Health Informatics Centre
University of Dundee

bsi ISO/IEC 27001 Information Security Management CERTIFIED
IS 802159

bsi UKAS MANAGEMENT SYSTEMS 0003
IS 802159

Security Policy

PURPOSE

This policy provides a framework for the management of information security within HIC Services. Personal data must be handled in accordance with the Data Protection Act 2018 (DPA) and in accordance with the University policy and guidance on personal data. The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This policy is supported by topic-specific Standard Operating Procedures (SOPs), which define the implementation of information security controls that are structured to address the needs of certain operational groups within the organisation.

This Policy and all other supporting policy documents shall be communicated as necessary throughout HIC Services to meet HIC Services' objectives and requirements.

SCOPE

This policy applies to:

- All those with access to HIC Services systems, including staff, researchers, visitors and contractors;
- All equipment and devices attached to the HIC Services' computer or telephone networks and any systems supplied by HIC Services;
- All information processed by HIC Services in its operational activities, including information in both digital and paper form and any communications sent to or from HIC Services.
- All services provided by external parties to HIC Services in respect of information processing facilities and business activities; and information assets, including the physical locations from which HIC Services operates.

DEFINITIONS

- **Appropriate** - suitable for the level of risk identified and justifiable by risk assessment.
- **Asset** – anything that has a value to HIC Services
- **Control** – a means of managing risk by providing safeguards. This includes policies, procedures, guidelines, other administrative controls, technical controls, or management controls.
- **Data** - Information held in electronic or paper form.
- **External Party** – (or Third Party) in relation to personal data, means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for the data controller or processor.
- **Information** - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form including textual, numerical, graphic, cartographic, narrative, and audio-visual.
- **Information Security** – Preservation of confidentiality, integrity, and availability
- **Information Systems** – Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.
- **Personal Data** – Any data held in a system, whether electronic or hard copy, that identifies a living individual (for a legal definition, see Data Protection Act 2018).

- **Policy** – overall intention and direction as formally expressed by management.
- **Risk** - the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats, and vulnerabilities.
- **Risk Assessment** – overall process of identifying and evaluating risk.
- **Third party** – person or body that is recognised as being independent of HIC Services.

RESPONSIBILITIES

ROLE	RESPONSIBILITY
HIC Operational Director	Accountable for HIC ISMS. The Operations Director of HIC Services has ultimate responsibility for information security within HIC Services and is responsible for ensuring that HIC Services is compliant with relevant external requirements, including legislation.
Information Security & Governance Manager	Responsible for HIC ISMS by leading on the compliance and framework of processes.
HIC Process Manager	Leading and deciding on the review and development of their processes. Providing training on SOPs and WIs relating to their team. Ensuring SOPs and WIs are followed and adhered to by their team.
HIC All Staff	Supporting, coordinating, and driving the initiation, review, implementation, communication, documentation, and training of processes and that which it is governed by - ISMS. Adherence to Policy, SOPs and WIs.
HIC Operational Committee	Review and approve SOPs, Policy, and Key Documents.
HIC Executive Committee	Review and approve SOPs, Policy, and Key Documents. The HIC Services Executive committee (HIC Exec), or any future equivalent body, is responsible to the University of Dundee Court and Regional NHS Boards for: 1. Ensuring that all HIC Staff and Approved Data Users are aware of this policy. 2. Seeking adequate resources for its implementation. 3. Monitoring compliance. 4. Conducting regular reviews of the policy, having regard to any relevant changes in legislation and organisational policies. 5. Ensuring that this information security policy for HIC Services' specific needs is consistent with

	the requirements of University’s policy. This security policy should identify HIC Services’ own information security requirements and provide a management framework for meeting those requirements. 6. Ensuring there is clear direction and visible management support for security initiatives.
HIC Information Security and Governance Committee	Oversight of policy and SOPs.
HIC Customers/Clients	Adherence to Policy and SOPs. Approved Data Users of HIC Services’ information and research support and management services will be made aware of their own individual responsibilities for complying with HIC Services and University policies on information security through HIC Services’ Data User Agreement and the University IT departmental Acceptable Use Policy documents. Agreements with third parties for providing, accessing, processing, communicating, or managing HIC Services’ information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

POLICY

1. HIC is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training, and awareness for information security and to ensuring continued business.

2. It is HIC’s policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory, and contractual compliance.

3. To determine the appropriate level of control that should be applied to information, a risk-based approach will be utilised to ensure residual risk is aligned to HIC’s risk appetite, as defined by the HIC Information Governance Committee.

4. Specialist advice on information security shall be made available to staff, researchers, and other users of HIC’s services.

5. All significant events suspected or actual will be reported for thorough investigation to the HIC Governance Manager, TASC and the HIC Information Governance Committee.

6. In order to meet these aims, HIC Services is committed to implementing security controls that conform to best practice. HIC Services will maintain and follow Governance Documentation covering:

- Risk Assessment and Classification of Information.
- Protection of Information Systems and Assets. Following risk assessment of HIC assets appropriate controls and procedures will be implemented to satisfy Data Controllers that any residual risks have been reduced to an acceptable level.
- Protection of Confidential Information through a set of HIC Information Security Management System (ISMS) documentation covering the secure transfer, storage, processing, access and disposal of data.

APPLICABLE REFERENCES

- Health Informatics Centre (HIC) - Standard Operating Procedures | University of Dundee, UK
- For Definitions see ISMS Glossary

DOCUMENT CONTROLS

Process Manager	Point of Contract
Jenny Johnston	hicbusiness-support@dundee.ac.uk

Revision Number	Revision Date	Revision Made	Revision By	Revision Category	Approved By	Effective Date
1.0	01/01/24	Moved SOP to Confluence from SharePoint and updated into new template	Bruce Miller and Symone Sheane	Superficial	HIC ISMS team member	10/01/24
1.1	10/04/24	Updated document control table, formatted and added in revision category	Bruce Miller and Symone Sheane	Superficial	HIC ISMS team member	10/04/24

All hard copies should be checked against the current electronic version within current versioning system prior to use and destroyed promptly thereafter. All hard copies are considered Uncontrolled documents.