Information Security Policy Summary

Introduction

The policy relates to the security of the organisation's information. Although a high proportion of the measures are concerned with the management of electronic information and associated systems, the policy also covers paper records, personnel matters and issues relating to buildings. It is therefore essential that the availability, of these assets are protected against any potential security incident.

HEFCW take Information Security very seriously and any breach of this policy could lead to disciplinary action being taken against employees.

The policy itself is detailed and technical in some areas. This summary is intended to enable all staff to gain some understanding of the security policy. However, this summary can only provide an overview. Reference should be made to the full policy to establish exact requirements.

The policy applies to all staff, agents and other organisations.

Information Security ISO27001 Control Overview

The structure of the summary below reflects that of the policy document to facilitate cross-referencing. The numbering reflects the ISO 27001:2013 control objectives and controls.

5. Information security policies

This section sets out the policies and how these are disseminated, reviewed, updated and approved:

- Dissemination of the policies to staff will be through the publication on the intranet and by providing training;
- Summaries will be available on the website for third parties or through formal processes such as procurement and contracts;
- Reviews will be undertaken every three years or after a major organisational, legislative or technological development, or the identification of new risks. Any proposed changes will be approved by Management Team and communicated to staff as appropriate;
- Annual review by Senior Management will review and consider information security issues.

6. Organisation of information security

The areas covered under organisation of information security are the security infrastructure including roles and responsibilities, confidentiality, independent review and security in respect of external parties. It also covers mobile devices and working:

- The Management Team together with the Information Security Officer will ensure that the policy is implemented. All managers are responsible for

ensuring their staff comply and all employees are personally responsible for information security in their own areas;
- Formal authorisation is required for new information systems;
- Third party contracts (where relevant) must include clauses relating to information security;
- Segregation of duties should be in place where appropriate;
- Project management processes must consider information security risks;
- Mobile working and access to systems shall be controlled and monitored;
- Staff and third parties are required to abide by security controls and processes in place when working away from the office. Awareness updates will be provided to remind users of the risks.

7. Human resources security

Issues covered relate to the security aspects of HR matters including terms and conditions of employment, training, disciplinary proceedings, and procedures for termination or change in employment:

- Job descriptions must include security roles and responsibilities as appropriate, confidentiality agreements must be signed and declaration of interest forms must be completed as necessary;
- Training will be provided and policies and procedures made available through the intranet;
- Normal disciplinary procedures apply to violations of the security policy;
- Security responsibilities are still valid after employment has terminated.

8. Asset management

This section sets out arrangements for keeping an inventory of assets, the use of information classification of both electronic and paper records, and the handling of media:

- Up to date registers of assets must be kept and all systems should have a named owner who will ensure compliance with the Information Security Policy;
- The use of information assets must be in accordance with the Acceptable Use Policy;
- Information must be labelled, handled, transferred and destroyed in line with its security classification as set out in the Protective Marking System;
- All assets, including IT and information assets must be returned on termination of employment or contract.

9. Access control

This section sets out the rules which limit access to information and systems that are required to discharge business responsibilities covering user access management, user responsibilities, network access control, operating systems access control, application and information access control:

- User access is controlled by user identifiers and passwords and the varying level of access rights depending on need;
- Good practice in the use of passwords is mandatory and automatic locking of desktops are enforced;

- Users must only have access to services they have been authorised to use;
- Appropriate controls on access to the network must be in place and authentication and secure paths must be used for remote access;
- Shared networks must have appropriate routing controls;
- Secure log-on procedures with user identification and authentication must be used.
- Access to systems utility programs and source code is restricted.
- When possible, inactive systems connections will be timed out;
- Use of systems may be monitored and audit logs maintained and reviewed regularly.
- Access to HEFCW data network is restricted to authorised employees and suppliers on the condition of compliance with the Information Security Policy.

10. Cryptographic controls

This section sets out the rules for using cryptographic controls:

- Cryptographic controls should be adopted when there is a need to protect the data and appropriate risk assessments must be carried out;
- IT must be informed before any encryption is used.

11. Physical and environmental security

This section relates to the provision of secure areas, the security of equipment, and general controls to improve information security:

- There must be physical entry controls to the building;
- Sign in and use of security cards must be enforced for staff and visitors;
- Areas within buildings, where sensitive information or equipment are held must be lockable;
- IT equipment must be installed and maintained by qualified staff according to manufacturers' instructions and be protected from power failure and other damage;
- Equipment will be disposed of in line with the agreed disposal process;
- Unauthorised access to information is reduced by an enforced clear-screen policy;
- Sensitive documents must be locked away when unattended;
- Equipment is not to be taken off-site without formal approval.

12. Operations security

The areas covered in this section are operating procedures and responsibilities, protection against malware, backup, logging and monitoring of events, managing operating system software, and information systems audits:

- Documentation should be maintained and reviewed at regular intervals;
- Change controls and arrangements for separation of development and operations must be implemented;
- Demands on systems and storage capacity are to be monitored, acceptance criteria agreed and systems tested before acceptance;
- Systems must be protected against viruses and other malicious software;
- Information must be backed up regularly;

- Logs must be kept securely;
- System documentation must be protected from unauthorised access and copies stored securely off-site;
- Operating and application systems, and updates must be tested before installation, and must only be installed by IT;
- Audits of operating systems must be planned to limit disruption.

13. Communications security

This section covers network security management and information transfer:

- Network monitoring must be undertaken regularly and logs kept securely;
- Formal agreements for information exchange should be established;
- Any information classified OFFICIAL-SENSITIVE must be protected during transfer.

14. System acquisition, development and maintenance

This section covers security requirements of information systems, security in development and support processes, and controls of test data:

- Security requirements must be documented for all information systems;
- Software and system developments shall take place in secure environments;
- Only approved software and packages will be used;
- Strict controls will be maintained over access to program source libraries;
- Change control procedures must be used and application systems testing is to be undertaken following changes;
- The Information Security Policy applies equally to any outsourced developments;
- Test plans should be developed to check for compliance with the specification and verification of security controls;
- Test data shall only be used in a controlled environment.

15. Supplier relationships

This section covers information security in supplier relationships and the service delivery management:

- Suppliers supporting information systems shall be required to agree with the Information Security Policy;
- Formal agreements shall be adopted which will include all relevant information security requirements as identified through risk assessments;
- Contracts shall be reviewed and any changes to the provision of service managed appropriately.

16. Information security incident management

This section deals with security incidents:

- Security incidents and/or weaknesses must be reported to the Information Security Officer (either directly or through line manager) and escalated as appropriate;

- The Information Security Team will record, agree corrective action and monitor incidents;
- Advice must be sought immediately from the Information Security Officer following an incident likely to lead to legal action before any further action is taken.

17. Information security aspects of business continuity management

This section covers plans for the continuity of information security:

- Information security continuity requirements shall be covered in the business continuity and IT disaster recovery plans;
- Plans shall be reviewed and tested as part of the overall business continuity process.

18. Compliance

The final section covers compliance with legal requirements, compliance with the security policies and standards and technical compliance, and systems audit considerations:

- The main legal requirements relate to the Data Protection Act (2018); the General Data Protection Regulation (2016/679); Copyright Patents and Design Act (1988); and the Computer Misuse Act (1990);
- Managers and asset owners will ensure adherence to security procedures in their areas of responsibility
- All staff are personally responsible and accountable for the handling of personal information;
- Security audits and penetration testing will be carried out periodically.

Version	Date	Comment
0.1	26/01/07	Initial draft
0.2	02/07	Amended with comments from IT
0.3	21/02/07	Amended with comments from external auditor
0.4	22/02/07	Further amendments
0.5	06/03/07	Updated with recommendations from IST meeting 28/02/07
0.6	13/06/07	Amended and reformatted
1.0	02/05/07	Approved by MB
1.1	20/02/08	Reviewed updated to include audit recommendations
2.0	14/03/08	Approved by MB
2.1	03/10/08	Amended to include recommendations from ISMS management review meeting 02/10/08
2.2	16/01/09	Style guided for EIA on 22/01/09
2.3	19/02/09	Reviewed and updated for IST
3.0	16/03/09	Approved by MB 11/03/09
3.1	18/05/10	Reviewed and updated
4.0	30/06/10	Approved by MB 07/06/10
4.1	15/07/10	Amended to include recommendations from ISO 27001 Auditor
4.2	24/01/11	Reviewed and updated
5.0	08/03/11	Approved by MB March 2011
5.1	30/04/13	Under review
5.2	02/07/13	Reviewed and updated to reflect changes resulting from new organisational policy process
6.0	16/07/13	Approved by MB 16/07/13
6.1	06/02/15	Updated to align with revised standard - ISO 27002:2013
6.2	24/04/15	Approved by IST 23/04/15. Agreed to seek MB approval.
7.0	04/06/15	Approved by MB 06/05/15 subject to EIA which was carried out 02/06/15
7.1	14/09/16	Reviewed to reflect the impact of the relocation to Bedwas on the information security controls
7.2	27/01/17	Amended to remove reference to network in IS statement
7.3	07/03/17	Include reference to new Data Disclosure Control Policy and Procedure
8.0	20/03/17	Approved by MB 15/03/17
8.1	02/08/19	Under review
8.2	30/09/19	Approved by IST17/09/19 with minor changes. Additional amendment to reflect secondment process.
9.0	11/12/19	Approved by Management Team 27/11/19

Policies, procedures and guidelines are available in alternative formats on request. Please contact info@hefcw.ac.uk