Last updated: March 2023
Last Reviewed: March 2023

Corporate Information Security Policy

1. Policy scope

This policy is based on ISO 27001:2013, the recognised international standard for information security. This standard ensures that IFS 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 will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

2. Top management responsibilities and commitment

IFS is committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions.

The Institute's top management is committed to satisfying all applicable requirements within this policy and to the continual improvement of the Information Security Management System (ISMS), and has therefore established this information security policy so that:

- it is appropriate to the purpose of the Institute;
- it includes information security objectives and provides the framework for setting new information security objectives annually.

This policy shall be available as documented information; be communicated within the Institute; and be available to interested parties, as appropriate.

Compliance with this policy and all other security policies and procedures is mandatory for all staff and others using the IFS network.

3. Leadership and commitment

The Director 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. The Information Security Forum is a subset of the IFS Computing Committee which is chaired by an Associate Director. This Associate Director is responsible for the oversight and approval of the ISMS and for discussing any issues with the Director.

The security policy confirms the Institute's commitment to continuous improvement and highlights the key areas to secure its information effectively.

Top management will continue to demonstrate leadership and commitment to the information security management system by:

- ensuring that the information security policy and information security objectives are established and are compatible with the strategic business direction of the Institute;
- ensuring the integration of the information security management system requirements into the organisation's processes;
- ensuring that the resources needed for the information security management system are available;
- communicating the importance of effective information security management and of conforming to the information security management system requirements;
- ensuring that the information security management system achieves its intended outcome(s);
- directing and supporting staff to contribute to the effectiveness of the information security management system;
- Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

4. Information security objectives

Information security objectives have been established and are compatible with the strategic direction of the organisation. The key objective is to work in line with the sections of the best practice standard ISO 27001:2013, detailed below.

Security objectives will be proposed by the ISF and will be approved annually Computing Committee meetings which is chaired by an Associate Director.

IFS will continually seek to improve the ISMS.

5. Organisation of information security

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

- reviewing and implementing strategic security issues;
- establishing relationships outside IFS with other security advisers;
- assessing the impact of new statutory or regulatory requirements ;
- 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 Forum meets regularly to address the above activities in order to assure the continuing effectiveness of the Institute's ISMS. The review process is defined in the ISMS Management Review Policy.

6. Human resources

All employees must read and sign up to the Conditions of Service which requires them to work in accordance with all policies and procedures, including information security specific requirements. Furthermore, IS Guidelines ensure that employees are made aware that they are required to follow best practices regarding information security. There is also a procedure for all employees who leave IFS (including temporary and contract employees) to disable their network accounts and recover all items of property.

All new employees (permanent, temporary and contractors) must be trained in 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.

7. Asset management

Institute information must be classified according to its sensitivity using the information classification and handling policy. Physical assets are recorded in the asset inventory an owner or a location is assigned. The physical asset inventory is updated when new assets are purchased.

8. Access control

Employees must be aware of and must follow a number of controls and procedures, which exist to limit access to confidential information. The Information Security Manager is responsible both for establishing and maintaining robust logical access controls. An Access Control Policy must be in place and complied with by all employees and third parties.

9. Cryptography

A policy on the use of cryptographic controls for protection of information must be developed and implemented.

10. Physical and environmental security

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 and individual alarm 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 policy;
- clear screen policy;
- procedures for the issue of media (memory sticks and laptops).

11. Operations security

The Institute will ensure the correct and secure operation of information processing facilities.

12. Communications

Staff must be aware that the use of technology and communications are established, controlled and managed by the Information Security Manager and the Head of ICT. They are responsible for ensuring that the appropriate security measures and processes are in place. IFS will ensure that the network and mobile and remote working systems are adequately protected.

13. System acquisition, development and maintenance

The IT Team must ensure that the appropriate information security processes are included in all projects. A secure development approach, comprising policy, procedures and testing, will be implemented.

14. Supplier relationships

Information security requirements for mitigating the risks associated with suppliers' access to the Institute's assets must be agreed with the supplier and documented.

15. Information security incident management

Security incident management records must be centrally maintained, updated and monitored via a manual process. 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 breaches of technical and physical security rests with the Information Security Manager.

16. Information security aspects of business continuity management

The Institute 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.

17. Compliance

The Institute must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

The Institute 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 the Institute takes 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.

18. Compliance review period

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

Signed:

Paul Johnson, Director

Date: **20/06/2023**

19. Policy review and audit log

Summary of audit and review findings

Date	Reviewed by	Audited by	Issues found	NC or Obs?	Action taken	Location of audit findings*
18/2/2021	EH	EH	Section 7 did not reflect current practice	obs	Policy amended	
15/3/2022	EH	EH	No issues			
20/3/2023	EH	EH	Small edit made	Obs		

*all audit findings are stored in subfolders within ISO27001\Policies and internal audits\7. Internal audit and review\

Log of changes made

Date	Changes made	Changes made by	Approved by	Major or minor change?	Where archived?* (major changes only)
18/2/2021	Changed 'Associate Director' to 'Deputy Director' in sections 3 and 4.	EH		Minor	
17/03/2021	Section 7 updated to reflect current practice.	ZO	EH	minor	
20/3/2023	Changed Chair of CC to Associate Director	EH		minor	
20/6/2023	Updated signature of director	EH		minor	

*all archived documents are stored in subfolders within ISO27001\Working documents and archive\Archive