The University of Huddersfield
I.T. Security Procedure Manual

1. Introduction

1.1. The purpose of this Procedure

The I.T. Security Procedure Manual is designed to be used in conjunction with the University of Huddersfield I.T. Security Policy.

It gives practical advice to members of the University and describes procedures that must be followed in order to implement the provisions of the I.T. Security Policy.

This document will be updated regularly in the light of the security threats we face and as the technological environment changes.

Terms defined in this Procedure will have the same meaning as used in the I.T. Security Policy.

1.2. Scope of this Procedure

This Procedure applies to all I.T. Systems.

2. Compliance

All members of the University, affiliates and third parties will comply with this I.T. Security Procedure.

3. Data Confidentiality Levels

3.1. Introduction

The security procedures that are appropriately applied to a given set of information will depend on the characteristics of that information. It is important, therefore, to have an easy-to-understand information classification scheme that indicates the level of protection that must be applied.

3.2. Information classification

	Access	Examples
Sensitive	To be accessed by a strictly controlled group of users, with owner's consent, and with highest security levels applied. Not to be passed on without consent. Subject to the Data Protection Act.	• Sensitive personal data (i.e. information about a person's racial or ethnic origin, political opinions, religious beliefs, health, criminal record and trade union membership) • HR record • Business critical information such as financial or contractual details. • Research data concerning topics such as terrorism or radicalisation.

	Access	Examples
Confidential	To be kept secure and accessed only for business need. To be passed to third parties only as required for the fulfilment of the University's contract with the individual, except with permission. Subject to the Data Protection Act.	A person's address, phone number, student record, results, general financial information. Information which is covered by ethical guidelines, or by research-related subject consent.

	Access	Examples
General	Not restricted	Data not relating to living individuals or confidential business information about the University or it partners and affiliates, or not sufficiently specific as to allow identification.

3.3. Access to personal data

It is important that those who, as part of their system management or troubleshooting roles, have access to personal data understand the implications of the Data Protection Act and how it affects them. For further information on Data Protection at the University see:

http://www.hud.ac.uk/informationgovernance/dataprotection/

All staff who are likely to have access to such data must sign a confidentiality declaration, which is retained by the School or Service. A pro-forma is given in Appendix B.

4. Personal Computer Security

4.1. Passwords

Passwords are the key to many systems and applications. A password helps to prove identity, and to ensure personal privacy and helps to protect the privacy of the data being accessed. Poor passwords compromise security. Passwords are managed by the University's FastPass self-service and management system. Passwords must comply with the advice in the following sections.

4.1.1. Good passwords

A good password is one that is difficult to guess. It will use a wide range of characters in an unpredictable order. A good password is one that can be remembered easily and typed in quickly so that anyone looking over your shoulder will not be able to see what you are typing.

A password must;

- be at least ten characters long
- contain a mixture of letters (upper and lower-case), numbers and punctuation
- not appear in any dictionary or any other list
- have no personal connection with the owner

example: Sg2MgVSgMx! (the first letter of each word of a line of a song or poem, with punctuation and numbers added)

4.1.2. Bad passwords

A bad password is simply one that is easy to guess, or so difficult to remember that the owner writes it down.

A password must not;

- be blank, or obvious, such as 'letmein', 'opensesame', or 'password'
- be less than ten characters long
- be written down, left in an open drawer, or pinned to a monitor
- contain simple sequences of letters or numbers such as qwerty, or 123456, or the reverse of a simple sequence
- contain a phone number or date
- be based on a nearby object at the time of choosing, such as 'monitor', or 'keyboard'
- appear in a dictionary (in any language) or any other list
- have a personal connection with the owner such as a car registration or pet's name.

examples: Ule4G (too short), Csb1-016 (room number and too short), 0143aikon (product name reversed and too short)

4.1.3. Changing passwords:

Passwords must be regularly changed, but not so often that they cannot be remembered.

4.1.4. Safeguarding passwords:

- if a password must be written down, it must be kept in a secure location; alternatively, hints could be written down and not the password itself
- passwords must not be disclosed to anyone else. If a password has been revealed, it must be changed immediately

- passwords must not be stored on a computer, or other device. The "save my password" feature must never be used
- passwords must never be sent electronically unless the transfer is encrypted
- computers left unattended must be logged off or have their keyboard locked
- public computers such as a cybercafé or lab PCs, must be shut down and restarted after use.

4.2. Securing your computer when you are away from your desk.

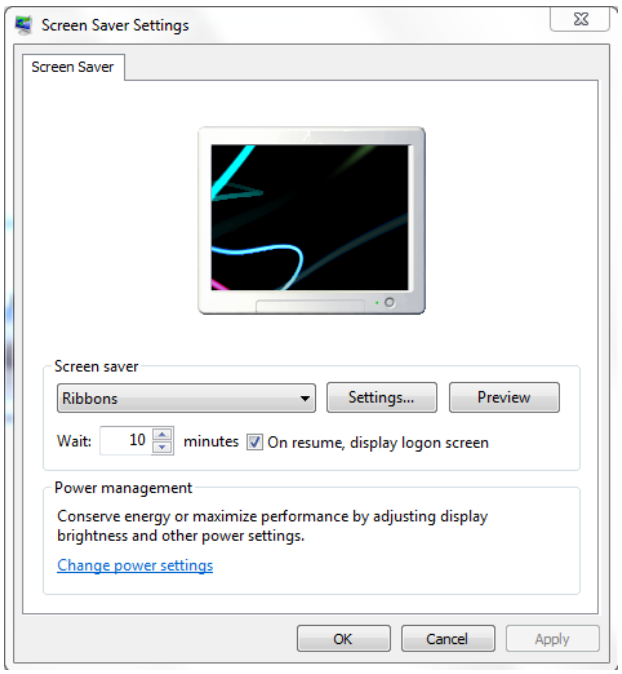
When a computer is left unattended, it is essential that that no unauthorised person can gain access to it.

There are a number of simple techniques that should be used.

- **Log out.**
  This will prevent any access until a valid username and password is entered.
- **Lock the keyboard.**

  To do this, press  and the L key at the same time

  To unlock the computer, use the Ctrl Alt and Del keys and re-enter your usual login password. Your computer will resume from the point at which you locked it.
- **Use a password-protected screensaver.**
  A screensaver with password-protection can be set to activate after a certain number of minutes of keyboard inactivity. To do this, right-click on a blank part of the Windows desktop area and choose **Personalize.** Choose the **Screen Saver** option to display the following screen;



Select a screensaver using the drop-down arrow, select a number of minutes to wait until it activates and put a tick in the **On resume display logon screen** then click **OK.** After the specified number of minutes of keyboard inactivity, the screensaver will activate. To remove it, you will need to re-enter your

usual login password and your computer will resume at the point at which the screensaver activated.

5. Security While Off-Campus

5.1. Purchasing laptops, smartphones, tablets and other mobile devices.

There are several additional checks that must be performed when a mobile device is purchased.

It is the responsibility of the person arranging the purchase to find out if the customer intends to use the portable device to hold or access sensitive or confidential data. If so, encryption must be used (see below).

Any data must be stored in such a way that it can easily be backed up or identified for encryption. Any data of value to the University must be placed on secure institutional storage such as the SAN or Unishare on return to campus. IT Support or local technical staff will be able to advise on the best way to achieve this.

5.2. Encryption

If a mobile device is being used to carry or access sensitive or confidential information, it must be encrypted. Additionally, the device must be secured with a password or passcode, if this is possible.

The use of remote management tools which can be used to locate, disable and wipe the data from a device is also required, regardless of whether the device is issued by the University or belongs to the individual user.

Advice on the options available can be obtained from IT Support, or local technical staff.

All University laptops must have encryption software installed and enabled. Any laptop which is subsequently re-imaged must have the encryption software re-installed.

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.

5.3. Using your own device

The provisions of this IT Security Procedure Manual apply to all devices that are being used for University purposes irrespective of their ownership. If you are not able to comply with the requirements stated here, you must not use the device for University business purposes.

The University's Using Your Own Device Policy describes acceptable use pertaining to staff whilst using their personally-owned devices to access University computing systems and services and the storing of confidential data on those devices.

5.4. Mobile device security

Users of mobile devices must follow these guidelines:

Mobile devices must be treated as carefully as if they were the user's own property.

Mobile device security is the responsibility of the user.

Mobile devices must be securely locked away when not in use and must not be left unattended in a public place.

If a securing cable is used, one key must be kept with the owner and another in a secure separate location.

When left in a vehicle, mobile devices must be locked away in the car boot and not left on view inside a vehicle.

Mobile devices must not be left within sight of ground floor windows or within easy access of external doors.

University-approved mobile device management software must be installed and activated at all times. Any devices not owned by the University that access University information (such as by syncing email) must also have University-approved mobile device management software installed and active.

Stolen or lost smartphones must be reported to Telephone Services (telephoneservices@hud.ac.uk).

Mobile devices that have been linked to a University email account and then subsequently lost or stolen must be remotely wiped using Outlook Web Access (staffmail.hud.ac.uk). Go to **Options**, then select **Mobile Devices**.

Irrespective of ownership, users of mobile devices that access University I.T. Systems or data are bound by the terms of the University Regulations Governing the Use of Computing Facilities. These regulations make it clear that The University's computing facilities are provided for the furtherance of the University's mission in connection with a course of study or contract of employment.

5.5. Using cloud storage (e.g. Dropbox, Google Drive, OneDrive)

Sensitive or confidential information should only be kept in a cloud storage service that is approved by the University and a Privacy Impact Assessment must be carried out before any such approval is given. In all other cases sensitive or confidential information must be stored on University servers only.

Many cloud storage systems are based outside the European Economic Area and are not secure. They are not subject to the same data protection levels as the U.K. To prevent loss, ensure that there are additional downloaded copies and that these are kept appropriately secured with respect to the sensitivity and/or confidentiality of the data.

5.6. Software security

Users of University-owned mobile devices must not install any unapproved software. This applies to software downloaded from the Internet, unlicensed or illegal software, or software obtained from any other source.

Users must not circumvent any built-in device security systems (known as 'jail-breaking' or 'rooting') in order to download apps from sources other than the official app stores, or to obtain 'super-user' privileges over the device.

5.7. Virus protection

University-owned mobile devices must have approved security software which includes, as a minimum, anti-virus and anti-spyware components, installed and active. For any queries, in the first instance contact IT Support (01484 472795), or local technical staff.

The anti-virus software's database of virus definitions must be updated regularly.

If a virus is discovered it must be reported immediately to I.T. Support (01484 473737).

University-approved anti-virus software is also available to download for personally-owned computers from the staff and student portals.

5.8. Password security

In addition to the general guidelines given in Section 4 concerning passwords, the following additional provisions apply to devices intended for use off-campus.

- passwords must not be displayed on screens as they are entered.
- when allocated a new/temporary password for start-up use by the system's manager/ administrator the user must immediately change it.
- passwords must be changed on change of staff or staff resignation.
- a start-up password or passcode must be used if this feature is available.

5.9. Losses and confidentiality/security breaches

All incidents where data security is potentially compromised, must be reported directly to IT Support. If sensitive or confidential information is involved, the person with responsibility for the data, such as the Dean/Director of the relevant School/Service, must also be informed immediately so that an assessment of the required action can be undertaken. The University Data Protection Officer must also be informed if the incident involves the loss or unauthorised disclosure of personal data.

Computing and Library Services will investigate the incident and establish the nature and potential security threat resulting from it.

Reportable incidents include, but are not limited to:

- Loss/theft of hardware.
- Loss/theft of software/data.
- Unauthorised access.
- Misuse of system/privileges.
- Illegal software download.

5.10. Off-campus access to data

When accessing data via an off-campus access connection such as Unidesktop, whether at home, via wireless, on another user's PC or in a public place, users must ensure that:

- sensitive or confidential information is secured by the use of passwords or file encryption
- information is not divulged to any family members or to anyone else outside the University
- up-to-date anti-virus and anti-spyware software is used
- the connection is closed immediately after use.

6. Equipment and Data Disposal

The University has an environmentally-responsible procedure for the disposal of all electrical and electronic equipment. In relation to the disposal of I.T. equipment, a secure data erasure procedure is integrated into the process.

6.1. Disposal of equipment or data.

This procedure applies to PCs, printers, hard drives, interface cards, laptops, tablets, external hard drives, smartphones, USB memory sticks, memory cards and any other devices that may potentially contain data.

Data stored on these devices could potentially contain sensitive or confidential data and must never be thrown away in bins or skips.

Leavers who take their equipment with them when they go must ensure that all University-related data is removed first. Software may only be taken away if the licence terms permit this.

6.2. Disposal procedure

Contact IT Supportt (it.support@hud.ac.uk, 01484 473737) to register your equipment collection.

All materials that are not re-usable will be disposed of in an environmentally-approved manner.

All data storage devices will be erased to the required standard and if not re-usable will be physically destroyed.

Computing & Library Services will retain all documentation related to the disposal.

7. Systems Security

7.1. Access to business systems

Authorisation to use any of the University's business applications must be requested from the system owner by the applicant or their line manager. The prospective user may be required to undertake some basic training prior to enabling use of the live system.

Requests for access to systems that contain sensitive or confidential information (such as ASIS, iTrent, or PAPA) are handled specifically. Authorisation is granted by the System Owner (e.g. for ASIS use, the ASIS Director) and the prospective user must sign a separate Data Protection declaration and undertake training before being given access to the system.

Anyone unsure of the procedure for obtaining authorisation to use any system should contact I.T. Support on 01484 473737 in the first instance.

7.2. Access by non-University members

The University has established the Affiliates Procedure for handling the granting of I.T. privileges to those who have a relationship with the University but who are not its students or employed by it. Access should only be requested and will only be granted to the extent required for the relevant purpose. All requests for affiliate access must use the procedure detailed on the Computing & Library Services website: https://www.hud.ac.uk/staff/it/affiliates/

7.3. System backups

System backups play an important role in ensuring business continuity in the event of an I.T. equipment or software failure by providing a method of restoring systems to pre-failure state.

When designing system backups a number of factors must be taken into consideration such as the rate at which system data changes and the length of time tolerable for the system to be out of operation. In essence, a system backup must be designed to capture all information required to restore the system to a working state as quickly as possible and to a point at which a minimum amount of data or transactions have been lost.

For major University systems such as email, Unilearn, student records, SAN directories and many others, system backups are performed by Computing & Library Services. However there are other I.T. systems which are managed at a local level by Schools and Services for which system backups must be performed by local staff. Anyone seeking advice about backups should contact I.T. Support on 01484 473737 in the first instance.

Computing and Library Services does not carry out system backups that capture data stored locally on PCs (for example on C: or D: drives), laptops or other mobile devices. Backup for data on these devices must be carried out by their owners.

7.4. Change management procedures

Changes made to systems under the management of Computing & Library Services must be governed by the agreed departmental change management procedure and, if appropriate, the University I.T. Strategy Group. Systems not under the management of Computing & Library Services must also use a change management procedure appropriate to the importance of the data to the University. Advice on a suitable process can be obtained from the Chair of the University I.T. Strategy Group.

7.5. Counter-terrorism legislation

Following notification by the Police of material which may contravene the Terrorism Act 2006, the University has two working days in which to remove it.

Owners of servers are required to provide details to Computing & Library Services. This must include any web services delivered on behalf of the University outside the University network, e.g. by broadband connections.

To comply with the law, system owners will be given one hour during normal working hours to remove notified material, or the server will be shut down. Outside normal working hours the Computing & Library Services Senior Management Team will arrange for the server to be shut down at the earliest convenience.

Where research is being undertaken which might require access to security-sensitive research material, including that restricted by the Terrorism Act 2006 or subject to military or security clearances, ethical approval must be obtained and appropriate arrangements must be put in place for the access to and storage of such information in accordance with the procedures set out in the University Research Ethics & Integrity Framework and in line with UUK guidance.

Pursuant to the Counter-Terrorism and Security Act 2015, the University is under a statutory duty to prevent people being drawn into terrorism; further information will be

made available in due course about how this duty might impact University I.T. Systems and their use.

7.6. Event log auditing

System audit logs must be created and maintained as appropriate to the importance of the system to the University.

System audit logs must be discussed with system owners to identify those areas of business systems which must be subject to audit logging to preserve the integrity of data.

Logs for all server-based business systems must be reviewed each week.

Logs for network logon/logoff, telephone traffic and web page access must be kept for at least 12 months.

8. Security and Third-Parties

8.1. Confidentiality declaration

Where the risk to sensitive or confidential data is deemed sufficient, the University requires that third-parties, such as suppliers, abide by a confidentiality declaration. There is an example pro-forma in Appendix A.

9. Network Security

9.1. Attachment of servers to the network

The attachment of a server to the network brings with it a number of security considerations. These are focussed on the data the server contains and the people who are going to access it. For these reasons, both the server and the network need to be protected.

Before the attachment of new servers, changes to existing servers or removal of servers, system owners or their representatives must contact Computing & Library Services via I.T. Support tel: 01484 473737 to ensure that the correct procedures are followed.

9.2. Firewall access procedures

In order to maintain an appropriate level of information security, the University of Huddersfield's computer network is separated from the Internet by a network firewall.

For many of the University's business systems to operate it is necessary to allow network traffic to pass through this firewall on an incoming and/or outgoing basis using a series of network 'port' numbers.

As there are many network ports which are commonly used by a variety of systems and where these are deemed to provide little or no risk to the University's information security, these are routinely configured as 'open ports' within the firewall. However, on occasion there may be a requirement for a system to use a network port which is not routinely open. In these instances it is necessary to undertake an assessment of the business need and associated risk factors prior to the port being opened in the firewall.

The procedure below describes how this must be done for clients outside Computing & Library Services.

A request for opening ports in the firewall must be made in the first instance to IT Support (tel: 01484 473737).

IT Support then obtain full details of the service being requested and who will require access to it including the following specific details:-

- A list of port numbers
- Whether traffic on these port numbers is required on an internal or external basis and whether the traffic is single or bi-directional
- MAC & IP address of the device/s for which port access is required.
- The preferred date from which access is desired. If access is only required for a limited period, then an end date must also be provided.
- Confirmation of appropriate Ethics Approval having been obtained where relevant (e.g. where the request is for access to blocked or restricted websites).

The Network Team will carry out an assessment of the request based on a combination of security best-practice and existing University of Huddersfield security policies.

If, on the basis of the information provided, the Network Team approves the request, the requestor will be notified via IT Support.

The Network Team will implement the change and maintain a record of firewall access which has been approved through this procedure.

If, on the basis of the information provided, the Network Team is unable to approve the request, further discussions will take place in order to obtain additional information, extra authorisation, or an alternative approach.

Where additional authorisation is felt to be necessary, this will need to be provided by the appropriate Head of Department or School Dean in the form of a written Service Level Agreement to be drafted by 2nd Line IT Support.

The Network Team will also maintain a record for access requests which have not been approved.

The procedure below describes how this must be done for clients within Computing & Library Services.

A request for opening ports in the firewall must be made to the Network Team mailbox. The request must include full details of the service being requested and who will require access to it including the following specific details:

- A list of port numbers
- Whether traffic on these port numbers is required on an internal or external basis and whether the traffic is single or bi-directional
- MAC & IP address of the device/s for which port access is required.
- The preferred date from which access is desired. If access is only required for a limited period, then an end date must also be provided.

The Network Team will carry out an assessment of the request based on a combination of security best-practice and existing University of Huddersfield security policies.

If, on the basis of the information provided, the request is approved, the Network Team will implement the change and maintain a record of firewall access which has been approved through this procedure.

If, on the basis of the information provided, the Network team is unable to approve the request, then the request will be forwarded to the Head of Computing Services for approval.

The Network Team will also maintain a record for access requests which have not been approved.

9.3. Wireless authentication procedure

Although providing many opportunities for more flexible use of I.T., wireless technologies are, in general, inherently insecure and therefore use of them on campus needs to be strictly controlled and monitored to ensure appropriate levels of security and regulatory compliance.

Only wireless networks that have been approved by Computing & Library Services will be permitted.

Any unauthorised wireless networks will be disconnected from the campus network without notice.

Authorisation to participate in the development of wireless networks can be sought via IT Support.

Personally-owned equipment can be connected to the University wireless network provided that it meets the required standards, and usage is in accordance with the University Regulations Governing the Use of Computing Facilities and the I.T. Security Policy. Any queries can be discussed with IT Support on 01484 473737.

9.4. Modem attachment

A modem is an electronic device that connects computers via a telephone line, allowing the exchange of information over the line. They are most commonly found in conjunction with fax machines, dial-up connections to remote facilities and servers which have remote access support arrangements with external suppliers.

Unless secured properly, such as by the use of dial-back, modems represent a potential security threat to the University's I.T. systems, therefore their use and configuration must be authorised by Computing & Library Services.

Any unauthorised modem connections which are identified will be disconnected from the campus network without notice.

Authorisation to install a device with a modem can be sought via IT Support.

9.5. Unauthorised monitoring

The use or provision of tools which allow the monitoring of network traffic (“sniffing”) is not allowed. Those who believe that they have a legitimate business need to use such tools (for example in teaching) should contact the Head of Computing Services in Computing and Library Services to discuss how this can be carried out with due regard to the relevant legislation and without breaching the personal security of network users.

10. Appendix A. Confidentiality Declaration

The University of Huddersfield.

C O N F I D E N T I A L I T Y D E C L A R A T I O N

OUTSOURCING AND THIRD PARTY ACCESS TO UNIVERSITY I.T. SYSTEMS

<Insert organisational details here>

< organisation name> undertakes to the University of Huddersfield that it shall (and shall procure that its employees, agents and sub-contractors shall):

a. keep confidential all information of a confidential nature (whether written or oral) that it obtains or receives as a result of the discussions leading up to, entering into, or performance of, any contract with, or let by, the University (the **"Information"**);

b. not without the prior written consent of the University disclose the Information either in whole or in part to any other person save those of its employees, agents and sub-contractors involved in the implementation or evaluation of the contract who have a need to know the same for the performance of their duties;

c. use the Information solely in connection with the implementation or evaluation of the contract and not otherwise for its own benefit or the benefit of any third party.

Provisions (a), (b) and (c) above shall not apply to the whole or any part of the Information to the extent that it can be shown by **<organisation name>** to be:

i. known to **<organisation name>** prior to the date entered below and not obtained directly or indirectly from any other party; or

ii. obtained from a third party who lawfully possesses such Information which has not been obtained in breach of a duty of confidence owed to the University; or

iii. in the public domain in the form in which it is possessed by the University other than as a result of a breach of a duty of confidence owed to the University; or

iv. required to be disclosed by legal process, law or regulatory authority.

Signed on behalf of <**organisation name>**

Name: _____

Signature: _____

Date: _____

11. Appendix B. Data Protection Statement

ACCESS TO PERSONAL OR INDIVIDUAL DATA

It is important that those staff who, as part of their system management or troubleshooting roles, have access to personal or individual data understand the implications of the Data Protection Act 1998 and how it affects them.

Under the terms of the Act, access to personal or individual data should be restricted to those data items which are necessary in order to perform system management or troubleshooting duties.

Additionally, data must not be disclosed to a third party without the express consent of the data subject or owner. In practice this means that documents, information, or the means to access them, should not be given to other members of the University or to external individuals or agencies, including the police, unless in exceptional circumstances; see below.

Staff should not use any additional access privileges granted to them to view or obtain confidential information relating to their own role(s) within the University, either as staff or student, which would not normally be available to them. Where any such access is likely to occur in the performance of a system management or similar task, staff should consult their line manager before proceeding.

In certain exceptional circumstances, personal or individual data may be given to a third party, for example to assist the police in a criminal investigation but only on production of a formal documented request.

Police enquiries should be directed to the Head of Registry.

A line manager may request access to the data stored in an absent employee's individual storage area, in order to assist the operation of the University, such as to retrieve lecture notes or assessment material required urgently.

Staff should also be aware of the consequences of accessing data beyond that which is necessary, or of disclosing personal or individual data without permission. In certain cases this could lead to disciplinary action or prosecution of the individual.

Any queries regarding what information may or may not be accessed or disclosed should be addressed to the University Secretary.

For further information on the University's Data Protection Policy see:

http://www.hud.ac.uk/informationgovernance/dataprotection/

I understand the implications of the Data Protection Act as outlined above.

Name: .....,.....

School/Service: .....

Signature: .....

Date: .....