

Title	ISMS: Information Security Policy for HEFCW	
Reference	ISMS001 Annex A	
Version	5.0	
Date	8 March 2011	
Author	Senior Information Security Manager	
Approved by	Management Board	
Classification	UNCLASSIFIED	
Review Date	31 March 2012	
EIA	22 January 2009	
Version	Date	Description
0.1	26 January 2007	Initial draft of new policy
0.2	February 2007	With additions from Alison Haggett
0.3	21 February 2007	With suggestions from Chris Hilder (NCC Auditor)
0.4	22 February 2007	Version for IST consideration
0.5	6 March 2007	Updated after IST by Rachel O'Gorman.
0.6	13 March 2007	Updated and reformatted by Alison Haggett. To be taken to MB.
1.0	2 May 2007	Version approved by Management Board with agreed changes
1.1	20 February 2008	Reviewed and updated to include audit recommendations
2.0	14 March 2008	Version approved by Management Board with agreed changes
2.1	3 October 2008	Minor amendments as agreed at the ISMS management review meeting 02/10/08
2.2	16 January 2009	Style guided for EIA
2.3	19 February 2009	Reviewed and updated for IST consideration
3.0	16 March 2009	Approved by MB on 11/03/09
3.1	18 May 2010	Reviewed and updated
4.0	30 June 2010	Approved by MB 07/06/10
4.1	15 July 2010	Amended after recommendation from ISO 27001 Auditor
4.2	24 January 2011	Reviewed and updated for MB approval
5.0	8 March 2011	Approved by MB March 2011

This document is available on the Intranet, in Braille, large print, on electronic CD and in DAISY (digital audio). Should you or someone you know require this in an alternative format, please contact us on (029) 2068 2218 (voice or via BT TypeTalk 0870 240 95 98) or email equality@hefcw.ac.uk.

HEFCW Information Security Policy

Information Security Policy Statement

The purpose of the information security policy is to protect the HEFCW, its staff and public from all information security threats, whether internal or external, deliberate or accidental.

The information security policy is characterized here as the preservation of:

- a) confidentiality: ensuring that information is accessible only to those authorised to have access;
- b) integrity: safeguarding the accuracy and completeness of information and processing methods;
- c) availability: ensuring that authorised users have access to information and associated assets when required;
- d) regulatory: ensuring that HEFCW meets its regulatory and legislative requirements.

HEFCW has set up an Information Security Team to introduce and maintain policy and to provide advice and guidance in its implementation.

HEFCW requires that all breaches of information security, actual or suspected, will be reported to and investigated by the Information Security Officer (Alison Haggett ext 2300)

HEFCW undertakes to provide appropriate information security training for all staff.

Third parties are required to ensure that the confidentiality, integrity, availability, and regulatory requirements of all business systems are met.

HEFCW will produce, maintain and test Business Continuity Plans.

It is the responsibility of all users of the network to adhere to the policy.

Members of the Management Board are responsible for ensuring the policy is implemented and adhered to by their staff, third parties and suppliers.

I expect and require all staff to adhere to the policy. Failure to do so may result in the use of disciplinary procedures as appropriate.

Authorised by

Philip Gummett
Chief Executive

Information Security Policy Summary

Introduction

The policy relates to the security of HEFCW'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. 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 structure of the summary reflects that of the policy document to facilitate cross-referencing. The numbering reflects the ISO 27001 control objectives and controls.

5. Security policy

This section deals with how staff will be made aware of the policy and how the policy will be reviewed and updated:

- Dissemination of the policy will be through the publication on the intranet together with summaries targeted at specific audiences and by providing training;
- Reviews will be undertaken annually and, if necessary, updating will follow organisational changes or the identification of new risks. Changes to this policy and associated annexes will be approved by Management Board.

6. Organisation of security

The areas covered under organisation of security are the security infrastructure including roles and responsibilities; confidentiality, independent review; and security in respect of external parties:

- The Management Board 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 must include clauses relating to information security.

7. Asset management

This section sets out arrangements for keeping an inventory of assets (hardware, software, systems) and the use of information classification of both electronic and paper records:

- 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 and managed in line with its security classification as set out in the Protective Markings Scheme;
- Information marked restricted must be locked up and destroyed by shredding when no longer required.

8. 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.

9. 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 restricted information (eg HR) or equipment (eg servers) are held must be lockable;
- ICT 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 policy;
- Unauthorised access to information is reduced by an enforced clear-screen policy;
- Restricted documents must be locked away when unattended;
- Equipment is not to be taken off-site without formal approval.

10. Communications and operations management

The areas covered in this section are: operating procedures and responsibilities; third party arrangements; systems planning and acceptance; protection against malicious and mobile code; backup; network security management; media handling; exchange of information; and monitoring:

- Change management standards and arrangements for separation of development and operations must be implemented;
- The risks associated with third party contracts must be assessed and contracts should address security issues and should be monitored;
- 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;
- Information on redundant disks or other media must be destroyed before disposal or proof that the information has been destroyed must be provided if a disposal company is used. Steps must be taken to protect information when a machine is taken off-site for repair;
- Network monitoring must be undertaken regularly and logs kept securely;
- System documentation must be protected from unauthorised access and copies stored securely off-site;
- Formal agreements for information exchange should be established
- Any information classified higher than restricted sent electronically must be protected.

11. Logical access controls

This section sets out the rules which limit access to information and systems to that required to discharge business responsibilities covering: user access management; user responsibilities; network access control; operating systems access control; application and information access control; mobile computing and home-working:

- User access is controlled by user identifiers and passwords and the varying level of access rights depending on need as set out in the Access Control Policy;
- Good practice in the use of passwords is mandatory and automatic log outs of PCs 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 is restricted. Inactive systems connections will be timed out;
- Use of systems will be monitored and audit logs maintained and reviewed regularly;
- Policies for mobile and home computing will include requirements for security controls;
- Laptop guidelines and mobile phone policy must be adhered to.

12. Development and maintenance

This section covers security requirements of information systems, correct processing in applications; cryptographic controls; security of system files; and security in development and support processes:

- Data validation and correction procedures must be used;
- Encryption of information should only be used when authorised by the ICT Team;
- 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.

13. Information security incident management

- 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.

14. Business continuity management

This section covers plans for Business Continuity:

- All aspects of business continuity are managed by the Business Continuity Group;
- The Business Continuity Plan is managed within the Shadow Planner system;
- Testing of the plans will be undertaken at least once a year;
- All staff are required to undergo training in the use of the system.

15. 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 (1998); 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;
- Security audits will be carried out periodically.