I.T. Security Policy

Purpose and Context

The purpose of the I.T. Security Policy is to ensure business continuity and to minimise operational damage by reducing the impact of security incidents.

Scope

This Policy applies in respect of all I.T-related systems, hardware, services, facilities and processes owned or otherwise made available by the University of Huddersfield or on its behalf, or which are connected to the University network and servers, including for the avoidance of doubt any personally-owned devices that are used in connection with University activities (together, **I.T. Systems**).

1. Introduction

1.1. The threats we face

The University is facing increasing security threats from a wide range of sources. Systems and networks may be the target of a variety of attacks, including computer based fraud, surveillance or vandalism. Such threats to I.T. security are generally expected to become more widespread, more ambitious and increasingly sophisticated.

Because of increasing dependence on I.T. systems and services, the University is becoming more vulnerable to security threats. The growth of networking, cloud services and mobile devices presents new opportunities for unauthorised access to computer systems or data and reduces the scope for central, specialised control of I.T. facilities.

In addition, legislation has been introduced, which places legal requirements on the University to protect personal privacy and to ensure the confidentiality and security of information and that its use is within the law. The pertinent legislation includes the Data Protection Act 2018, the Copyright, Designs and Patent Act 1988, The Regulation of Investigatory Powers Act (RIPA) 2000, the Computer Misuse Act 1990 and the Counter-Terrorism and Security Act 2015 (which encompasses the 'Prevent' duty).

This Policy contains terms relating to the classification of data. There are three classifications: sensitive, confidential and general. Information about which types of information fall into the different categories is set out in the I.T. Security Procedure Manual (see below).

This Policy should be read in conjunction with the University Data Protection Policy Computing Regulations,Research Integrity and Ethics Policy and the Retention and Disposal schjedule

1.2. I.T. Security Procedure Manual

This Policy is supported by a separate document, known as the **I.T.** Security Procedure Manual, which contains detailed guidance and operational procedures to help to ensure that users of the University's I.T. systems do so in compliance with this Policy.

2. Compliance

The University's Regulations Governing the Use of Computing Facilities set out the responsibilities of anyone using University I.T. Systems and are included in the Student Handbook of Regulations.

This Policy supports and expands the provisions in the University's Regulations Governing the Use of Computing Facilities. All members of the University, including staff, students and any other user with access to University I.T. Systems, must comply with this I.T. Security Policy.

3. Information Handling

3.1. Classification of information

An inventory will be maintained of all the University's major corporate I.T. assets and the ownership of each asset will be clearly stated. Within the inventory, the information processed by each I.T. asset will be classified according to sensitivity.

3.2. Precautions against hardware, software or data loss

Equipment must be safeguarded appropriately, especially when left unattended. Files downloaded from the internet, including files attached and links within email, must be treated with caution to safeguard against Phishing type attacks for both malicious code and the harvesting of personal information.

3.3. Disposal of equipment

When permanently disposing of equipment containing all types of storage media (including removable media) all sensitive or confidential data and licensed software should be irretrievably deleted during the disposal process. Damaged storage devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the permission of the information asset owner.

3.4. Working practices

The University advocates a clear screen policy particularly when employees are absent from their normal desk and outside normal working hours. Employees should log out or lock their workstations when not in use. In addition, screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons. This applies to both fixed desktops and mobile devices.

3.5. Off-site removal of data

Removal off-site of the University's sensitive or confidential information, either in print or held on any type of computer storage medium, including tablets, phones or USB drives whether owned by the University, or not, should be authorised by the relevant Dean or Director and only in accordance with the University Data Protection Policy. Sensitive or confidential information must not be kept in a cloud storage service which is not approved by the University.

3.6. Backup and recovery

Information owners must ensure that tested backup and system recovery procedures are in place. Backup of the University's information assets and the ability to recover them are important priorities. All system managers must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles; especially where such files may replace files that are more recent.

3.7. Archiving

The archiving of information must take place with due consideration for legal, regulatory and business issues, with liaison as needed between IT staff, records managers and data owners, and in keeping with the University's Retention Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

3.8. Information lifecycle management

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. Day to day data storage must ensure that current information is readily available to authorised users. Any archives created must be accessible in case of need.

3.9. Sensitive or confidential information

Sensitive or confidential data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured and in accordance with the University Data Protection Policy. Sensitive or confidential data (as defined in the IT Security manual) should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

3.10. Use of electronic communication systems

The identity of online recipients, such as email addresses and fax numbers should be checked carefully prior to dispatch, especially where the information content is sensitive or confidential. Information received electronically must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

Sensitive or confidential information should only be sent electronically (e.g. by email) to external recipients when it is encrypted or protected by a password.

3.11. Access to personal or individual data for systems management purposes

Some individuals may need access to personal data identifying individuals, or to data which belongs to others, in order to manage systems or to fix problems. These individuals will be required to sign a data protection declaration before they are sanctioned to carry out these duties.

4. Mobile and Remote Computing

4.1. Authorisation

Those remotely accessing information systems, data or services containing sensitive or confidential information must be authorised to do so by an appropriate authority, usually the line manager.

4.2. Use of computing equipment off-campus

Computers or other devices should only be used off-campus for University related activities if University-approved security controls are in place. This provision applies to all equipment, irrespective of ownership. If sensitive or confidential information is being stored or accessed from off-campus, only the member of staff concerned should use the equipment, unless the highest levels of security are in use and an approved access solution, such as via Unidesktop, is used. No sensitive or confidential information is to be stored on any I.T. System that has not been approved by the University.

4.3. Travelling

Portable computing or storage devices are vulnerable to theft, loss or unauthorised access when travelling. University-approved mobile device management software must be installed and activated at all times. Devices must be provided with an appropriate form of access protection such as a password or encryption to prevent unauthorised access to their contents. Equipment and media should not be left unattended in public places and portable devices should be carried as hand luggage. To reduce the opportunities for unauthorised access, automatic shutdown features should be enabled. Passwords or other similar security tokens for access to the University's systems should never be stored on mobile devices or in their carrying cases. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons

Export and import controls apply when travelling to certain countries which restrict the use of encrypted devices. Advice should be taken from IT Support before any travel arrangements are made.

5. Outsourcing and Third Party Access

5.1. External suppliers

All external suppliers who have access to University I.T. Systems or data must work under the supervision of University staff and in accordance with this Policy. A copy of the Policy will be made available to the supplier, if required.

5.2. Confidentiality declaration

The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality declaration to protect its information assets. This will be the responsibility of the system owner. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of this Policy.

5.3. Service level agreements

Any facilities management, outsourcing or similar company with which the University may do business must be able to demonstrate compliance with the University's I.T. Security Policy and must enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

6. Operations

6.1. Building access control

Areas and offices where sensitive or confidential information is processed will be given an appropriate level of physical security and access control. Line managers will provide information on the potential security risks and the measures used to control them to staff with authorisation to enter such areas.

6.2. Operational procedures

System owners must ensure that the procedures for the operation and administration of the University's business systems and activities are documented and that those procedures and documents are regularly reviewed and maintained. Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of I.T. security incidents that might result in financial or other material damage to the University.

6.3. Procedure for reporting of concerns

System owners must ensure that procedures are established and widely communicated for the reporting to IT Support of security incidents and suspected security weaknesses in the University's I.T. Systems. They must also ensure that mechanisms are put in place to monitor and learn from those incidents. Procedures must be established for the reporting of software malfunctions and faults in the University's I.T. Systems. Faults and malfunctions must be logged and monitored and timely corrective action taken.

6.4. Change management

Changes to operational procedures or hardware must be controlled to ensure continuing compliance with the requirements of this Policy and must have management approval. Development and testing facilities for business critical systems will be separated from operational facilities and the migration of software from development to operational status will be subject to formal change control procedures. Acceptance criteria for new information systems, upgrades and new versions will be established and suitable tests of the system carried out prior to

migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place. Procedures will be established to control the development or implementation of all operational software, which must be approved by University IT Strategy Group before introduction and a Privacy Impact Assessment must be completed and approved by the Records Management Service for any new system that will involve the processing of personal data. All systems developed for or within the University must follow a formalised development process.

6.5. Risk assessment

The security risks to the information assets of all system development projects will be assessed by system owners and access to those assets will be controlled.

7. User Management

7.1. User identification

System owners must ensure that procedures for the registration and deregistration of users and for managing access to all information systems are established to ensure that all users' access rights match their authorisations. These procedures must be implemented only by suitably trained and authorised staff. All users must have a unique identifier (user ID) for their personal and sole use for access to all the University's information services, which should authenticate against the institutional directory where practicable.

7.2. ID security

The user ID must not be used by anyone else and associated passwords must not be shared with any other person for any reason. Password management procedures must be put into place to assist both staff and students in complying with best practice guidelines.

7.3. Access control standards

System owners must establish appropriate access control standards for all information systems which minimise information security risks yet allow the University's business activities to be carried out without undue hindrance. Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Procedures must be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the organisation. Users' access rights must be reviewed at regular intervals.

7.4. Starters, Leavers and Affiliates

Line managers must ensure that access to I.T. Systems is only available to employees during their period of employment. In particular, line managers must ensure that the system access of leavers is withdrawn as soon as employment is terminated. Those requesting Affiliate status must ensure that system access does not extend beyond the requirements of the Affiliate's activities. Those requesting Affiliate status must also ensure that system access is withdrawn as soon as the

Affiliate's relationship with the University ceases.

7.5. User training

All those who wish to access the University's I.T. Systems must have successfully completed the training which is deemed appropriate for their role. Advice on what training is required is available from line managers or direct from the team who manages each system (e.g. ASIS Support or Agresso Support).

8. System Planning

8.1. Authorisation

New I.T. Systems relating to teaching, research or the administration of the University, or enhancements to existing systems, must be authorised by the University's I.T. Strategy Group. The business requirements of all authorised systems must specify appropriate security controls. The implementation of new or upgraded software or hardware must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

8.2. Risk assessment and management

System owners must ensure that the information assets associated with any proposed new or updated systems are identified, classified and recorded, and a risk assessment, including, where relevant, a privacy impact assessment, is undertaken to identify the probability and impact of security failure. Equipment supporting business systems must be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

8.3. Access control

System owners must ensure that access controls for all I.T. Systems are set at appropriate levels in accordance with the value and classification of the information assets being protected. Access to operating system commands and application system functions must be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

8.4. Testing

System owners, in consultation with Computing and Library Services, must ensure that prior to acceptance, all new or upgraded systems or hardware are tested to ensure compliance with this Policy, access control standards and requirements for ongoing information security management.

9. I.T. Systems Management

9.1. Staffing

I.T. Systems must be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff must have relevant training in I.T. security issues.

9.2. Access control

System owners must ensure that access controls are maintained at appropriate levels for all I.T. Systems and that any changes of access permissions are authorised by the manager of the system or application. A record of access permissions granted must be maintained. Access to all I.T. Systems must use a secure login process and access may also be limited by time of day or by the location of the initiating terminal, or both.

System owners must ensure that all access to systems containing sensitive or confidential information is logged to identify potential misuse of systems or information. They must also ensure that password management procedures are put into place to ensure the implementation of security procedures and to assist users in complying with best practice guidelines.

Remote access to the network must be subject to robust authentication as well as appropriate levels of security. Virtual Private Network, wireless, and other connections to the network are only permitted for authorised users.

Access to operating system commands must be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored.

9.3. Change management

System owners must ensure that the procurement or implementation of new or upgraded software is carefully planned and managed and that any development for or by the University always follows a formalised development process with appropriate audit trails. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. Business requirements for new software or enhancement of existing software must specify the requirements for information security controls.

The implementation, use or modification of all software on the University's business systems must be controlled. All software must be checked before implementation to protect against malicious code.

Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by Computing and Library Services according to procedures laid down by them.

All changes must be properly tested and authorised before moving to the live environment.

9.4. Network design

Computing and Library Services must ensure that the University data and telecoms network is designed and configured to deliver high performance and reliability to meet the University's needs whilst providing a high degree of access control and a range of privilege restrictions. Appropriately configured firewalls or other security devices must be used to protect the networks supporting the University's business systems.

9.5. Logging

System owners must ensure that security event logs, operational audit logs and error logs are properly reviewed and managed by qualified staff. System clocks must be regularly synchronised between the University's various processing platforms.

Acknowledgement

This document draws on copyright information contained in the UCISA Information Security Toolkit (ISBN 0-9550973-0-4) Edition 2.0, August 2005 and the UCISA Information Security Management Toolkit, Edition 1.0, March 2015.

POLICY SIGN-OFF AND OWNERSHIP DETAILS

Document name:	IT Security Policy
Version Number:	2.0
Equality Impact Assessment:	December 2018
Approved by:	SMT on 28 February 2019
Effective from:	1 May 2019
Date for Review:	February 2020
Author:	Information Security Manager
Owner (if different from above):	
Document Location:	https://www.hud.ac.uk/media/policydocuments/IT-Security-Policy.pdf
Compliance Checks:	Breaches of the Regulations handled under the respective student or staff University disciplinary processes.
Related Policies/Procedures:	• IT security Procedure Manual • Computing Regulations • Using Your Own Device Policy • Data Protection Policy

REVISION HISTORY

Version	Date	Revision description/Summary of changes	Author
V1.0	October 2017	First draft using Policy Framework. Minor drafting updates.	Head of BQP
V2.0	December 2018	Additional links to policies added (DP Act 2018 and Uni DP policy) Working practices section - applies to mobile devices as well as desktops Clarity on email attachments that should be password protected (external only) References to Phishing Inclusion of removable media in disposal section Privacy filter explicitly mentioned in travelling section PIAs now checked by Records Management instead of DP officer	Information Security Manager