

IT Security Procedure Manual

Purpose and Context

The IT Security Procedure Manual is designed to be used in conjunction with the [University of Huddersfield IT Security Policy](#). The procedures in this document apply to all University staff and affiliates and are not intended for students.

It gives practical advice to members of the University and describes procedures that must be followed in order to implement the provisions of the [IT Security Policy](#), the purpose of which is to reduce the opportunity for information security and cyber security breaches to occur as well as limit the impact of these on the University should they do so

This document will be updated regularly in light of the ever-evolving security threats we face and as the University's technological environment changes.

Terms defined in this Procedure will have the same meaning as those used in the IT Security Policy.

Scope

These procedures apply to all IT-related systems, hardware, services, facilities and processes owned or otherwise made available by the University of Huddersfield or on its behalf, whether utilising the University's network and servers or those provided through cloud-based environments. These procedures include, for the avoidance of doubt any personally owned devices that are used in connection with University activities (together, **IT Systems**).

1. Compliance

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

2. Data Confidentiality Levels

2.1. Introduction

The security procedures that are appropriately applied to a given set of information will depend on the characteristics of that information and the impact to the University should that information be inadvertently disclosed, changed, or destroyed without proper authorisation. It is important, therefore, to have an easy-to-understand information classification scheme that indicates the level of protection that must be applied.

Information classification

	Access	Examples
Sensitive	To be accessed by a strictly controlled group of users, with the data owner's consent, and with the highest security levels applied. Not to be passed on without consent. Subject to the Data Protection Act.	<ul style="list-style-type: none"> • Aligns to the GDPR's definition of special category data • 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.	<ul style="list-style-type: none"> • Aligns to GDPR's definition of personal data • 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	<ul style="list-style-type: none"> • Data not relating to living individuals or not sufficiently specific as to allow identification of individuals. • Non-confidential business information about the University or its partners and affiliates.

2.2. 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:

<https://www.hud.ac.uk/informationgovernance/dataprotection/>

Where a role requires access to specific business systems that contain sensitive personal or financial information, individuals may be required to sign a data protection declaration before they are sanctioned to carry out these duties. A pro-forma is given in Appendix B of this document. Line managers will make staff aware if they are required to do this and line managers will oversee the process within their School or department. The completed pro-forma will be retained by the School or department where the completion of data protection declaration is required.

3. Personal Computer Security

3.1. Passwords

Passwords are the key to many systems and applications. A password helps to prove identity and to protect the privacy of the data being accessed. A poorly chosen password can lead to the compromise of system security. As well as being used to log in to IT systems, passwords may also be used to secure information sent between two parties. All passwords must comply with the advice in the following sections, even where a system does not enforce the same requirements

3.1.1. Good passwords

A good password is one that is difficult for others to guess. Current best practice is to use a 'passphrase' made up of three random words, rather than a single word password. 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 sixteen characters long
- contain at least one upper case and one lower-case letter
- not appear in any dictionary or any other list
- have no personal connection with the owner

examples: Coffeebrickshoes, Balloonpurpledogs

3.1.2. Bad passwords

A bad password is one that is easy for others to guess, or so difficult to remember that the owner writes it down. Malicious software that is designed to break passwords use lists of commonly known weak passwords and so dictionary words are more likely to succeed when as passphrase, as described above, is not used. A determined hacker will use social media profiles to gather personal information that staff may use in passwords.

A password must not;

- be blank or less than sixteen characters long
- be a single dictionary word or simple sentence in any language
- be obvious, such as 'letmein', 'opensesame', or 'password'
- contain simple sequences of letters or numbers such as qwerty, abcdabcd, or 123456, or the reverse of a simple sequence
- be based on a nearby object at the time of choosing, such as 'monitor', or 'keyboard'
- have a personal connection such as a car registration, family members' or pet's name, phone number or date of birth

3.1.3. Changing passwords:

If you have a strong passphrase as stated above, you do not need to regularly change it. However, if you think your account has been compromised or your password is known by someone else then you must change your password immediately.

If you have been enrolled into the Self Service Password Reset (SSPR) system you can change your password or unlock your account yourself at any time. For information on how to change your password, on either a University computer or through the SSPR system, visit [here](#).

3.1.4. Safeguarding passwords:

- Passwords must never be physically written down or stored digitally where they can be discovered
- It is not permissible to share your individual user password(s) to anyone. Actions and activities carried out on IT systems are recorded and tied to the user ID used, regardless of who is actually using the account.
- Where passwords used for administrative purposes must be shared amongst several individuals the password must be stored in a secure

password manager accessible only to those that need it. If a physical backup is required, then these must be stored in a fire safe with a combination lock known only to restricted persons.

- 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 of a web browser must never be used
- Passwords must not be reused across multiple accounts where the account holder has more than one account, for example where they hold two different roles at the University or have a secondary administrator account.
- Passwords must not be sent electronically unless the transfer is encrypted and never sent with the item it is protecting
- Avoid using your University email address to register for non-work-related web sites and systems. Where this is unavoidable never use your University password. If an external web site is compromised your credentials may be stolen and used to gain access to University systems.
- System administrators should ensure that systems are configured to limit the number of failed logins attempts to no more than 10, at which point an account should become locked out. This will protect a system from password guessing and brute force attacks.

3.1.5. Reusing Passwords:

- Wherever possible University systems will link back to the central directory systems – this is known as 'single sign on' or SSO and reduces the need to create and remember numerous passwords. Those implementing new systems should endeavour to integrate logins to the University's account directories, either Active Directory, for on-campus applications; or Azure Active Directory, for cloud-hosted Software as a Service (Saas) application.
- Where SSO is not supported and you are required to set a password to each system, the password must be unique. It is not permitted to reuse passwords across multiple University systems.
- Do not use your University password for any non-University web site or system even where you need to register with your University email address.

3.1.6. Sharing Passwords:

The passwords you use to log in to University systems must be kept secret at all times and never shared with others. Passwords are linked to your account identity and therefore any action undertaken with that identity is attributed to you.

Where line managers have a responsibility to share the temporary password of a new account with a new member of staff or affiliate the username and password must not be sent together in the same email. Best practice is to provide one or both elements of these details over the telephone on the account holder's first day or as part of an induction. Login credentials must not be shared with new members of staff/affiliates until their first contracted day. The account holder must change the password immediately to one that meets the password requirements above and that is known only to themselves.

There are however times where a password may be used for other purposes, such as protecting a file sent between two parties and there is a requirement to share this password with the intended recipient. In such cases email should be avoided, sharing this password via a telephone call or SMS to a verified number provides good separation. The password must never be sent with the file that it is protecting.

Wherever possible share documents using modern methods such as OneDrive or SharePoint, these require the recipient to log in to access the document and remove the need to share a password at all. OneDrive or SharePoint also provide a method to withdraw access to documents when it's no longer needed unlike email which once sent externally cannot be retracted.

3.1.7. Default Passwords:



For those that procure, configure or install new IT equipment or systems it is important to know that these will often come with default passwords which have been set by the vendor. It is not uncommon for a vendor to reuse the same password on all of the products it distributes and then publish this password in instruction manuals. These vendor-supplied default passwords may be known others and for this reason passwords that come with any system, software or device must be changed before deployment and build processes should include this step where relevant.

3.2. 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 two simple techniques that should be used.

- **Log out.**
This will prevent any access until a valid username and password is entered. When you log out of a computer it also allows security updates to take place so is good practice if you won't be using the computer for longer periods of time.
- **Lock the keyboard.**
This is a quick and easy way to secure your computer if you are stepping away for a short period of time.

Microsoft Windows	Press  + L key at the same time.
Apple macOS	Click the  Icon and select Lock Screen or

	Press Command+Control+Q keys at the same time
--	---

3.3. Using Email Securely

3.3.1. Identifying malicious emails

Email continues to be one of the most common, and successful methods used by criminals to spread malicious software and undertake social engineering aimed at capture login credentials and other sensitive information. The University has a sophisticated filtering system which significantly reduces the likelihood for malicious emails to reach staff and student mailboxes, however some will still make it through. There are different types of email that may be received, with various levels of threat:

- Spam - email which is generally not malicious or specifically a threat but is counterproductive, usually unsolicited and can lead people to sign up to services with University Mailboxes. When these sites are compromised University email addresses may be captured and become part of riskier activities.
- Phishing - carries a higher risk as they're usually designed to trick IT users in to disclosing sensitive information about themselves or others or capture login credentials which are used by or sold to criminals to use for unauthorised access to systems.
- Malware - The biggest threat comes from email containing attached malware or including clickable links to websites that host malware, potentially leading to the successful installation and propagation of malware including ransomware.

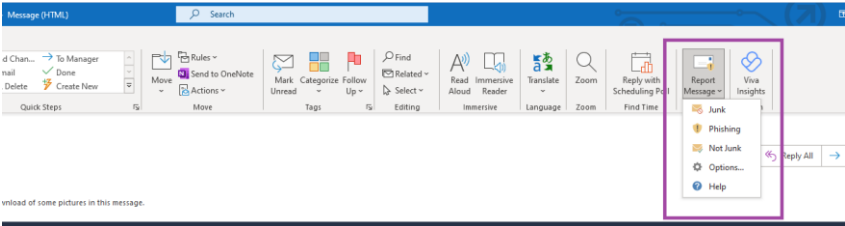
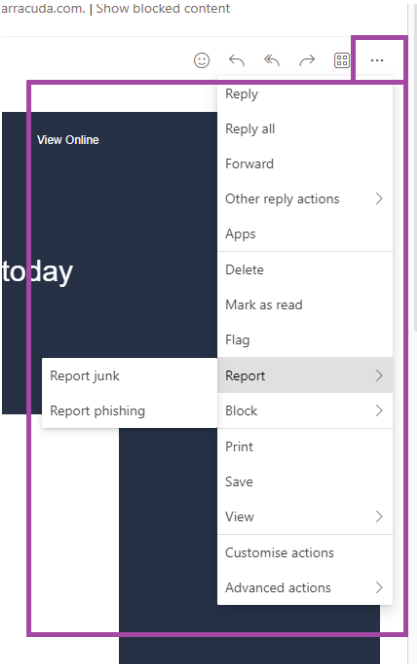
Malicious emails can be very convincing and difficult to spot, though there are some general ways to spot them and help avoid falling victim:

- Be cautious of emails that are received from an unknown sender, or from someone you know but where the subject, content or request is unusual.
- Double check the sender's email address for attempts to impersonate a genuine email address, for example 'it.support@hud-uni.com'.
- Malicious emails may try to provoke an emotional response such as panic and urgency or appear to come from a senior or authority figure.
- Generic greetings, spelling mistakes, and emails that are received outside of office hours are also indicators of it not being genuine.

If in doubt never reply to the email; or click any links, open attachments, scan QR codes or call phone numbers contained within the suspicious email. You should always verify the authenticity of a dubious email with the individual directly if you know them or gain a genuine contact number for a company from their official web site.

3.3.2. Reporting spam, phishing, and malicious emails

Emails that are suspected or identified of being spam, phishing or malicious should be reported using the 'Report Message' button in the Outlook desktop client or Outlook web browser:

<p>Outlook desktop client</p>	<p>Open the email, click “Report Message” in the top right hand corner.</p>  <p>Chose “Junk” for spam emails, and “Phishing” for emails suspecting as being used for phishing or containing malicious links, attachments and QR codes.</p>
<p>Outlook via a web browser</p>	<p>Open the email. Firstly click “...” (three dots symbol) in the top right hand corner to open ‘more actions’, the click “Report”.</p>  <p>Chose “Junk” for spam emails, and “Phishing” for emails suspecting as being used for phishing or containing malicious links, attachments and QR codes.</p>

When asked if this action should be reported to Microsoft, chose "Report". This not only removes the email from the inbox but provides Microsoft with valuable information that can help prevent similar items being delivered in the future.

If you open an attachment, click a link, or scan a QR code from an email that you later realise is probably malicious please contact the IT Support as soon as possible so that steps can be taken to investigate.

4. Security While Off-Campus

4.1. 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).

It is the responsibility of the device user to inform Computing and Library Services (CLS) IT Support via the link [here](#) if changes in circumstances mean that a device will need to hold or access sensitive or confidential data so that checks can be undertaken to ensure the appropriate protection is in place.

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 OneDrive or SharePoint. IT Support or local technical staff will be able to advise on the best way to achieve this.

Approved mobile device management software must be installed and activated on University owned mobile and portable devices at all times. At the time of writing the minimum expectation is:

- University Windows desktop computers are enrolled into Microsoft Endpoint Configuration Manager (ECM).
- University Windows laptop computers are enrolled into Microsoft InTune.
- University Apple macOS and IOS devices are enrolled in to JAMF.
- University Android mobile phones and tablets will be enrolled into Microsoft InTune over Academic year 2023-2024 and device users will need to comply with requests to enroll their device to InTune when requested.

4.2. Encryption of data on mobile devices and portable storage

Sensitive or confidential information stored on laptops, other mobile devices and portable storage, such as a USB storage device must be encrypted. Additionally, the

device must be secured with a password, passcode, Touch-ID or Face-ID wherever this is possible. Advice on the options available can be obtained from IT Support, or local technical staff.

The use of USB storage devices is a common source of computer viruses, malware and spyware infections and should be avoided. Where data must be stored on USB storage, business data must be stored on a dedicated work USB stick to avoid cross-contamination with personal files; reduce the likelihood of a virus or malware infection on University computers; and minimise the risk of loss of University data on personal USB storage devices.

USB storage devices which are not from a known and trusted source must not be attached to a University computer. Criminals are known to leave USB storage devices infected with malware in public places in the hope of someone plugging it in leading to the compromise of that computer. Files on trusted USB storage devices must be scanned with an anti-virus product before use or transfer to University systems and network drives.

All University laptops must have encryption software installed and enabled. Any laptop which is subsequently re-imaged must have the encryption software re-installed. The user must never disable the encryption protection in place as this can put University information at risk.

Hard disk, or data at rest, encryption algorithms used must not be vulnerable, that is susceptible to a brute force attack. At the time of writing the minimum acceptable standard that can be implemented is the Advanced Encryption Algorithm (AES) with a 256-bit key length, also known as AES-256. There is currently no known practical attack that could brute-force an AES 256 key.

The data at rest encryption software must remain free from vulnerabilities that could be used to bypass the protection it offers, through the application of software upgrades and security patches.

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.

4.3. 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.

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 and must be adhered to at all times

The use of personally owned devices that don't meet the University's requirements introduces risk to business systems and data. If you are not able to comply with the requirements stated here, you must not use the device for University business purposes.

Access to sensitive or confidential information using your own device should be avoided and instead an approved access solution such as Unidesktop should be used so that data remains within University systems.

Staff should regularly check their own computers for University data and remove it when no longer needed, it is good practise to ensure copies of important information exist in University storage systems before deletion from personally owned computers.

Data stored on staff owned devices should be encrypted to protect it from digital and physical theft, guidance on how to achieve this can be found [here](#). Microsoft BitLocker hard disk encryption is not available on Windows 10 Home edition (HE). Users of Windows 10 HE must not save Personal or Sensitive data to their computer unless an appropriate data at rest encryption product is installed and activated. Users of Apple's MacOS must ensure Apple's FileVault is turned-on, or an appropriate third-party product is installed and enabled.

Computing and Library Services (CLS) will continue to implement systems that support the Using Your Own Device Policy and which may prohibit access to University systems and data from personal devices that do not meet minimum security standards or devices that are identified as having an increased risk profile, for example a device that has anti-virus protection installed but where a scan has not recently been completed; or a discovered threat could not be removed.

4.4. Mobile device security

Users of university owned 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.
- Mobile phones and tablets must have an initial PIN to access the device of no less than six digits or a password in line with the password requirements. This may be complimented with fingerprint ID once the PIN is configured.
- University-approved mobile device management software must be installed and activated at all times.
- Never attempt to uninstall or change the settings of the security protections that have been configured on devices.

- Stolen or lost mobile devices must be reported to the IT Service Desk (it.support@hud.ac.uk) IT Support will take the appropriate steps to ensure the security of your account and University data which may reside on the phone through a password reset and remote wipe of the device where possible.

Irrespective of ownership, users of mobile devices that access University IT 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, research or contract of employment.

4.5. Using cloud storage

Sensitive or confidential information must never be uploaded to a cloud storage service that is not approved by the University.

Microsoft OneDrive is the University's approved cloud storage platform and is available for use by all staff. OneDrive has undergone due diligence to assess the security and privacy implications of its use for the storage sensitive and confidential University information.

Many cloud storage systems are based outside of the European Economic Area in countries which do not have UK equivalent data protection laws. Cloud storage systems are often designed for convenience rather than built with the security needed for sensitive business data in mind and are therefore inherently not secure.

If a business need arises to use a cloud storage service other than Microsoft OneDrive, approval must be sought through the Opportunity Statement process and a Privacy Impact Assessment carried out before any such approval is given.

To prevent loss, ensure that additional downloaded copies are kept within appropriate University systems and that these are kept correctly secured with respect to the sensitivity and/or confidentiality of the data.

4.6. Software security

Users of University-owned mobile devices (laptops, tablets and mobile phones) must not install any unapproved software as this can lead to the unintentional introduction of malicious software such as viruses and ransomware. This applies to software downloaded from the Internet, unlicensed or illegal software, or software obtained from any other source. Always consult with CLS prior to installing additional software.

Users must not circumvent any built-in mobile 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.

4.7. Virus protection

Regardless of ownership, all mobile devices must have approved security software which includes, as a minimum, anti-virus and anti-spyware components, installed and active. This applies to all access to University systems and data and not just that labelled Personal or Sensitive, because undetected malicious software can capture log in credentials and spread malware to other files and folders.

Anti-virus software relies on daily updates to its virus definitions to be effective and to know about new viruses. Users must ensure that devices, including spare stock are regularly connected to the network or Internet in order to receive these important updates.

The user must never disable or attempt to make changes to the anti-virus protection in place as this can put University systems and information at risk.

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

4.8. Password security

In addition to the general guidelines given in Section 3 concerning passwords, the following additional provisions apply to mobile devices that are 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 PIN of at least 6 digits must be used if this feature is available.

4.9. Losses and confidentiality/security breaches

All incidents where data security is potentially compromised, must be reported directly to IT Support immediately (01484 473737). 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.

CLS 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 including computers, laptops and smartphones
- Loss/theft of software/data including that stored on USB memory sticks
- Unauthorised access.
- Misuse of system/privileges.
- Illegal software download.

The University Data Protection Officer must also be informed if the incident involves the loss or unauthorised disclosure of personal data. If you need to notify the

University of a suspected data breach, you should complete the [Data Breach Evaluation Form](#).

4.10. Off-campus access to data

In addition to the requirements described in section 4.3 – Using your Own Device, when using either personally owned equipment or University issued IT equipment being used off campus careful consideration must be given to the surrounding environment to ensure that others cannot see your screen or overhear your conversations.

Public networks and Wi-Fi connections such as those in hotels and coffee shops may not be secure and should be avoided. It is trivial for someone to set up a fake Wi-Fi access point with a trusted name to encourage connections which they can then use to view your internet traffic or gain access to your device. Where connection to a public WiFi network is unavoidable always take steps to verify the Wi-Fi network with the venue before connecting. If you are unsure of the security of any wired or wireless network then you should not use it.

Wherever possible multifactor authentication (MFA) will be enforced for access to University systems when being used away from campus. MFA validates the account holder's identity and reduces the risks relating to weak, shared or compromised passwords. The recommended form of MFA is through the Microsoft Authenticator mobile application as this allows users to validate their connection via once touch approval. MFA through SMS text message is also available though this requires the user to type the string of digits they received into the authentication portal.

5. Equipment and Data Disposal

The University has an environmentally-responsible procedure for the disposal of all electrical and electronic equipment. This involves working with an approved 3rd party supplier for the secure disposal of IT waste. In relation to the disposal of IT equipment, a secure data erasure procedure is integrated into the process.

5.1. 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.

Where devices have been used to store sensitive or confidential data and must never be thrown away in bins or skips, as tools do exist to recover data even when devices are considered broken

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.

5.2. Disposal procedure

Contact IT Support via the HudHelp link [here](#) 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.

CLS will retain all documentation related to the disposal.

6. Systems Security

6.1. Access to business systems

University staff will be provided with a unique computer account providing access to a limited range of business resources. This will usually consist of an email mailbox, personal storage, and collaboration tools such as OneDrive, SharePoint and Teams. Shared storage areas used by the wider team may also be provided.

Authorisation to use any of the University's business applications must be requested by the applicant or their line manager and approved by the system owner. 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 and the prospective user may be requested to 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 create a support ticket with IT Support in the first instance, Via the link [here](#).

6.2. Access by non-University members

The University has established the Affiliates Procedure for handling the granting of IT 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 CLS website:

<https://www.hud.ac.uk/staff/it/affiliates/>

Those requesting Affiliate status must ensure that system access does not extend beyond the requirements of the Affiliate's activities and ensure that the accounts created for those with Affiliate status is withdrawn as soon as the Affiliate's relationship with the University ceases. It is good practise to add an expiry date to such accounts when they are requested, to cover the extended period of the relationship, this date can be extended where required.

6.3. System backups

System backups play an important role in ensuring business continuity in the event of an IT 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, Azure, student records, SAN directories and many others, system backups are performed by CLS. However there are other IT systems which are managed at a local level by Schools and Services for which system backups must be performed by local staff. All systems have a responsibility to be aware if their systems is backed up by CLS or that responsibility is with themselves, for advice relating to backups contact IT Support in the first instance via the link [here](#).

CLS does not backup data stored locally on PCs and laptops (for example on C: or D: drives) or other mobile devices. Data should not be stored locally on devices as it is susceptible to loss should the hard disk break or the device is stolen. Where this cannot be avoided, the device owner is responsible for moving copies of data from the device to University systems, such as shared drives, OneDrive and Sharepoint to reduce the risk of data loss. Additional information on where to save documents online can be found [here](#).

6.4. Change management procedures

Changes made to systems under the management of CLS must be governed by the agreed departmental change management procedure and, if appropriate, the Strategic Projects, Processes and Infrastructure Group (SPPIB). Systems not under the management of CLS 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 SPPIB.

6.5. 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 CLS. 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 CLS 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 UK guidance.

Pursuant to the Counter-Terrorism and Security Act 2015, the University is under a statutory duty to prevent people being drawn into terrorism.

6.6. 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.

To support post-incident investigation, security logs from firewalls, authentication systems and VPNs should be available for a minimum of 90 days. Wherever possible server activity logs should also be kept for this duration.

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.

6.7. Encryption of data in transit

Data in transit is information as it travels from a computer to web server or between two systems. Most web sites now apply transit layer security (TLS) encryption to protect sensitive personal information or passwords entered into them. A secure web site address will start with 'https', a web site address starting with 'http' is not protecting the information being entered into it with encryption, meaning any person or system that can intercept the information can read it.

All University web services should use data in transit encryption as default for all traffic types and over all network, including internal networks. Web services which store or transact any form of sensitive or confidential information or accept user logons must encrypt the data in transit.

System owners must ensure that the security protocols used on their web services are not vulnerable to known attacks. At the time of writing the minimum acceptable standard is TLS version 1.2, though version 1.3 which is faster and more secure should be considered for new implementations. TLS version 1.1 and below as well as all versions of Secure Sockets Layer (SSL) are insecure and must be disabled. HTTP Strict Transport Security (HSTS) is a security policy which instructs browsers to remain in a secure state when accessing a web site, wherever possible HSTS must be applied to University hosted web sites and web applications.

6.8. System design and implementation

New systems and services should be designed and implemented with security in mind. Applying security later is generally more costly and complex to achieve. As a minimum, those responsible for creating new systems or configuring any new device should:

- Use security frameworks such as the Open Web Application Security Project ([OWASP](#)) Top 10 to ensure common coding mistakes are avoided in new web services.
- Undertake system hardening through removing or disabling all software and services that are not required, reducing the attack surface of the system and

opportunity for vulnerabilities to occur.

- Provide system users with the minimum rights required to use the system as standard, also known as 'the principle of least privilege'. Administrative tasks should require escalation using separate privileged accounts to approved individuals only on a need to have basis.
- Follow vendor build guidelines and security baselines to ensure secure configurations of applications, operating systems and network hardware. Most vendors offer these with detailed explanations of how and why to apply them.
- Build and deploy from 'gold' images and documented procedures to guarantee consistency and remove the risk of manual error that can lead to weaknesses in individual deployments. Ensure system and device users cannot change these standards without authorisation.

Firewalls should be used to provide segregation at network boundaries, particularly where the data classification of systems differ. Traffic should be blocked by default and permitted only as required following the principle of least privilege.

A demilitarised zone (DMZ) creates segregation between system components based on their role. A firewall creates a barrier between web facing components such as a web site or web application and any backend applications and database servers. Only the web facing element of the system are positioned in the Internet facing DMZ. This design ensures that should an internet facing web server become compromised; there is limited data stored on the server; and there is limited scope for the attacker to move inbound to more secure networks hosting servers that do hold sensitive data.

Proposed system implementations should include a detailed network design diagram which describes all system components, their role in the solution and the interactions between them. Designs should be validated, and system components installed into the appropriate network for its role.

6.9. Vendor advisories

System owners and those responsible for the maintenance of hardware, software and firmware of any device or system connected to the University network should sign up to receive for vendor security advisories related to that product. These security advisories provide an early warning about newly discovered vulnerabilities in their software as well as information about malicious parties that may be seeking to exploit them. Vendor advisories often provide detailed information on how to remediate vulnerabilities and provide temporary work arounds where security patches are not yet available. Additionally, these advisories are likely to include any end of support dates for software well in advance, giving time plan system upgrades or replacements.

6.10. System security testing

IT systems hosted and maintained by the University will be periodically tested for known vulnerabilities and weaknesses caused by misconfigured security controls or bugs in vendor released software. Security testing allows CLS and local technical

staff to take mitigating actions that secure the systems before a person with malicious intent can exploit the vulnerability. Exploits for newly discovered vulnerabilities can be available within hours of them being published.

The industry Common Vulnerability Scoring System (CVSS) is a common way to assess known vulnerability and provides a score rating based on how easy it for an attacker to exploit the vulnerability and the business impact should this happen. The table below defines the CVSS version 3.0 score rating, the related severity and target timescale for applying vendor patches or configuration fix to remove the found vulnerability. Any reboot needed to apply the patch must also occur within the timescale.

CVSS Rating	Severity	Patch / Fix Target
9.0 – 10.0	Critical	Within 14 days “immediately”
7.0 – 8.9	High	Within 1 month “earliest opportunity”
4.0 – 6.9	Medium	Within 3 months “routine patching cycles”
0.1 – 3.9	Low	Within 6 months “routine patching cycles”
0.0	None	N/A “routine patching cycles”

In exceptional circumstances, such as where vendor advisories or threat intelligence suggest there is an active campaign to find and exploit specific vulnerabilities, a patch may need to be implemented faster than those requirements outlined in the table above.

Applications hosted and maintained by third party providers, such as cloud Software as a Service (SaaS) systems, must be tested by the vendor at least annually. Proof of testing must be provided by the vendor prior to University data initially being uploaded or entered into the application. This gives confidence that third party providers are actively undertaking vulnerability and patch management to protect their systems and University information.

6.11. System patching

System owners must ensure that all system components including hardware, operating systems and applications that they are responsible for remain within vendor support and that these are regularly patched with software security updates in order to reduce the opportunity for the exploit of known vulnerabilities.

It is good practice to implement automated patching wherever possible as this ensures that security and functionality updates are applied on a regular basis without the need for manual intervention, which may otherwise be difficult at busy times. Where this is not possible, a formal patching schedule should be implemented by the system owner which allocates dedicated time for the planning, communication, testing, and implementation of system patches.

System patches must be applied within the timescales detailed in 6.10.

For Microsoft products CLS maintains an enterprise Endpoint Configuration Manager (ECM) platform and encourages system owners across all areas of the University to enrol their systems on to it, providing asset management and software version visibility. It is also possible that current manual tasks can be automated such as patching and consistent policy enforcement. To find out more contact IT Support via the link [here](#).

7. Security and Third-Parties

7.1. 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.

7.2. Third party remote access to university systems

System owners are responsible at all times for the network access that third party suppliers have, and the actions undertaken by them. It is good practice that wherever possible supplier remote access accounts remain disabled by default and enabled temporarily, as required to undertake a specific task, at the request of the system owner or administrator limiting access to agreed timeframes to reduce the opportunity for unauthorised activities that may lead to data loss or unintended disruption. Accounts must be immediately deleted when no longer required.

This ensures that should a third-party support partner's network become compromised there is limited onward access to the University network and systems, for unauthorised persons to undertake what is known as a 'supply chain attack'.

All activities undertaken by third party suppliers must be agreed in advance to reduce the opportunity for unplanned changes and system downtime.

8. Network Security

8.1. Attachment of servers and other infrastructure to the network

The attachment of digital infrastructure including network hardware and servers to the network brings with it a number of security considerations. These are focussed on the data the infrastructure transmits or contains and the people who are going to access it. For these reasons, all elements of digital infrastructure need to be protected.

The University has a published network attachment protocol that provides instruction and guidance on the steps you need to take before attaching a device to the network.

8.2. 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 via the link [here](#).

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 required for a system or service to operate
- 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.

In all cases the Network Team will routinely undertake housekeeping of the firewall rules in place. Where a rule has not been used for 90 days the open port may be removed unless there is an approved and documented exception.

8.3. Wireless authentication procedure

Although providing many opportunities for more flexible use of IT, wireless technologies are, in general, inherently insecure and extend the network beyond physical boundaries, 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 CLS will be permitted.

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

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 [IT Security Policy](#). Any queries can be discussed with IT Support.

8.4. Modem, router and wireless access point attachment

Modems, routers and wireless access points are devices which extend or link networks together. Plugging one of these devices into the University campus network could inadvertently permit unauthorised access from insecure and unapproved devices. Wireless access points would also extend the secure campus network outside of the physical confines of University buildings, to car parks and publicly

accessible areas where unauthorised people can then connect. It is trivial for someone to connect to a poorly configured wireless access point provided onward access to the secure campus network, greatly increasing the risk to University systems and data.

The connection, configuration or use of modems, routers and wireless access points is permitted only by the CLS Network and Telecoms Team, who will use only approved solutions.

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

Requests for new or additional modem, router and wireless access points can be sought via IT Support via the link [here](#).

8.5. Unauthorised monitoring

The use or provision of tools which allow the monitoring of user activity, including but not limited to: 'sniffing' network traffic or the use of 'keyloggers' that capture user keyboard input, is not permitted. Those who believe that they have a legitimate business need to use such tools (for example in teaching) should contact the Head of IT Services in CLS to discuss how this can be carried out with due regard to the relevant legislation and without breaching the personal security of network users.

9. Appendix A. Confidentiality Declaration

The University of Huddersfield.

CONFIDENTIALITY DECLARATION

OUTSOURCING AND THIRD PARTY ACCESS TO UNIVERSITY IT 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: _____

10. 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 2018 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:

POLICY SIGN-OFF AND OWNERSHIP DETAILS

Document name:	IT Security Procedure Manual
Version Number:	5.0
Equality Impact Assessment:	Not applicable – not a policy document
Approved by:	CLS SMT
Effective from:	18 September 2023
Date for Review:	August 2024
Author:	Information Security Manager
Owner (if different from above):	Deputy Director and Head of IT Services
Document Location:	https://staff.hud.ac.uk/media/policydocuments/IT-Security-Procedure-Manual.pdf
Compliance Checks:	Results of annual and/or other Security Testing (including penetration testing).
Related Policies/Procedures:	IT Security Policy Computing Regulations Using Your Own Device Policy

REVISION HISTORY

Version	Date	Revision description/Summary of changes	Author
V1.0	October 2017	First draft using Policy Framework. Minor drafting updates.	Derek Heathcote
V2.0	May 2020	Added wording to make it clear that the policy is for staff and not students. 3.1 Changes to password section to refer to new 16 character passphrase Change to examples of good and bad passwords 3.1.3 changes to wording in changing your password section 3.1.4 improved wording to	Alan Radley

		<p>include use of password managers</p> <p>3.2 removed reference to password protected screen savers</p> <p>4.2 added face-ID and touch-ID as possible solutions for securing mobile devices</p> <p>5 added info to highlight that disposal is carried out by a 3rd party</p> <p>8.1 – added link to network attachment protocol</p>	
V3.0	May 2021	<p>Update of general password guidance – Section 3</p> <p>Addition of 3.15 – Reusing Passwords</p> <p>Addition of 3.16 – Sharing Passwords</p> <p>Addition of 3.17 – Default Passwords</p> <p>Addition of 6.7 – Encryption of data in transit</p> <p>Addition of 6.8 – System design and implementation</p> <p>Addition of 6.9 – Vendor advisories</p> <p>Addition of 6.10 – System security testing</p> <p>Addition of 6.11 – System patching</p> <p>Addition of 7.2 – Third party remote access to university systems</p> <p>Update of 8.1 to include other digital infrastructure</p>	Information Security Manager
V4.0	Sep 2022	<p>Minor adjustments to text.</p> <p>Addition of account logon failure lockout - 3.1.4</p>	Information Security Manager

		<p>Addition of new starter password distribution guidance 3.1.6</p> <p>Update of USB storage guidance - 4.2</p> <p>Major changes to Using your own Device 4.3</p> <p>Addition of PIN requirements for mobile devices - 4.4</p> <p>Addition of device hardening and least privilege to system design - 6.8</p> <p>Update Modem Attachment to include routers and wireless access points – 8.4</p>	
V5.0	Sep 2023	<p>Addition of password reuse – 3.1.4</p> <p>Added new section Using Email Securely – 3.3</p> <p>Major update to Cloud Storage section - 4.5</p> <p>90-day security log retention period - 6.6</p>	Information Security Manager