Corporate Information Security Policy

Table of Contents

Document Control

Table of Contents

1. Overview
2. Purpose
3. Scope
4. Policy
5. Policy Compliance
6. Related Standards, Policies and Processes
7. Definitions and Terms
8. Revision History

Document Control

Document Name	Corporate Information Security Policy
Classification	INTERNAL
Revision Number	3.5
Revision Date	05/12/2024
Custodian	Enterprise Security Manager
Approval	Insights IS Forum
Audit	Annual: Enterprise Security Manager
Next Review	December 2025

1. Overview

This policy is based on ISO 27001:2022 the recognised international standard for information security. This standard ensures that the Insights complies with the following security principles:

Confidentiality: All sensitive information will be protected from unauthorised access or disclosure.

Integrity: All information will be protected from accidental, malicious and fraudulent alteration or destruction; and,

Availability: Information services will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

2. Purpose

The purpose of this policy is to demonstrate the commitment that Insights Learning and Development has towards the security of data it is responsible for and demonstrating the controls and responsibilities in place to support the Information Security Management System, ISMS, which has ISO 27001:2022 at its main framework.

3. Scope

The scope of this policy covers all internal and external parties and supports Insights continued commitment to ISO 27001:2022.

4. Policy

4.1 Executive Responsibilities

Insights' Executive are committed to satisfy all applicable requirements within this policy and to the continual improvement of the Information Security Management System (ISMS), and therefore have established this information security policy so that:

- it is appropriate to the purpose of Insights;
- it includes information security objectives and provides the framework for setting continual information security objectives.

This information security policy shall be available as documented information; be communicated within Insights; and be available to interested parties, as appropriate.
Compliance with this policy and all other security policies and procedures is mandatory for all staff.
The CEO approves this policy. The Information Security Forum has the responsibility for ensuring that the policy is implemented and adhered to across the business covered by the scope of the ISMS.

4.2 Leadership and Commitment

The Executive will continue to demonstrate leadership and commitment with respect to the ISMS by:

- ensuring the information security policy and information security objectives are established and are compatible with the strategic business direction of Insights;
- ensuring the integration of the ISMS requirements into Insights' processes;
- ensuring that the resources needed for the ISMS are available;
- communicating the importance of effective information security management and of conforming to

the ISMS requirements;
- ensuring that the ISMS achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the ISMS;
- Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

4.3 Information Security Objectives

Information security objectives have been established and are compatible with the strategic direction of Insights, the key objective is to work in line with the sections of the best practice standard ISO 27001:2022 detailed below.
Furthermore, security objectives will be set by the Information Security Forum as an ongoing task and at ISMS Management Review Meetings.

4.4 Continual Improvement of the ISMS Framework

Insights will seek to continually improve the information security management system in line with a PLAN-DO-CHECK-ACT approach to improve processes embedded within its ISMS.

The importance attached to information security is demonstrated by the existence of the Information Security Forum; The function of the Information Security Forum is outlined below;

- reviewing and progressing strategic security issues;
- establishing relationships outside of Insights with other security advisers;
- assessing the impact of new statutory or regulatory requirements imposed us;
- monitoring the effectiveness of the ISMS e.g. from the results of Internal Audit reports and Security Incident Reports;
- recommending /endorsing changes to the ISMS.

The Information Security Forum meets regularly to address the above activities in order to assure the continuing effectiveness of Insights' ISMS. The review process is defined in the 'Information Security Forum Management Review Policy'.

This Corporate Information Security Policy confirms Insights commitment to continuous improvement and highlights the key areas (referred to as 'themes') to effectively secure its information, namely:

- Organisational Controls
- People Controls
- Physical Controls
- Technological Controls

4.5 Organisational Controls

Organisational Controls are the responsibility of the Information Security Forum and address the following areas:
- Strategic Information Security Policies – which covers this policy, Security Objectives Policy and Communications Policy.
- Roles and Responsibilities – the Enterprise Security Manager chairs the Information Security Forum.
- Identity and access management - the Enterprise Security Manager / Team Leaders are responsible for both establishing and maintaining robust logical access controls. An appropriate policy is in place and must be complied with by all staff and external parties.
- Asset Management – Insights information must be classified according to its sensitivity and an information owner assigned. Enterprise Security Manager will maintain an information asset inventory which is updated periodically, according to its risk profile and protected accordingly.
- Relationships – Information security requirements for mitigating the risk associated with the supplier's access to Insights assets must be agreed with the supplier and documented.
- Cloud provider agreements need to be established, documented and subject to ongoing review.
- Incident Management - Security incident management records must be centrally maintained, updated and monitored on an ongoing basis. All employees must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to. The responsibility for the oversight of all security breaches rests with the Enterprise Security Manager.

- Business Continuity Management - Insights must ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

- Compliance - Insights must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. Insights must take technical and organisational measures to protect personal data against accidental or unlawful destruction, or accidental loss or alteration, and unauthorised disclosure or access. In particular, Insights should take measures that are intended to ensure that:

    - Anyone managing and handling personal data understands that they are contractually responsible for following good data protection practice.
    - Everyone managing and handling personal data is appropriately trained to do so; and
    - Everyone managing and handling personal data is appropriately supervised.

4.6. People Controls

People Controls are the responsibility of the Human Resources Team and address the following areas:

- All employees must sign up to the Employee Handbook which requires them to work in accordance with all policies and procedures which includes information security specific requirements.
- A Personal Information Security Policy ensures that employees are made aware that they are required to follow best practices regarding information security.
- There is also a procedure for all employees that leave Insights (including temporary and contract employees) to disable their network account and recover all items of property.
- All new employees (permanent, temporary and contractors) must be trained on procedures in the areas described above as part of their induction programme. Ongoing training must be provided in the form of a programme of regular updates and training sessions by the Information Security Forum.

4.7 Physical Controls

Physical Controls are the responsibility of the Facilities Team and address the following areas:

- Staff must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include:

    - building alarm and CCTV systems
    - restricted access to the building and further restricted access within it
    - secure lockers, drawers, safes and storage, fireproof storage
    - secure offsite backups and archiving
    - clear desk and clear screen arrangements
    - procedures for the issue of any media
    - the need for ongoing monitoring of all physical security measures

4.8. Technological Controls

Technological Controls are the responsibility of the Enterprise Technology & Security Team and address the following areas:

- All endpoint devices must be adequately protected and encrypted where appropriate.
- Identity and access management – IT systems administrators (privileged users) ensure that the agreed access controls and procedures are managed in line with the established policy.
- Cryptography - Where cryptographic controls are employed by Insights a policy on the use of cryptographic controls for protection of information has been developed and implemented.
- IT Operations Security - Insights will ensure correct and secure operations of information processing facilities. The Enterprise Technology & Security Team conduct ongoing monitoring on all IT operational activities.
- IT Communications Security - staff must be aware that the use of technology and communications are established, controlled and managed by the Enterprise Security Manager. He is responsible for ensuring that the appropriate security measures and processes are in place. Insights will ensure that security around the network, endpoint and remote working are adequately protected.
- IT Systems Development Security - the Enterprise Security Manager ensures that the appropriate

information security processes are included in all projects. A secure development approach including policy, procedures and environment and testing are in place.

4.9. Policy Review Period

The Information Security Forum will review this Policy at least annually.

5. Policy Compliance

Compliance Measurement: The Security Team and/or Information Security Forum will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions: Any exceptions to this policy must be approved via the policy Custodian and Approver. In their absence, such as annual leave, this will fall to the responsibility of a member of the Custodian and/or Approvers line management or Information Security Forum

Non-Compliance: An employee found to have violated this policy, that impacts the reputation of Insights Learning and Development or the wider Insights Group may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

Item	Int or Ext	Document Title
1	Internal	ISMS Document Management System
2		
3		
4		
5		
6		

7. Definitions and Terms

Non-Applicable

8. Revision History

Revision	Date	Amended by	Description
2.0	09/01/2020	Graham Watson	Policy approved by CEO
2.1	24/09/2021	Kevin McAuley	Minor changes based on changes in roles and structure
3.0	30/11/2021	Kevin McAuley	Policy approved by Executive Board
3.1	13/02/2023	Dave McClure	Policy Update adding new policy's
3.2	06/03/2023	Dave McClure	Roles and responsibilities moved to new policy
3.3	05/04/2023	Ian Gowen	Added Internal Ref Table
3.4	28/04/2023	Ian Gowen	Changed the order of Internal References
3.5	05/12/2024	Andy Moore	Annual Review and CEO sign off

Signed: 

Date: 5th December 2024

Fiona Logan
Chief Executive Officer