ISO 27001:2013 ISMS Scope Statement

1. Document scope

This document 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. ISMS scope

The scope of the ISO 27001:2013 compliant Information Security Management System (ISMS) is all employees, systems, data and processes incorporated under IFS at the following location.

Premises address

7 Ridgmount Street
London
WC1E 7AE

The following functions are covered:

- Information and communication technology
- Finance
- Human resources
- Facilities
- Research
- Communications
- Operations

3. Information security forum

An Information Security Forum has been established. An up to date list of membership is kept here: https://intranet.ifs.org.uk/share/page/site/ifs-net/wiki-page?title=Information_Security_Forum

4. ISMS Scope Context

The IFS is an independent research institution with the principal aim of better informing public debate on economics. The IFS relies heavily on its reputation and any information security breach would impact negatively on that. The Institute makes use of research and administrative datasets from external organisations and to gain access to these datasets we need to be able to demonstrate compliance with information security issues.

5. Identification and Expectations of Interested Parties

The organisation has determined external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

Party	Interest	Expectation
Employees	Employees comply with the practices outlined in the ISMS. Their data is also subject to the practices outlined in the ISMS	That their data will be kept secure and that practices outlines in the ISMS are clearly communicated so that they can adhere to them.
Regulators and Government	They create information security law Government provide us with data	That we adhere to all data protection laws.
Funders	They have an interest in ensuring that IFS do not breach data protection since that would have a detrimental effect on their own reputation.	That IFS keeps all confidential information about the funder secure and that we ensure we do not have any information breaches that would risk our own and their reputation.
Research data owners	They have a strong interest in our data protection and information management systems because they share data with us. Any data breach by IFS would put their data at risk.	That IFS keeps all their data secure and minimises the risk that data is breached or lost.
Collaborators	Organisations that work with us have an interest in ensuring that we do not have any data breaches since that would have a detrimental impact on their own reputation and on their ability to work with us on an ongoing basis.	That IFS keeps all information about the collaborator secure and free from risk of disclosure and that we do not have any information security breaches that would harm their reputation or our working relationship.
Research participants	They have a strong interest in our data protection and information management systems because any breach would put their data at risk.	That IFS keeps all their data secure and minimises the risk that data is breached or lost.

6. Scope exclusions

No exclusions.

7. Policy review and audit log

7.1 Summary of audit and review findings

Date	Reviewed by	Audited by	Issues found	NC or Obs?	Action taken	Location of audit findings*
05/10/2020	ZO	ZO	• Audit procedure does not reflect current way of working • Some aspects of the policy are still being implemented	NC Obs	Policy re-written to better reflect current audit practice.	Internal audits\2020_21
09/02/2021	ZO	ZO	Added another interest of the government to be "Government provide us with data" Minor editing changes	obs	Minor edits	Internal audits\2020_21
16/03/2022	ZO	ZO	Minor editing changes	obs	Minor edits	Internal audits\2021_22
07/12/2022	ZO	ZO	New interested party added (research participants) Additional functions added	obs	Minor edits	Internal audits\2022_23
06/12/2023	ZO	ZO	No issues found			Internal audits\2024_24

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

7.2 Log of changes made

Date	Changes made	Changes made by	Approved by	Major or minor change?	Where archived?* (major changes only)
09/06/2020	added link to wiki page for ISF membership Added section for identification and expectations of interested parties Added section on ISMS Scope context	ZO	EH	Major	
09/02/2021	Updated Information technology to "Information and Communication technology" in section 2.	ZO		minor	
16/03/2022	Link to ISF documents corrected (moved from I drive to P drive)	ZO		minor	
07/12/2022	Added communications and operations to the list of functions	ZO		minor	
07/12/2022	Added research participants to the list of interested parties	ZO		minor	

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