AND PROCEDURE

---

Revision History

<i><b>Version</b></i>	<i><b>Revision Date</b></i>	<i><b>Revised by</b></i>	<i><b>Section Revised</b></i>
V.1		Senior Information Compliance Officer	



## 1. Policy Statement

The **Sustainable Energy Authority of Ireland** (*hereinafter referred to as “SEAI”*) is committed to its obligations under the regulatory system in accordance with the General Data Protection Regulation (GDPR) and maintains a robust and structured programme for compliance and monitoring. We carry out frequent risk assessments and analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to SEAI and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws, including the Data Protection Act, 2018.

### 1.1 Purpose

The purpose of this policy is to provide SEAI's intent, objectives and procedures regarding data breaches involving personal information. SEAI has obligations under the GDPR, and also has a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

Under the GDPR, all personal data breaches that present a risk to data subjects must be reported to the relevant Supervisory Authority, the Data Protection Commission (DPC), within 72 hours of first becoming aware of the breach. Any person within SEAI who becomes aware of a data breach or a suspected data breach must report it to SEAI's Data Protection Officer (DPO) without delay to allow an assessment and report to be made to the DPC if required. The process flow map for the process is set out at Appendix 1.

While SEAI makes every effort to avoid data breaches from occurring, it acknowledges that breaches can and do happen. It aims to create an environment where everyone, regardless of role, feels comfortable reporting their concerns quickly so that any potential data breach or incident can be investigated swiftly, risks to data subjects identified and mitigated and valuable learning adopted to improve policies and procedures.

## 2.Scope

This policy applies to all staff within SEAI (*meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with SEAI*) and SEAI Board Members. It also applies to clients and third parties with access to SEAI's information and IT resources.

All staff have a responsibility to engage in good data protection practices and report any security incidents and breaches or suspected breaches of personal data. Adherence to this policy is mandatory and non-compliance may lead to disciplinary action.

## 3.Data Security & Breach Requirements

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed<sup>1</sup>. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error. A personal data breach is a security incident that negatively impacts the confidentiality, integrity, or availability of personal data.

Data Breaches occur in a variety of different contexts, for example:

- Disclosing confidential data to unauthorised individuals. For example, accidentally sending an email containing confidential or sensitive data to the wrong recipient or recipients as a result of human error.
- Loss or theft of data, including equipment on which data is stored (e.g. , smartphone, tablet, etc.) or paper records.
- Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords).
- Equipment failure.
- Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account).
- Collection of personal data by unauthorised individuals.
- Hacking, viruses or other security attacks on IT equipment, systems or networks.
- Breaches of physical security (e.g. forcing of doors / windows / filing cabinets).

---

<sup>1</sup> Article 4 GDPR

Not all security or access incidents will result in a personal data breach. Existing security measures may determine that a breach has not occurred as a result of the incident. However, this must only be determined by SEAI's Data Protection Officer (DPO). For example:

- The personal data is securely encrypted or anonymised such to make the personal data unintelligible; and/or
- There is a full, up-to-date back-up of the personal data (in cases of accidental destruction).

If there is any doubt as to whether a data breach has occurred, the DPO should be consulted immediately.

SEAI carries out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including (*but not limited to*): -

- Pseudonymisation and encryption of personal data.
- Restricted access permissions.
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- New Cyber Security Strategy
- New Information Security policies and standards that are audited on an annual basis.
- ISO27001 (due 2025Q1)
- Continuous Cyber Security reviews and Tests (e.g. Pen Tests, Red Team, Phishing, etc.)
- 24x7x365 Security Information & Event Management Service (SIEM).
- Audit procedures on a regular basis to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations.
- Frequent and ongoing data protection and cyber security training and awareness programs for all employees.

## 4. Objectives

- To adhere to the GDPR and the relevant Data Protection legislation and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches.

- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information.
- To minimise the risk to data subjects in the event of breaches occurring.
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches.
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information.
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring.
- To use the Data Breach Incident Form for all data breaches, regardless of severity, so that any patterns in causes can be identified and corrected.
- To protect all SEAI stakeholders, clients and employees, including their information and identity.
- To ensure that the Data Protection Officer is involved in and notified about all data breaches and relevant risk issues.
- To ensure that the Data Protection Commission is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of SEAI having become aware of the breach.

## 5. Data Breach Procedures & Guidelines

SEAI has robust objectives and controls in place for preventing data breaches and for managing them when they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

### 5.1 Breach Monitoring & Reporting

SEAI has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to [dataprotection@seai.ie](mailto:dataprotection@seai.ie) with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, the matter is raised with the appropriate vendor for resolution.

## **5.2 BREACH INCIDENT PROCEDURES**

### **5.2.1 IDENTIFICATION OF AN INCIDENT**

As soon as a data breach has been identified or where there is a suspected data breach, it is reported to the direct line manager and [dataprotection@seai.ie](mailto:dataprotection@seai.ie) immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of SEAI and is not about apportioning blame. These procedures are for the protection of SEAI, its data subjects, staff, third party processors and stakeholders and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, data subject, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

### **5.2.2 SEAI DATA BREACH NOTIFICATION FORM**

Any individual who has become aware of a data incident or who may have been the cause of a personal data breach, should report the matter to [dataprotection@seai.ie](mailto:dataprotection@seai.ie) and follow any immediate instruction from the DPO and thereafter complete SEAI's Data Breach Notification Form (Appendix 2). This form must be returned without delay to [dataprotection@seai.ie](mailto:dataprotection@seai.ie), cc'ing Line Manager and should provide as much detail as possible in assisting the DPO in assessing if a breach has occurred, the severity of the breach and what actions are required.

### **5.2.3 THIRD PARTY BREACH NOTIFICATION**

Where a third-party who processes personal data on behalf of SEAI, or where another Controller who shares personal data with SEAI becomes aware of a personal data breach compromising the personal data of the data subjects of SEAI, they must complete SEAI's Data Breach Notification Form (Appendix 2) without delay and within twenty-four (24) hours of becoming aware of the breach. The form should be returned to [dataprotection@seai.ie](mailto:dataprotection@seai.ie) and the information provided on this form may be shared with the Data Protection Commission if required.

### **5.2.4 SEAI DATA BREACH LOG**

SEAI maintain a Data Breach Log to register data breaches and data security incidents with SEAI. The DPO will record the incident on the breach log, making notes of any notifications, such as to data subjects and the Data Protection Commission, as required.

### **5.2.5 SEAI DATA BREACH INTERNAL REPORT**

SEAI utilises a Breach Internal Report Form for all incidents, which is completed by the DPO or a member of the Information Compliance Office team, for recording and assessing data breaches and incidents that are reported. This form specifies (i) the facts relating to the data breach or data incident,

(ii) its likely effects (iii) any remedial action taken or proposed to be taken by SEAI (iv) an assessment of the severity of the risk to data subjects (v) root causes of the risk and (vi) outcomes and lessons learned. A full investigation is conducted and recorded on the form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

### 5.2.6 NOTIFICATION TO DPC AND DATA SUBJECTS

If applicable, the Data Protection Commission and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 4 of this policy*). The Data Protection Commission protocols are to be followed and their '**Security Breach Notification Form**' should be completed and submitted by the DPO or a member of the Information Compliance Office.

In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

### 5.2.7 NOTIFICATION TO OTHER PARTIES

SEAI should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements (such as to the National Cyber Security Centre (NCSC), Gardaí, insurers, external legal advisers, etc.).

## 6 INVESTIGATION, ASSESSMENT OF RISK AND MITIGATION

The DPO will ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

### 6.1 BREACH MANAGEMENT TEAM

In cases of data breaches, and where appropriate, the DPO will establish an appropriate Breach Management Team to investigate the causes and impact of the breach or incident. This team will comprise of relevant individuals who can assist the DPO in determining the cause of the breach and actions required to mitigate risk. For example, the team may include members from the relevant Programme where the breach occurred, a Programme Manager, members from IT if the breach requires technical expertise and / or a nominated agent from a SEAI trusted partner where a third- party processor is involved. The Team will meet as required and assist the DPO in carrying out a full investigation and assessment of the incident and appointing the relevant staff to take recommended actions to contain the breach and mitigate risk to data subjects.

The Breach Management Team will look at: -

- The type of information / categories of personal data involved.
- Its sensitivity or personal content.
- The number and type of data subjects affected.
- What protections are in place (e.g. encryption).

- What happened to the information/Where is it now?
- Risks to the data subjects
- What immediate actions are required.
- Whether there are any wider consequences/implications to the incident or data subjects.

The DPO will keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

In the event of a cybersecurity incident, the cybersecurity incident response process may be invoked by the IT or crisis management team in response to a data breach. The Cybersecurity Incident Response Team (CSIRT) assembled will compose of The Crisis Management Team (CMT), Business Continuity Planning (BCP) manager, Chief Information Officer, (CIO), Chief Information Security Officer (CISO), Cyber Security Executive, Legal team, DPO, PR/Marcomms and Human Resources representatives. Roles and responsibilities are outlined in the SEAI Cybersecurity Incident Response plan.

## **6.2 HUMAN ERROR**

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and if necessary, an interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with SEAI's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Reminders on security of personal data and the measures they can take to ensure a similar incident does not recur.
- Re-training in specific/all compliance areas.
- Re-assessment of compliance knowledge and understanding.

## **6.3 SYSTEM ERROR**

Where the data breach is the result of a system error/failure, SEAI's IT team (and external IT vendors if required) are to work in conjunction with the DPO to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Internal Report Form.

Any identified gaps that are found to have caused/contributed to the breach are to be reviewed and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed.
- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system.
- The use of back-ups to restore lost, damaged or stolen information.
- Advising users of portals etc. that delays may be experienced in accessing / registering SEAI systems, as appropriate.



## 7. BREACH NOTIFICATIONS

SEAI recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of SEAI's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

### 7.1 SUPERVISORY AUTHORITY NOTIFICATION

The Data Protection Commission is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. Where applicable, the Data Protection Commission is notified of the breach no later than 72 hours after SEAI becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Data Protection Commission of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be **unlikely** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Data Protection Commission in accordance with Article 33 of the GDPR.

The notification to the Data Protection Commission will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information*)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (*including measures to mitigate its possible adverse effects*)

Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

### 7.2 DATA SUBJECT NOTIFICATION

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach.
- Recommendations for the data subject concerned to mitigate potential adverse effects of the breach.
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information).
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing each individual data subject of a breach involves disproportionate effort, we reserve the right to instead make a public communication whereby all the data subject(s) are informed in an equally effective manner.

## **8. RECORD KEEPING**

All records and notes taken during the identification, assessment and investigation of the data breach are recorded and authorised by SEAI's Data Protection Officer and are retained for a period of 7 years from the completion of the investigation. Incident forms are to be reviewed periodically to assess for patterns or breach recurrences and actions taken to prevent further incidents from occurring.

## **9. RESPONSIBILITIES**

SEAI will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the reach incident reporting lines.

The Data Protection Officer, with the appropriate resources and support from Senior Management, is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups.

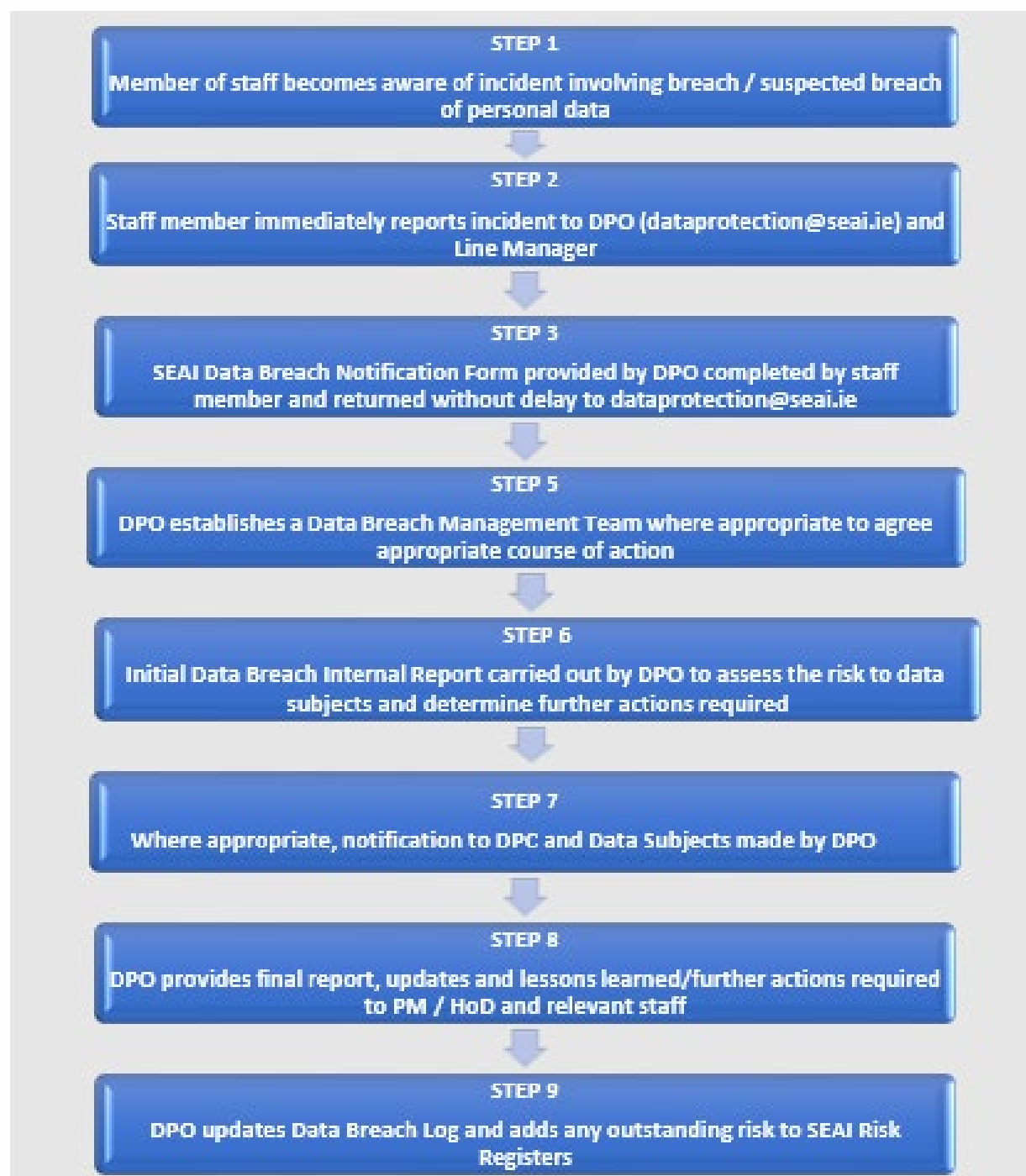
## **10. FURTHER GUIDANCE**

For further information and advice about what to do in the event of a suspected data breach please contact SEAI's Data Protection Officer at:

Email: [dataprotection@seai.ie](mailto:dataprotection@seai.ie)

Phone: 01 808 2234

## APPENDIX 1 - DATA BREACH PROCEDURE



## APPENDIX 2 –SEAI DATA BREACH NOTIFICATION FORM

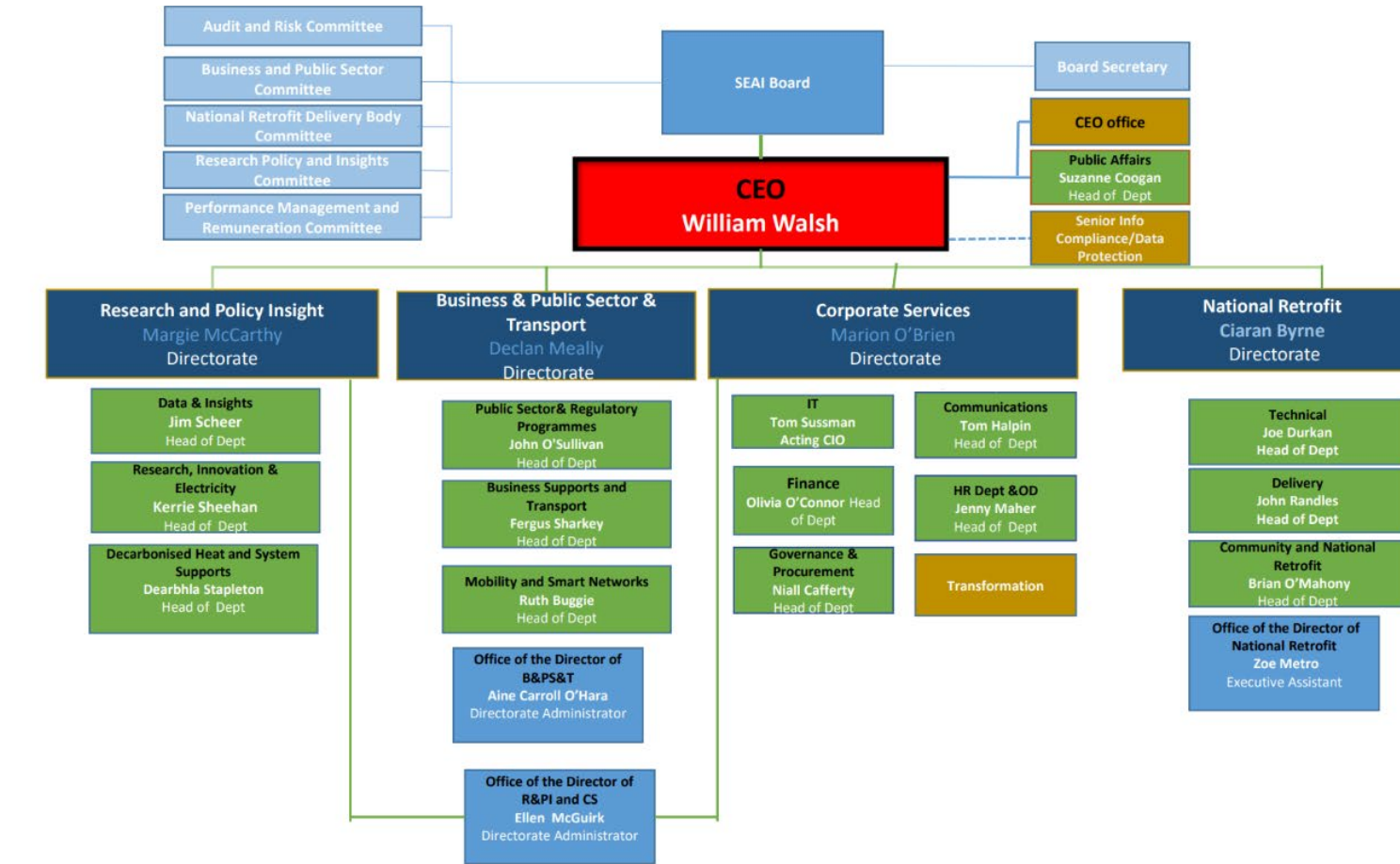
It is extremely important that you take immediate action upon learning of a breach or suspected incident involving the destruction, loss, alteration, unauthorised disclosure of, or access to personal data and contact the Data Protection Officer at [dataprotection@seai.ie](mailto:dataprotection@seai.ie) and Cc'ing your Line Manager without delay. Any incident or concerns that the confidentiality, integrity or availability of personal data may have been negatively impacted should be reported and all emails should be marked 'Urgent'.

Section A: Incident Timeline - Complete all sections	
1. Internal / External Breach (Internal relates to SEAI staff and Board Members) (External relates to service providers, contractors etc.)	
2. If External (third party / service providers) Name of Company:	
3. Name of person reporting incident:	
4. Department:	Programme:
1. Has the Line Manager been informed? If not, please give a reason. If this is an external breach, please confirm and identify the appropriate point of contact in SEAI who has been notified.	Yes / No
2. Date and precise time <u>of the incident</u> :	Date: Time:
3. Date and precise time the <u>incident was detected</u> :	Date: Time:
4. Date / time <u>of reporting the incident to Data Protection Officer</u> : Timely reporting is crucial to satisfy the GDPR's <b>72-hour deadline</b> . If you are reporting outside of this timeframe, please explain why.	Date: Time:

5. Is the incident ongoing?	Yes / No
6. Date / time that <u>the incident ended</u> :	Date: Time:
<b>Section B: Incident Detail</b>	
Please describe how the incident occurred. Provide as much detail as possible.	
What types of records and personal data were disclosed? Provide detail	
<p>Were there any special category*, criminal or confidential data involved? Provide detail.</p> <p>*Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation</p>	
<p>What categories of data subjects were affected? (For example, SEAI employees, Homeowners, Contractors)</p>	
<p>Do you know the number of affected individuals? Provide detail.</p>	
<p>Do you know the number of affected records? Provide detail.</p>	
<p>Were vulnerable* individuals affected? E.g., children, clients with special needs, employees, the elderly</p> <p>* Individuals can be vulnerable where a power imbalance exists between the data subject and controller and where circumstances may restrict the data subject's ability to freely consent or object to the processing of their personal data or to understand its implications</p>	

What measures have been taken in response to the incident?	
Have you secured / retrieved any breached data?	
If not, please outline why you have not secured / retrieved the data.	
What in your view are the potential consequences of the incident for affected individuals?	
Are the affected individuals aware of the incident?	
How many affected individuals have been made aware?	
What information was communicated to the affected individuals? In particular, please indicate if you have related to affected individuals the steps they should take to mitigate any adverse consequences which have been caused or could be caused to them by this incident.	

## Appendix 16 – SEAI Organisation Chart





## **Appendix 17– Delegated Authorities Framework Overview**

**(Approved by the Board 27 July 2022)**

### **Delegated Authority Framework (“DAF”)**

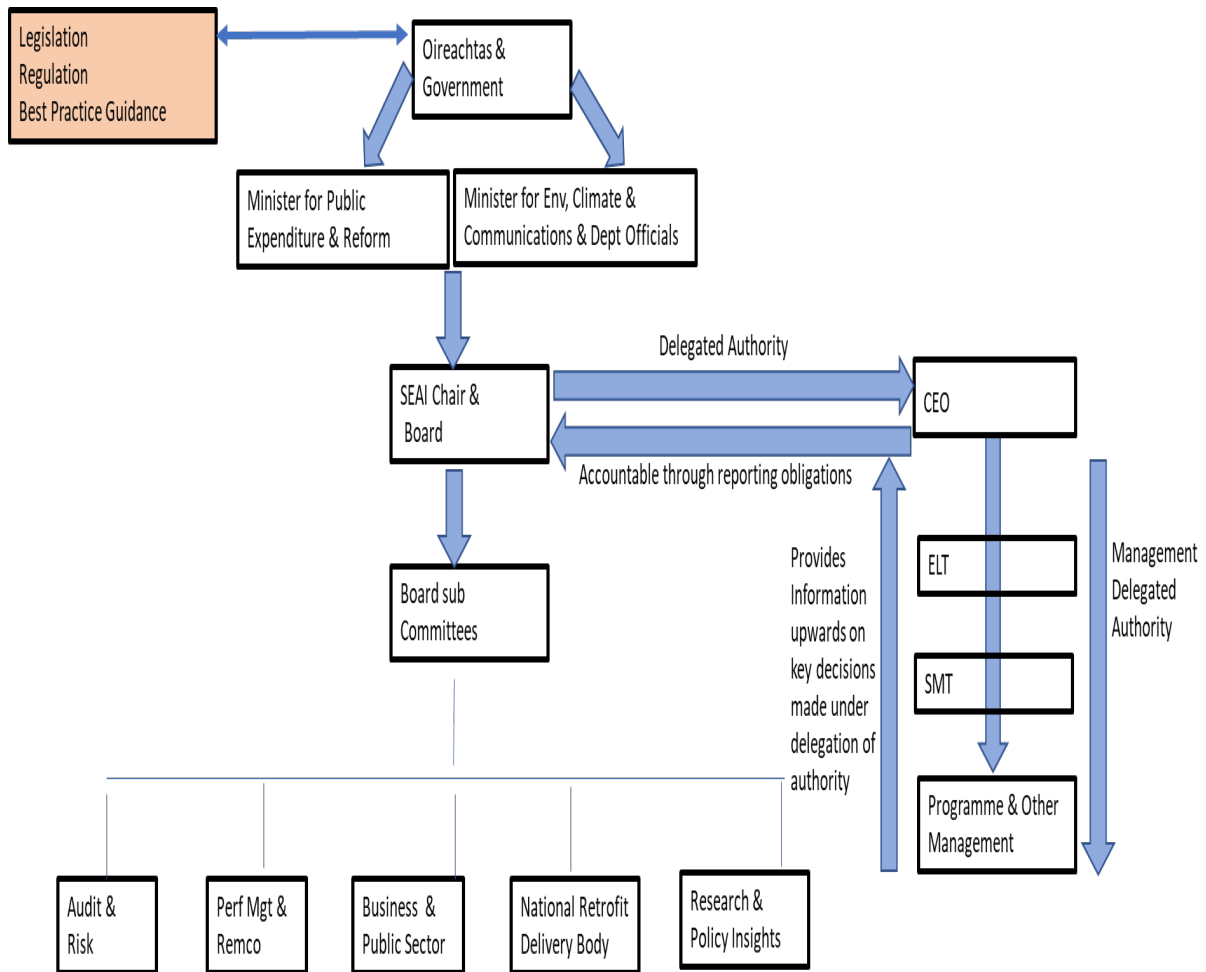
The DAF is a reference document that summarises those matters that require approval (including financial thresholds for delegated transactions) at various levels of authority up to Ministerial/Department level, Board and layers of management. It is designed to aid users by ensuring that they have a quick reference guide to authority levels. Execution of authority set out in the DAF by the relevant parties is of course subject to compliance with the policies, procedures and processes underpinning the particular transaction and supporting the governance of the organisation.

### **Structure of DAF & Guiding Principles**

The DAF provides a schematic of the governance structure in SEAI, a high-level summary of core roles and responsibilities, guiding principles and schedules of matters reserved and delegated. The guiding principles underpinning the DAF are as follows:

- The lists of decisions described in the **Delegated Authorities Framework (“DAF”)** and in the schedules as set out are not intended to be exhaustive but rather are designed to provide guidance on delegated authorities to decision making fora in the context of SEAI’s overarching governance model.
- The lists should be read in conjunction with the referenced material including policies and procedures where relevant.
- The Minister, Department and Board will in the normal course of business be notified of other matters, not specifically set out in the schedules, by way of CEO updates or other forms of communications between the parties.
- Matters deemed to be of strategic and tactical importance will be notified and discussed as appropriate with the Board and /or relevant Government Department.
- In all cases, the authority to approve is subject to the capacity to do so within one’s scope of responsibility and financial capacity to absorb the incremental expenditure within the budgetary allocation for the relevant cost head, taking account of prior expenditure and approvals as relevant.
- Approvals are incremental such that at each level of approval the matter will have been considered and recommended for approval at less senior levels before being system escalated.
- Segregation of duties apply with appropriate segregation achieved through operating procedures and division of responsibilities between requesters, approvers and checkers.
- Many decisions require input from other colleagues and/or experts, and it is the duty of those presenting matters for decision to ensure that appropriate views are sought prior to making recommendations to decision makers.

## Schematic of the Governance Structure in SEAI



## Responsibilities

Those charged with responsibility for managing SEAI's operations are required to do so in line with SEAI's values, in compliance with laws and regulations, codes of conduct and ethical standards. They are also always expected to exercise a duty of care and a duty of candour which in the context of Delegated Authorities requires diligence in decision making. Decision makers in authorising actions on behalf of SEAI are expected and required to exercise sound judgement supported by accurate and timely information.

## Reserved Matters & Delegated Matters

The objectives of the Delegated Authorities Framework are to establish and communicate:

- Matters Reserved for Ministerial and/or Department approval or notification
- Matters Reserved for Board approval or notification
- Authority limits to empower the executive management team and staff to make effective and appropriate decisions in relation to SEAI's activities

## Appendix 18 – SWiFT 3000 Certification (re-certified December 2024)



### Certificate of Compliance

utilising

**SWiFT 3000:2010**

is awarded to

### **Sustainable Energy Authority of Ireland**

**Wilton Park House  
Wilton Place  
Dublin 2**

---

NSAI, the National Standards Authority of Ireland, certifies that the Corporate Governance framework of the above organisation has been assessed in accordance with SWiFT 3000:2010 - Code of Practice for Corporate Governance Assessment in Ireland.

The assessment confirmed compliance of the organisation's corporate governance practices, with the Department of Public Expenditure and Reform - Code of Practice for the Governance of State Bodies 2016.

Approved by:  
**Fergal O'Byrne**  
Head – Business Excellence, NSAI

---

Registration Number: SW3K.001  
Original Registration: 18 February 2011  
Last amended on: 19 December 2024  
Valid from: 19 December 2024  
Remains valid to: 18 December 2025

*This certificate remains valid on condition that the Corporate Governance framework is maintained in an adequate and efficacious manner and verified through on-going annual assessment.*

---

All valid certifications are listed on NSAI's website – [www.nsai.ie](http://www.nsai.ie). The continued validity of this certificate may be verified under "Certified Company Search"



NSAI (National Standards Authority of Ireland), 1 Swift Square, Northwood, Santry, Dublin 9, Ireland T +353 1 807 3800 E: [info@nsai.ie](mailto:info@nsai.ie) [www.nsai.ie](http://www.nsai.ie)  
NSAI Inc. 20 Trafalgar Square, Suite 603, Nashua, New Hampshire, NH 03063, USA T +1 603 882 4412 E: [info@nsaiinc.com](mailto:info@nsaiinc.com) [www.nsaiinc.com](http://www.nsaiinc.com)

## Appendix 19 ISO/IEC 27001:2022 Certificate of Registration (awarded November 2024)



### CERTIFICATE OF REGISTRATION

The management system of certificate number **529909**

#### **Sustainable Energy Authority of Ireland**

St. Kevins, 3 Park Place, Hatch Street Upper, Dublin 2,

has been assessed and certified as meeting the requirements of:

#### **ISO/IEC 27001:2022**

The provision of energy analysis and advice, energy grants to homes, businesses and communities, and the operation of regulatory programmes within Ireland.

This is in accordance with the Statement of Applicability **Version 1 dated 20/09/2024**.

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.



Valid from:  
**Initial certification:** 12 November 2024  
**Latest issue:** 12 November 2024  
**Expiry date:** 11 November 2027  
**Recertification before:** 11 November 2027  
Subject to annual assessments.

Authorised by

A handwritten signature in black ink, appearing to read 'Mike Tims'.

Mike Tims  
Chief Executive Officer

**amtivo.ie**

Certificate issued by Amtivo (Ireland) Limited

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.  
Amtivo (Ireland) Limited, Block 20A, Beckett Way, Parkwest Business Park, Dublin 12, D12 P8R2.