Aston University

IT SECURITY POLICY

Version	2021.7 Final
Executive Sponsor	Chief Operating Officer
Officer Responsible for Policy/ Procedures	Director of Digital Services
Consultation Process	Executive Operations Group
Date of Approval and Committee and/or Executive Officer	Executive Senate Council
Effective Date	July 2021
Reviewed:	Annually

INTRODUCTION AND CONTEXT

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as Aston University, where information will relate to people, learning and teaching, research, administration and management. This Policy is concerned with the management and security of the University's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the University) and the use made of these assets by its members and others who may legitimately process University information on behalf of the University.

This Policy is structured in accordance with the recommendations set out in the "UCISA Information Security Toolkit" which in turn, is based on the control guidelines set out in the industry standard ISO 27001.

This Policy includes a number of sections of equal standing for ease of use that contain high-level descriptions of requirements and principles. They do not, and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sections of the Policy.

Acknowledgement: The policy document "A Suggested Charter for System and Network Administrators" was adapted to reflect local arrangements, and permission granted by its author, Andrew Cormack, Chief Regulatory Advisor, JANET, is gratefully acknowledged.

1. SCOPE OF THE POLICY

1.1 Purpose of the Policy

An effective IT security policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

This Policy applies to:

- all information assets which are owned by the University, used by the University for business purposes or which are connected to any networks managed by the University.
- all information which the University processes, irrespective of ownership or form.

1.2 What is covered by the Policy

This Policy outlines what Aston staff and students need to know about the management and security of information and information systems. It applies to all users of any university owned networks, computers or mobile devices, and to anyone using personally owned equipment to connect to those systems such as mobile phones, tablets and laptops.

The University ensures that its teaching and research is underpinned and supported by effective information protocols and that our systems are compliant, robust and fit for purpose for all staff and students.

In summary, the key policy points are:

- Information will be protected in line with all applicable legislation.
- Information will be protected against unauthorised access.
- Information assets will be assigned a security classification, ranging from Public to Secret which is applied when the document is created and reviewed upon each modification of asset.
- Each area of the policy and each information asset will have a responsible owner.
- Every member of staff and every student will be assigned a personal user ID and will create a password that must not be divulged to anyone for any reason. Passwords must be strong.
- User access will be ended three months after a student has graduated and three months after a member of staff leaves. On departure access will be read only.
- Personal use of university facilities is permitted, but only where it does not interfere with study or work and does not contravene any University policies.
- Data storage facilities should only be used to store university data.
- Standard USB sticks should not be used to store sensitive data.
- University data should not be stored in cloud storage other than that provided by the University, or with external collaborators with agreement by an Executive Dean or Director of Service.
- Outsourcing data to third parties or to cloud systems represents a risk and must comply with this policy and be agreed by the Director of Digital Services.
- Personally owned equipment should not be connected to the university network other than the wireless network.
- Unacceptable usage may be dealt with under disciplinary procedures.
- Software and hardware must only be purchased under contracts delivered by Digital Services.

- Managers must be aware that access to many systems is not yet automatically controlled and must make requests for changes – for example a member of staff leaving – to the systems manager as well as to Human Resources.
- The University will restrict access to certain categories of material on the internet including terrorist related or pornography. Access will only be available to researchers under research agreements.
- Research related to these categories will be housed in dedicated storage and only accessed from dedicated PCs.
- By default no user will have rights to install software or change security settings without permission from Digital Services.
- All systems will be managed by suitably skilled and qualified staff, these staff and/or external assessors will subject all systems to regular vulnerability scanning.
- All software will be actively managed to ensure it is up to date and secure.
- Software licences must be in place before usage.
- Non-approved software that creates significant risks to the network such as File Sharing, Games, Instant messaging, Dropbox, Wireshark, Downloaders, VPN software are not permitted.
- Mobile working is permitted from both personal and university owned devices. These devices must be password protected and secure. No work data classified as Confidential or higher should be downloaded to a personal device. All university laptops are encrypted.
- Staff and students should be aware that the university may access records of use of internet, email or telephone to conform to any applicable legislation, to check for operational effectiveness and to detect unauthorised use.
- Systems and network administrators will respect the confidentiality of users, files and correspondence and require formal authorisation from the owners of the system they are responsible for, namely the Director of Digital Services.
- All services will have a privacy policy in place.
- All systems will be subject to external penetration testing annually with mission critical systems such as Finance tested more frequently and if issues are revealed, they will be dealt with within 28 days at the latest.

1.3 Who is covered by the Policy

This Policy is modular and applies to all members of the University and any others who may process information on behalf of the University. Please familiarise yourself with those sections that directly concern you using the table below for guidance. Mobile and remote working, passwords and cloud storage may, for example, be of relevance to most members of staff, but guidelines for systems administrators will not.

Section	Undergraduate	Post Graduate/ Researcher / Academic	Technical / System Owners
Section 1 - Scope of the Policy	√	√	√
Section 2 - The Policy Statement	√	√	√
Section 3 – Compliance Requirements	√	√	√
Section 4 – Responsabilities and Behaviour	√	√	√
Section 5 – Purchase and Disposal of Equipment		√	√
Section 6 - Outsourcing and Third Party Compliance		√	√
Section 7 - Training			√

Section	Undergraduate	Post Graduate/ Researcher / Academic	Technical / System Owners
Section 8 – Internet Filtering, Recording and Retention			√
Section 9 – Information Handling and Labelling		√	√
Section 10 – User Management			√
Section 11 – System Planning and Development			√
Section 12 – System Management			√
Section 13 – Network Management			√
Section 14 – Software Management			√
Section 15 – Cloud Storage		√	√
Section 16 – Encyption		√	√
Section 17 – Security Sensitive Research		√	√
Section 18 – Investigation of Computer Use		√	√
Section 19 - Passwords	√	√	√
Section 20 – Guidelines for Systems and Network Administrators			√
Section 21 – Guidelines for Security and Penetration Testing			√

1.4 Breach of this Policy

Any breach of this Policy and its associated procedures by staff will be investigated in accordance with the University's disciplinary procedure.

Minor breaches of policy will be dealt with by the Director of Digital Services. The relevant Executive may be informed of the fact that a breach of Policy has taken place.

More serious breaches of policy (or repeated minor breaches) will be dealt with under the University's disciplinary procedures. A serious breach may amount to gross misconduct and could therefore result in summary dismissal.

Any breach of this Policy and its associated procedures by non-staff will be investigated and steps taken in accordance with the law and any relevant contract.

Where appropriate, alleged breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

1.5 Policy Ownership

The Executive has approved this Policy, the Chief Operating Officer is the Executive sponsor and the Director of Digital Services is the officer responsible for the Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Director of Digital Services. For the sake of brevity and clarity the document refers to the Director of Digital Services, this is the Director of Digital Services (or his nominees namely, in his absence for whatsoever reason, the IT Technical Director or IT Support Director).

2. THE POLICY STATEMENT

2.1 Guiding Principles

The following guiding principles underpin this Policy:

- Information will be protected in line with all applicable legislation and relevant University policies.
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.

3. COMPLIANCE REQUIREMENTS

3.1 Applicable Law

The University must comply with certain legislation and associated regulations in relation to the use, storing and handling of information. At the time of this policies approval or review, this legislation includes but is not limited to the following statutory instruments referred to for the purposes of this document as “applicable laws”:

- the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Regulation of Investigatory Powers Act (RIPA) 2000
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Human Rights Act 1998
- Equality Act 2010
- Terrorism Act 2006
- Limitation Act 1980
- Official Secrets Act 1989
- Malicious Communications Act 1988
- Digital Economy Act 2010
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
- Police and Justice Act 2006
- Counter-Terrorism and Security Act 2015
- Obscene Publications Act 1959
- Obscene Publications Act 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Criminal Justice and Immigration Act 2008
- Prevention of Terrorism Act 2005
- Defamation Act 1996
- Defamation Act 2013

A reference to a particular law is a reference to it as it is in force for the time being taking into account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.

The University maintains policy statements, regulations, and guidance for all staff and students in relation to applicable laws. Users of the University`s online or network services are individually responsible for their activity and are made aware of their obligations when using such services through the relevant policy statements, regulations, and guidance. Any suspected breach of the University's policy statements, regulations, and guidance must be reported to the Chief Operating Officer. The University reserves its rights to collect evidence in relation to a potential claim or internal investigation. Where there is suspicion of a criminal offence involving the University`s information or systems subject to appropriate internal authorisation, the University will cooperate with the relevant agency to assist in the preservation and gathering of evidence.

3.2 JANET policies

As at the date of this Policy the University, along with other UK educational and research institutions, uses the 'JANET' (Joint Academic NETwork) electronic communications network and must therefore comply with JANET's Acceptable Use and Security Policies. Both of these policies are available from the JANET website.

3.3 Payment Card Industry Data Security Standard (PCI DSS)

The University must comply with the Payment Card Industry Data Security Standard (PCI DSS) when processing payment (credit/debit) cards.

3.4 Software licence management

All software used for University business must be appropriately licensed. The University must comply with the software and data licensing agreements it has entered into. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved. Agreements may need to be specifically negotiated to enable the University to comply. Therefore, no software must be purchased or otherwise brought into the University other than via Digital Services.

3.5 Records management

The University is required to retain certain information, whether held in hard copy or electronically, for legally defined periods as stated in the Information Management Policy.

4. RESPONSABILITIES AND BEHAVIOUR

4.1 Introduction

This section sets out the responsibilities and required behaviour of users of the University's information systems, networks and computers including when using users own equipment to access University resources.

All members of the University (staff, students and associates), members of other institutions who have been granted federated (where an agreement to have single sign on, shared between institutions) access to use the University's facilities together with any others who may have been granted permission to use the University's information and communication technology facilities by the Director of Digital Services are subject to this Policy.

4.2 User identification and authentication

Each member will be assigned a unique identifier (UserID) for his or her individual use. This UserID may not be used by anyone other than the individual user to whom it has been issued. The associated account password must not be divulged to anyone, including Digital Services staff, for any reason. This University password should not be used as the password for any other service. Individual members are expected to remember their password and to change it if there is any suspicion that it may have been compromised.

Each member will also be assigned a unique email address for his or her individual use and some members may also be given authorisation to use one or more generic (role based) email addresses. Members must not use the University email address assigned to anyone else without their explicit permission.

Email addresses are University owned assets and any use of these email addresses is subject to University policies, as well of those of hosted systems such as Microsoft Office 365.

4.3 Personal use of facilities

University information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the University. Very occasional personal use is permitted but only as long as:

- It does not interfere with the member of staff's work nor the student's study.
- It does not contravene any University policies.
- It is not excessive in its use of resources.

University facilities should not be used for the storage of data unrelated to membership of the University. In particular, University facilities should not be used to store copies of personal photographs, videos, music collections or personal emails.

Members of staff and research postgraduates should not use a personal (non-University provided) email account to conduct University business and should maintain a separate, personal email account for personal email correspondence.

All use of University information and communication facilities, including any personal use is subject to University policies, including the Investigation of Computer Use (Section 18).

4.4 Connecting devices to University networks

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with the JANET Acceptable Use and Security policies, it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the University's wireless networks.

Further to reduce risk of data loss, members of staff and research postgraduates should not connect any personally owned peripheral device which is capable of storing data (for example, a personally owned USB stick) to any University owned equipment, irrespective of where the equipment is located.

USB sticks should not be used to store any sensitive or personal data. Any device connected to the University network or owned by the University must be managed effectively this includes:

- Up to date antivirus.

- Hard drive encryption on all laptops.
- Hard drive encryption on desktops that contain sensitive data.
- Be able to receive updates from the University's patching tool.
- A supported operating system that is regularly patched.
- Designed for a corporate environment.
- Must not put at risk others by its use.

Devices which are not managed effectively, are liable to physical or logical disconnection from the network without notice.

4.5 Unattended equipment

Computers and other equipment used to access University facilities must not be left unattended and unlocked if logged in. Members must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended. Particular care should be taken to ensure the physical security of all equipment when in transit and must never be left in an unattended vehicle.

4.6 Unacceptable use

The following uses are also considered to be unacceptable uses of the University's facilities:

- Any illegal activity or activity which breaches any University policy.
- Any attempt to undermine the security of the University's facilities which includes undertaking any unauthorised penetration testing or vulnerability scanning of any University systems.
- Providing access to facilities or information to those who are not entitled to access.
- Any use which brings the University into disrepute.
- Any use of University facilities that could be reasonably construed as bullying, harassment, intimidating, victimising or otherwise causing alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of the University.
- Creating, storing or transmitting any material which could reasonably be construed as infringing copyright.
- Creating, storing or transmitting defamatory or obscene material. (In the unlikely event that there is a genuine academic need to access obscene material, the University must be made aware of this in advance and prior permission to access must be obtained from the Director of Digital Services.)
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the University's facilities.
- Failing to report any breach, or suspected breach of information security to Digital Services.
- Failing to comply with a request from an authorised person for you to change your password.

5. PURCHASE AND DISPOSAL OF EQUIPMENT

5.1 Purchasing of Digital Equipment

Software and hardware must only be purchased via the contracts established by procurement and administered by Digital Services, to make sure that everything being purchased is compatible with the University systems. To purchase IT equipment, ITS Helpdesk need to be

contacted to discuss requirements. A quote will then be obtained and can then be purchased via ITS Helpdesk who will then configure to our standard setup.
When new hardware is purchased, by default it is assumed that it is replacing existing equipment that Digital Services will take away to be either recycled or used as spares. Extra equipment can only be retained with the express permission of the relevant member of the Executive or Director of Digital Services, and an additional fee may be levied to cover licensing additional software and IT Support costs.

Under no circumstances should software or hardware be purchased by staff or students, or on University credit cards without the authorisation of the Director of Digital Services, users will not be reimbursed for the costs involved for unauthorised purchases, and will be subject to disciplinary processes.

5.2 Disposal of Equipment

All equipment whether it was purchased from University budgets, PASA accounts or research grants remains the property of the University, and must be disposed of via Digital Services. Under no circumstances may equipment be removed when a user leaves the University or replaces equipment.

This is a legal requirement for licensing, data protection and insurance purposes and if not adhered to could result in significant fines on the University.

6. OUTSOURCING AND THIRD PARTY COMPLIANCE

6.1 Introduction

This section outlines the required conditions that are required to maintain the security of the University's information and systems when the University enters into arrangements with third parties, other than the University's own staff or students.

6.2 Scope

This third party access could occur in a number of scenarios, common examples being:

- The use of cloud computing services.
- Involvement of third parties in the design, development or operation of information systems for the University.
- The granting of third party access to the University's information systems from remote locations where computer and network facilities may not be under the control of the University.
- When users who are not members of the University are given access to information or information systems.

6.3 Managing outsourcing risk

Prior to outsourcing or allowing a third party access to the University's non-public information or systems, a decision must be taken by staff of appropriate seniority, after consulting with the asset owner, that the risks involved are clearly identified and acceptable to the University. The level of staff seniority will depend on the nature and scale of the outsourcing. Advice should be sought from the Director of Digital Services, and Head of Procurement during the decision-making process. In the event that the University uses a third party providers services this will be subject to compliance with applicable laws and communications of such arrangements to all individuals concerned as required.

6.4 Due diligence

The process of selecting a third party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the University is not exposed to undue risk. This process may involve advice from members of the University with expertise in contract law, IT, information security, data protection and human resources. This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the University.

6.5 Contracts with third parties

All third parties who are given access to the University's non-public information or systems must agree to following terms in any agreement;

- Compliance with this Policy.
- Compliance with the Privacy Policy.
- Appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to and other supplier.
- Confidentiality obligations where a third party is given access to the University`s non-public information.

These requirements should be signposted to third parties early in negotiations and advice sought from Procurement and/or the Office of the General Counsel (as required) to ensure that the contracts are compliant with the University practice, procedure and risk appetite. The use of third party services must not commence until the University is satisfied with the information security measures in place and a contract has been signed and has taken legal effect. All contracts with external suppliers will be monitored and reviewed by Office of the General Counsel to ensure the information security requirements are being satisfied. Advice should be sought from the Office of the General Counsel and/or Procurement in relation to contractual arrangements.

6.5 Personal data

Any outsourcing arrangement involving the transfer of personal data to a third party must include the acceptance of the University's standard personal data processing terms as set out in the Privacy Policy and its associated procedures.

6.6 Informal outsourcing

There are extensive Digital Services that are available to members of the University via the internet which the University will have no formal agreement or contract in place with - examples include email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions and the University has no ability to negotiate as it would via the formal outsourcing procedure.

The use of such services for storing University information present a real risk to the University as there is no way the University can ensure the confidentiality, integrity and availability of the information without a formal agreement in place. The storage of personal data with such providers is likely to be a breach of data protection law for which the University could be penalised by the Information Commissioner.

In cases where it is necessary to remove data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Further advice is available from Digital Services and/or the General Counsel.

University staff and students must not configure their University email account automatically to forward incoming mail to third party services or email providers with which the University have no formal agreement. This applies equally to systems that "scrape" email from other accounts such as Google, or websites such as LinkedIn and Facebook that ask for permission to access your address book to find connections. Forwarding emails from your Aston account to an external account is not permitted. This includes the setting up of forwarding rules and also manually forwarding of emails. Forwarding from one Aston account to another Aston account is permitted as the data does not leave our organisation and is therefore compliant.

6.7 Third party physical access

A risk assessment must be completed prior to allowing a third party to have access to secure areas of the University where confidential information and assets may be stored or processed. This assessment should take into account:

- What computing equipment the third party may have access to.
- What information they could potentially access.
- Who the third party is.
- Whether they require supervision.
- Whether any further steps can be taken to mitigate risk.
- Access to be given for only as long as absolutely necessary.

7. TRAINING

7.1 Introduction

This section sets out the processes that must be implemented to ensure that staff are able, trained and required to protect the University's information assets.

7.2 Recruitment, references and screening

For roles involving handling of strictly confidential information or accessing sensitive information systems, Human Resources may use a pre-employment or change of role screening process to help ensure that employees selected are suited to the demands of the job.

7.3 Employee termination, suspension or change of appointment

Upon termination, suspension or change of appointment, Human Resources will revise the staff records system accordingly. This will trigger appropriate account management processes on centrally managed IT systems. Managers, however, should be aware that access to many sensitive systems is not yet automatically controlled and should make appropriate requests for access, change of permissions or denial of access to the relevant system managers, a list of which is kept by Human Resources.

Upon termination, all employees, contractors and third parties must return all information assets and equipment held which belong to the University to the employing / commissioning manager.

7.4 IT usage monitoring and access

The Executive Director of Human Resources and Organisational Development may authorise for the legally compliant monitoring of IT systems to be undertaken for legitimate University

purposes. The Policy relating to how the University may monitor usage of its IT systems is outlined in Investigation of Computer Use (Section 18).

7.5 Conduct procedure

Any employee who is suspected to have breached this Policy will be subject to the University's policies and procedures in relation to misconduct and, any investigation undertaken in accordance University policy and procedures.

Where there are reasonable grounds for suspecting misuse of a computer account, the Director of Digital Services may authorise for that account to be suspended and/or investigated by authorised members of Digital Services at any stage in the conduct procedure.

7.6 Aston Student Placements

If you are employing an undergraduate or postgraduate student as an intern, consideration must be given to the information they are able to access. Access levels must be appropriate based on the role they are performing. Access to the personal data of other University students and staff is unlikely to be appropriate. Under no circumstances will students be given "staff" access to the Student Information System.

8. INTERNET FILTERING, RECORDING AND RETENTION

8.1 Introduction

This section sets out the requirements relating to internet filtering, recording of access and the retention of such records and specifically addresses the requirements of the Counter Terrorism and Security Act 2015.

The University uses a third party tool that categorises websites, along with other tools to restrict access to websites either where required by legislation, industry best practice or to restrict access to content that may damage or try to affect the security of the University's network or data.

Repeated attempts by users of the University facilities to access any filtered material are itself likely to be something that is automatically investigated.

8.2 Filtered material

Access to material that falls into the following categories is restricted by the University's firewall and access is only granted to those users that require it, after approval from the University following the procedure described in Section 17 – Security Sensitive Research:

- Terrorism
- Extremism
- Child Pornography / Abuse
- Extreme Pornography / Abuse
- Drug Abuse
- Hacking / Avoidance / Misuse
- Pornography

8.3 Recording of access

The University records internet activity for a period of up to 90 days as a matter of course and records the following information.

- Web site (and page) + Category
- Date and time
- User ID (where available)
- Machine ID (where available)
- IP address (source)

The University, where requested by an appropriate authority, may extend the period in which it keeps these logs for a particular user of University facilities.

9. INFORMATION HANDLING AND LABELLING

9.1 Introduction

This section sets out the requirements relating to the handling of the University's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

9.2 Inventory and ownership of information assets

An inventory of the University's main information assets will be developed and maintained and the ownership of each asset clearly stated. Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

9.3 Security classification

Each information asset will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

- **Public** – available to any member of the public without restriction.
- **Open** – available to any authenticated member of the University.
- **Confidential** – available only to specified members, with appropriate authorisation.
- **Strictly Confidential** – available to only a very small number of members, with appropriate authorisation.
- **Secret** – the most restricted category. It is not anticipated that many University assets will be assigned this classification.

In principle, any information which is disclosed under the Freedom of Information Act 2000 will be classified as **Public**. Any data which are classified as sensitive personal data under the Data Protection Act 1998 (or its successor legislation) will be classified as **Strictly Confidential**. Any data which are subject to the Official Secrets Act 1989 will be classified as **Secret**. Any information which are not explicitly classified will be classified as **Open**, by default.

The information below sets out further detail regarding permitted storage locations for digital information assets:

Aston University Digital Information Asset Classification Matrix

Classification of Information	PUBLIC	OPEN	CONFIDENTIAL	STRICTLY CONFIDENTIAL	SECRET
Impact if information is made public	None	Low May result in very minor reputational or financial damage to the University. May result in very minor privacy breach for an individual.	Medium An intermediate reputational, financial or privacy impact. May make it less likely that the University would be trusted with similar information in future.	High Could substantially damage reputation of the University. Would result in a serious privacy breach to one or more individuals.	Critical May damage national security.
Definition	May be viewed by anyone, inside or outside the organisation.	Available to authenticated users at the University such as staff, research students, or students.	Only approved access to a specific group of people that are granted permission to. The list is regularly reviewed and amended. Least privilege best practice followed.	Access is restricted to a small number of people who are listed by name. The list is regularly reviewed and amended. Least privilege best practice followed.	Known only to a very small number of staff/researchers who have been explicitly cleared and vetted for access. Least privilege best practice followed.
Description	**Public** information assets may include but are not limited to: • Publications. • Press releases. • Course information. • Principal University contacts for public facing roles i.e. name, e-mail address and work telephone number. • Public events. • Freedom of information replies.	**Open** information assets may include but are not limited to: • Contact information for most staff. (e.g. name, role, e-mail address, work telephone number) • Approved Internal University. communications. • Policies. • Procedures. • Guidelines.	**Confidential** information assets may include but are not limited to: • Personal details and identifiable information e.g. name /address/telephone number/email address/date of birth/National Insurance Number). • Information relating to the health of a University member. • Wage slips. • Death certificates. • Employee contract information. • Non-Disclosure Agreements.	**Strictly Confidential** information assets may include but are not limited to: • Bank details. (sort code/account number) • Financial data. • Student transcripts. • Examination papers. • Staff/student medical records. • Certain medical research data. • Research papers intended to lead to patentable results (If research is ongoing and has not been published). • Details of servers and server rooms. • Passwords. • Investigations/disciplinary proceedings. • Submitted patents/Intellectual Property Rights. • University and third party contract/supplier information. • Market sensitive information (e.g. concerning some property purchases).	**Secret** information assets access is subject to or obtained under the Official Secrets Act or equivalent.
Permitted storage locations	• On Premise - Aston University Local Data Servers. • Aston Box Cloud storage account. • Website. • Hard Drive/portable drive.	• On Premise - Aston University local data servers. • Aston Box Cloud storage.	• On Premise - Aston University local data servers. • Aston Box Cloud storage. • Approved Encrypted portable drive. • Encrypted University provided PC/Laptop. • University Portal with appropriate login.	• On Premise - Aston University local data servers. • Aston Box Cloud storage. • Approved encrypted portable drive. • Encrypted University provided PC/laptop. • University portal with appropriate login.	• On Premise – Aston University local data servers. • Hardware encrypted approved memory Stick. • Encrypted University provided PC/Laptop.
Other Storage Considerations	Some information should only be released with appropriate consent.	• Documents should converted to PDF format to prevent unauthorised modification. • This includes documents such as Policies, Procedures and Guidelines.	• **Must be encrypted and have secure password.** • Removal of access as soon as not required. Secure handling may include but is not limited to: **Electronic Information assets (In Transit/Rest)** • Encryption. • Password protection. • SFTP (Secure file transfer protocol). • Secure file stores. • Secure disposal. • Reduced access rights/Level of privileges.	• **Must be encrypted and have secure password.** • Removal of access as soon as not required. Secure handling may include but is not limited to: **Electronic Information assets (In Transit/Rest)** • Encryption. • SFTP (Secure file transfer protocol). • Secure file stores. • Asset tags. • Secure disposal. • Access rights/Level of privileges.	• **Must be encrypted and have secure password.** • Removal of access as soon as not required. • Individual projects may require differing controls above/or below) local circumstances. • Each requirement will be reviewed on a case by case basis in line with HMG controls. • HMG advice and guidance is subject to regular change.

9.4 Access to information

Users will be granted access to the information they need in order to undertake their roles within the University. Users granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

9.5 Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of in accordance with University procedures. Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the University, unless the disposal is undertaken under contract by an approved contractor, in which case disposal certificates must be obtained.

In cases where a storage system (for example a computer hard drive) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the University until it is disposed of securely. Digital Services will arrange this service.

9.6 Removal of information (from University premises or systems)

The removal of any information from the University is permissible on an exceptional basis and is subject to appropriate security measures to protect the data from unauthorised disclosure or loss. Strictly confidential data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner. Particular care needs to be taken when information assets are in transit. University supplied mobile devices must always be fully encrypted. Data handled by the University on behalf of users such as Research Councils, NHS, European Union and Social Care organisations will be processed in accordance with the relevant policies, procedures and privacy notices.

9.7 Hardware encrypted USB memory sticks

All data removed or extracted from University systems (and not stored on Network drives etc. or encrypted machines) must only be copied onto hardware based encrypted USB devices. Hardware Encrypted Memory Sticks can be ordered from Digital Services. They must be a model that Digital Services have tested and sanctioned as compliant. All these devices conform to FIPS 140-2 Level 3 Encryption Algorithm or above. They must be configured by Digital Services so that any default user and admin password is removed prior to using and a unique secure password is applied, without this process, these devices are not secure. A list of recommended devices is listed below:

- iStorage datAshur USB2.0 – Available from 4GB to 32GB.
- Kingston DataTraveler 2000 USB3.1 – Available from 4GB to 64GB.
- iStorage diskAshur Pro SSD 1 – Available 128GB or 256GB.
- IronKey D300 Standard – Available 8GB to 128GB.
- IronKey D300 Managed – Available 8GB to 128GB.

9.8 Using personally owned devices

Any processing or storage of University information using personally owned devices must be in accordance with the IT Remote Working Policy.

9.9 Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Screen privacy filters are available to be purchased for this purpose.

9.10 Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

As a minimum, nightly backups must be taken that are retained for two weeks, weekly backups that are kept for twelve weeks, and monthly backups that are retained for a minimum of six months.

Information which is entrusted to the care of Digital Services (and stored on network drives) meet these requirements.

9.11 Exchanges of information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party in accordance with Section 6 – Outsourcing and Third Party Compliance.

Information classified as strictly confidential may only be exchanged electronically both within the University and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner. Hard copies of information classified as strictly confidential or above must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission. Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified. University employees must not disclose nor copy any information classified as confidential, strictly confidential or secret unless they are expressly authorised to do so.

9.12 Reporting losses

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset in accordance with the Privacy Policy and its associated procedures.

10. USER MANAGEMENT

10.1 Introduction

This section sets out the requirements for the effective management of user accounts and access rights. To ensure that access to the University's information and information systems is restricted to authorised users only.

10.2 Scope

All information systems used to conduct University business, or which are connected to the University network must be managed in accordance with this Policy.

10.3 Eligibility

User accounts will only be provided for:

- Permanent and fixed term university employees.
- Students (including those on placement year and awaiting graduation)
- Emeritus staff and those who have otherwise been granted honorary or associate status (Associates will include staff from other organisations which provide services to the University who may require access to the University's information systems in order to fulfil their contractual obligations to the University. Associates will also include external research collaborators but all of which whom will be included on core to recognise their status.)
- Members of Council (who will be recorded in the HR Systems).
- Non-human accounts only where absolutely necessary, subject to approval procedure and regular review.

User accounts give users access to the network, and an email account. This user account then makes it possible for users to be given access to resources, information systems or facilities on an individual or group basis.

Visitors to the University including conference guests are able to use the public Wi-Fi that is provided by a third party.

10.4 Authorisation to manage

The management of user accounts and privileges on the University's information systems is restricted to suitably trained and authorised members of Digital Services.

10.5 Account and privilege management

Accounts will only be issued to those who are eligible for an account and whose identity has been verified via the HR system or Student Information System. The credentials for these accounts must not be shared to any other person, user or service.

When an account is created, a unique identifier (UserID) will be assigned to the individual user for his or her individual use. This UserID may not be assigned to any other person at any time (UserIDs will not be recycled). On issue of account credentials, users must be informed of the requirement to comply with this Policy.

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles.

Procedures shall be established for all information systems to ensure that user's access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (for example, when a member of staff changes their role or a member of staff or student leaves the University).

Privileged accounts are accounts used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

10.6 Password management

Passwords for new students will be sent along with registration information and can be set by the student during on-line registration. Passwords for staff members will be automatically generated and sent to the user. Exceptionally, the new member may be informed of an initial, temporary password, which must be communicated in a secure way and must be changed by the new member immediately. This change should be enforced automatically wherever possible.

10.7 Creation of user accounts

User accounts can only be created from automated feeds from either the University Human Resources or student system, there is no other way for these accounts to be created and, therefore, it is essential that University processes for the recruitment of staff and students are followed. Temporary users, including agency staff and placements must be registered on CORE, visiting students (who are not using Eduroam) will only be given access if they are registered on SITS. Staff on Honorary contracts, Emeritus staff and members of Council will all be recorded on the HR system.

10.8 Ending of user access

To make sure that only those who are entitled to access University resources do so, it is important to make sure there is a robust process in place for when someone leaves the University.

Where a student leaves the University on completion of a course they will have access to University systems three months from the end of their course, where a student leaves the University (for reasons other than successful completion the Director of Student services or Director of Digital Services may request that an account is suspended immediately).

When a member of staff reaches their leaving date, any system access is automatically revoked. Access to email is removed and only recoverable for a short period after this date. Any backups of personal data should be completed before leaving the University. University data, especially sensitive data or privileged information cannot be copied off or backed up for personal use due to privacy reasons. Handover to shared resources such as BOX items for your team should be dealt with during the handover process in the notice period.

The line manager may request access for a maximum period of ninety days after the staff member has left. Twelve months after this, the account along with all email and network drives will be deleted. Files stored on a local machine are likely to be erased much sooner as the machine will be reimaged before being passed to another user. If this needs to be a more flexible arrangement, it has to be approved by the Executive in accordance with internal audit recommendations.

Where leavers are not automatically deleted from systems, Human Resources will distribute a list of names to all system owners so that these users' can be disabled as quickly as possible, and certainly within 14 days of receiving the list from Human Resources.

10.9 Local machine administration rights (Elevated User Rights (EUR))

By default, no user will have administrative rights to a local machine to install software, make changes to security settings etc. Some software by its nature requires these elevated user rights to run and so therefore some users may need these privileges, however the University has software that grants these rights to certain 'approved' applications. Some staff by the nature of their work may require elevated user rights because of their research or development activities, if this is the case, this level of access will be authorised (annually) by the Executive Dean of the appropriate School and communicated to the Library & Digital Services stakeholder group and to the University Audit and Risk Committee each year. These elevated user rights will only be available on a secondary account.

This Policy applies equally to servers that must be restricted and controlled, the principles in this document however apply to all servers and control of EUR should be discussed with Digital Services.

The controlled management of the EUR is vital to the business of the University to ensure:

- Staff have a secure and reliable desktop facility.
- Research, personal and corporate data is protected from corruption, misuse or breach of law.
- Support time is minimised by reducing variable or unknown configurations.
- Access to the University network is limited to those with the correct authorisations.
- Software deployed is correctly licensed.
- Global updates can be applied quickly and remotely.
- Restore times are faster in the event of a machine failure.

In all but the most exceptional cases Digital Services expect to retain full control of computers for example, where machines are in public or student facing areas or all applications on a desktop are centrally managed. Running computers with Local Administrative rights always increases risk from malicious software or cyber-attack or machine corruption. Vital data can be lost and/or time is lost in restoring service.

10.10 General Principles for granting local administrative rights

Digital Services restricts the number of employees with local administrator rights to a minimum because running with these additional rights significantly adds risk to data loss; computer virus or machine malfunction. Requests for local administrative rights may however only be granted where it is absolutely necessary and all other options have been exhausted by an engineer.

For a user to have administrative rights they must first successfully complete the online IT security training.

In the event of a machine malfunction, IT staff will do their best to restore service as quickly as possible. Any machine administered locally may however have changes made that IT staff know nothing about. Digital Services staff can only guarantee restoration of the machine to the latest version of the standard PC deployment. Employees must store data on central file stores and not the local hard disks of their PC or laptop for resilience.

EURs will be withdrawn if a particular threat is identified or, for example, the machine is compromised on multiple occasions. Appropriate notification will be given to staff depending on the threat posed to data security.

11. SYSTEM PLANNING AND DEVELOPMENT

11.1 Introduction

This section sets out the responsibilities and required behaviour of those who undertake system planning and management on behalf of the University (this includes staff who are not part of the Digital Services team).

Information systems are key to the University conducting its core functions of Teaching and Learning, Research and Administration and its key that all of these work effectively, securely and integrate together.

11.2 Environments

It is recommended that each information system has the following environments, to enable testing and training to take place, outside of live solution.

- Live
- Test
- Training

11.3 Characteristics

Each system that is purchased by the University or for current system should aspire towards the following functionality:

- Access control that integrates to Active Directory.
- Can be resilient and virtualised.
- Different levels of user access.
- Logging of activity.
- Ongoing support and maintenance from supplier.
- Integration and interoperability using BizTalk.
- Developed in line with OWASP guidelines wherever possible.

11.4 Go live testing

Before any system or new version goes live it is essential that it is properly tested. This must always include:

- Reconciliation of number of records, values etc.
- Testing using a number of scenarios laid out in a plan for scenario for end users – User Acceptance testing (UAT).
- Tested on multiple machines and devices that are used the access the system.
- Penetration testing by the University's external contractor – both to check it is secure from external to the University and from internally.
- Use of vulnerability testing software (currently OpenVAS) on the hardware that the application sits upon.
- Training materials for staff.
- Volume testing.
- Testing of interfaces and feeds to other systems.
- Properly authorised change control from the Digital Services Change Advisory Board (CAB).

11.5 Business continuity testing

Before any system goes live either for a new system or following an upgrade the following need to be in place.

- System has been successfully backed up and restored.
- If the system is designed to failover etc. to other locations or load balanced between multiple servers, this functionality needs to be tested.
- Business continuity plans must be in place for users of the system.
- Digital Services must be informed and they will update their plans including the overall priority of recovering this system in the overall recovery plan of University systems.

12. SYSTEM MANAGEMENT

12.1 Introduction

This section sets out the responsibilities and required behaviour of those who manage computer systems on behalf of the University.

12.2 Scope

The University's computer systems must be managed by suitably skilled and qualified staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability). These system managers will undertake their duties in collaboration with the IT Technical Director and IT Support Director whose services are running on these computer systems. This Policy applies to all members of staff who use administrator (or Elevated User Rights) privileges on any University multi-user computer system (server) to administer the system or the services running on the system. The management of desktop systems is not in scope.

12.3 Duties and responsibilities

System and service managers are in uniquely privileged positions and play a key role in ensuring the security of the University's systems and services. They are expected to be aware of this Policy in its entirety and must always abide by this Policy.

System managers and owners should assign a business criticality level in their business continuity plan to their systems and ensure that their systems are registered in Digital Services' asset database (Configuration Management Database). Depending on the level of criticality, they are responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service. The level of criticality will be validated by the Library & Digital Services strategy board to ensure consistency across the University. They should also assign (and record) a confidentiality level to their systems which indicates the suitability, or otherwise, of using any individual system for the storage or processing of different categories of University data in accordance with Section 9 - Information Handling and Labelling. This is in order to allow data owners to make informed decisions as to whether the system meets their security requirements.

System managers / owners are responsible for ensuring that their services are registered in Digital Services' Service Catalogue.

System managers should deploy systems to agreed secure baselines (systems will be "hardened"). Baselines will be agreed with IT Technical Director (and his team) and will be defined for hypervisors (where relevant), operating systems, applications and any required "middleware". Baselines must be reviewed from time to time.

System managers are also responsible for ensuring the on-going security of their systems and must apply software patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches must be applied in accordance with software suppliers' recommendations (or requirements) or within 5 working days of release, whichever is the shorter. If it is not possible to patch within this time period, other compensatory control measures must be taken to mitigate risk.

Systems Managers in conjunction with System Owners are authorised to act promptly to protect the security of their systems, but must be proportionate in the actions that they take, particularly when undertaking actions which have a direct impact on the users of their systems. Any actions which may be potentially invasive of users' reasonable expectations of privacy must be undertaken in accordance with Investigation of Computer Use (Section 18) and the associated "Guidelines for system and network administrators" document.

System managers must immediately report any information security incidents to Digital Services (or, if unavailable, by email to: abuse@aston.ac.uk).

12.4 Change management

All changes to computer systems are subject to Digital Services' established change management processes and procedures. These requests will be analysed and go through a Change Board for approval. File integrity monitoring software should be used where possible to help detect unauthorised system changes.

12.5 Access control

Access to all computer systems must be via a secure authentication process, with the exception of read-only access to publicly available information. Wherever possible, authentication should be either via the University's single sign on service or against the University's central authentication database. Locally administered accounts should be avoided wherever possible, will be audited regularly and removed at the earliest convenience.

Access must only be granted in strict accordance with Section 10 - User Management, and in all case users of systems must successfully complete the online IT Security training before being given access to the University's information systems.

Administrator accounts and accounts with elevated privileges must only be used when necessary in order to undertake specific tasks which require the use of these accounts. At all other times, the principle of "least privilege" should be followed.

Access to administrator accounts (whether direct or indirect) from untrusted networks (from home, for example) or when using personally owned devices should be protected by two-factor authentication wherever possible. Each system must have no more than three administrator level user accounts, any more than this and it must be communicated to the Library & Digital Services stakeholder group annually, with the reasons the higher number of accounts is required, and the mitigations that are in place for having a greater number of accounts.

12.6 Monitoring and logging

The use and attempted use of all computer systems should be logged. The data logged should be sufficient to support the security, compliance and capacity planning requirements of the system but should not be unnecessarily intrusive. Users of systems should be given clear information of what information is recorded, the purposes of the recordings and the retention

schedule of the data collected. This information should be made available to users in the form of a system specific privacy policy.

It is recommended that log files are recorded on a different system from the system being monitored.

Audit logs should be configured to record any actions undertaken using administrator or elevated privileges. Audit logs should be secured to protect them from unauthorised modification.

12.7 Annual audit of users

Each year, system owners must confirm to the Library & Digital Services stakeholder group that they have undertaken their review of user accounts and their levels of access, to satisfy themselves that they believe the users and their access is appropriate to undertake their role.

12.8 Test / Development or Training Systems

Under no circumstances should personal or identifiable data be used in these systems. System owners will be asked to confirm their compliance annually.

12.9 Vulnerability scanning

All systems are subject to regular vulnerability scans (at least every 12 months and after any significant change has been made to a system). These scans may be undertaken by appropriately skilled University staff or by approved external assessors. Business critical systems and other systems which are used to process or store data classified as strictly confidential or above are subject to more regular penetration testing by an approved external assessor.

12.10 System clocks

All system clocks must be synchronised to reliable time sources. These sources will be the University's official internal time servers, with the exception of these official internal servers themselves which must be synchronised with official JANET time servers.

12.11 Default Passwords

All default vendor supplied passwords that come with any system or software must be changed before deployment and is completed by IT Engineers.

13. NETWORK MANAGEMENT

13.1 Introduction

This section sets out the responsibilities and required behaviour of those who manage communications networks on behalf of the University.

13.2 Scope

All of the University's communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over the networks (data or voice).

13.3 Management of the network

The University's communications networks will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability).

Network staff are in highly privileged positions and play a key role in contributing to the security of the University's information assets. They are expected to be aware of this Policy in its entirety and must always abide by it. Network staff are authorised to act promptly to protect the security of their networks, but must be proportionate in the actions which they take, particularly when undertaking actions which have a direct impact on the users of the network. Any actions which may be potentially invasive of users' reasonable expectations of privacy must be undertaken in accordance with Investigation of Computer Use (Section 18) and the associated "Guidelines for system and network administrators" document.

Network staff must immediately report any information security incidents to the Information Security Manager (or, if unavailable, by email to: abuse@aston.ac.uk).

13.4 Network design and configuration

The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the University's business needs, whilst providing a high degree of control over access to the network.

The network will be secured so that access requires authentication and structured in such a way as to minimise the impact of any issues or attacks.

13.5 Physical security and integrity

Networking and communications facilities, including wiring closets, data centres and computer rooms must be adequately protected against accidental damage (fire or flood, for example), theft, or other malicious acts. The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

13.6 Change management

All changes to network components (routers, firewalls etc.) are subject to Digital Services' established change management processes and procedures.

13.7 Connecting devices to the network

It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose.

It is permissible to connect personally owned equipment to the University's wireless networks. Any device connected to a University network must be managed effectively, this includes:

- Up to date anti-virus and anti-malware software, with latest definitions.
- A currently supported operating system.
- Capable of reporting centrally to IT on the current state of its patches and versions, and capable of receiving the latest patches.
- Correctly configured firewall.
- Must not introduce additional risk to the University's infrastructure.

Devices which are not are liable to physical or logical disconnection from the network without notice. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal operational practices.

13.8 Network address management

The allocation of network addresses (IPv4 and IPv6) used on the University's networks shall be managed by IT Technical Director who may delegate the management of subsets of these address spaces to other teams within Digital Services. Network addresses (IPv4 or IPv6) assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

13.9 Access controls

Access to network resources must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques. Digital Services is responsible for the management of the gateways which link the University's network to the Internet. Controls will be enforced at these gateways to limit the exposure of University systems to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation and unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.

13.10 Firewall management

The University firewall is regularly updated and will be no more than two major release behind the latest version for example, 12.3, versions 12.2 and 12.1 are acceptable. It is constantly updated to block known malicious sites and reduce vulnerabilities.

14. SOFTWARE MANAGEMENT

14.1 Introduction

This section sets out the principles and expectations for the security aspects of managing software by IT staff and end users where relevant.

14.2 Definitions

The following terms apply to this section 14:
Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on computers owned by, managed by or for the University.
Computers - includes all end user computing devices, including tablets and smartphones, as well as servers, whether or not they are on a University site.

14.3 General software management principles

All software, including operating systems and applications must be actively managed. This function is normally managed by Digital Services, however, where users have the ability to do this it is particularly important that they follow all rules and guidance around software use and licensing, and in particular the following applies.

There must be an identifiable individual and deputy, or organisational unit, taking current responsibility for every item of software formally deployed.

Individuals installing software and authorised are themselves responsible for that installation, Digital Services will not install any software where there is any doubt that it is appropriately licenced for use in the University (and for the context in which it is being used). Digital Services keep an approved software list to ensure engineers can quickly respond to and rectify faults with this software.

Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities. When the software is no longer needed, it should be uninstalled to reduce the attack surface of vulnerabilities for the device. Software managers and system owners are responsible for ensuring the on-going security of their software and must apply security patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk.

Staff involved in managing or developing software must be suitably skilled. Where possible, automatic updates should be enabled.

14.4 Software procurement

When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls. These could include manual controls required during operation.

When software for use by the University is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose. It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

On occasion, Digital Services may need to contact users to recall a machine. For instance, to apply a critical security patch that cannot be deployed via automatic methods.

14.5 Software installation

Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage. Automated installs should be used wherever possible - in line with current procedures. Media / files must be stored securely and managed.

Software must not be put into user service on University systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. Appropriate assessment / tests should be made to avoid new software causing operational problems to other systems on the network. Individual authorised users installing software on their own computers do so at their own risk.

Change control procedures must be followed and proper records maintained.

14.6 Software regulation

Use or installation of unlicensed software and using software for illegal activities could be construed to be a disciplinary offence.

Use of software which tests or attempts to compromise University systems or network security is prohibited unless authorised by the Director of Digital Services.

Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.

Software found on University systems which incorporates malware of any type is liable to automated or manual removal or deactivation.

14.7 Software maintenance

All changes to computer systems are subject to Digital Services' established change management processes and procedures.

Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible - commensurate with the risk. High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk.

Software and machines managed centrally by Digital Services will have upgrades installed on them automatically, and users are advised that overnight never to leave their machines with unsaved data, as Digital Services may reboot these machines to make sure patches and upgrades are installed as required.

Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their University network connectivity withdrawn. Operating systems or software that are no longer supported will not be allowed on the University network. In the case of operating systems Digital Services will have a planned program to update machines, users are responsible for the costs of purchasing of new equipment and hardware that is no longer on a supported platform. Those that can't be upgraded the risks will be mitigated where possible, however if this is not possible the Director of Digital Services is authorised to remove on utilitarian grounds.

14.8 Software removal

Software that is not licence compliant must be brought into compliance promptly or uninstalled. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service. Change control processes and procedures must be used, commensurate with the risk.

When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence. Often this will free up the license so it can be reused, but this depends on the licensing pertaining to the specific software.

14.9 Permitted, regulated and prohibited use of software

The University must comply with its overriding legal and contractual obligations. Some of these obligations affect software and the uses to which it may be put. The Director of Digital Services has responsibility for IT at the University and this may include the prohibition of particular software.

Requests for access for restricted software need to be raised with the Digital Services helpdesk, along with a justification for access which will then be considered by the Director of Digital Services on a case by case basis.

14.10 Prohibited software and protocols

Certain software or protocols are barred from the University to protect the network for all users and to make sure that we comply with our obligations, and some software or protocols are limited to certain users who need it for academic purposes and who understand the risk of using the software.

- Network 'Sniffing' software & hardware.
- Instant messaging software (except those approved by IT).
- Games.
- Software that allows remote access to PCs other than that provided by Digital Services.
- Dropbox client (or equivalent).
- Malware.
- Any software or protocols to bypass firewalls.
- Key loggers.
- Any other software that hides or attempts to hide or disguise a user's activity on University provided facilities.

14.11 Restricted software / protocols

These software and protocols are restricted based on need, and similar to Elevated User Rights. This must be approved for access by your Executive Dean or Head of Department and the request forward to the IT Security team for access.

- Access to the Dark Web (Unless authorised by the Director of Digital Services).
- Torrent/file sharing applications (Only for accessing Linux distributions etc. that are non-copyrighted material).
- Penetration testing software (Only where authorised by the Director of Digital Services).
- Virtual Private Network Connections (Only where authorised by the Director of Digital Services).

14.12 Attempted use

Use or attempted use of any banned or restricted software on the University network will be considered a serious breach of the University disciplinary rules and will be dealt with by the appropriate conduct policy.

15. CLOUD STORAGE

15.1 Introduction

This section sets out the additional principles, expectations and requirements relating to the use of cloud storage and other similar services.

15.2 Definitions

The following terms apply to this section 15:
cloud storage refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be **synchronised** to multiple computers and mobile devices

such as mobile phone and tablets. They may also have facilities for sharing files with other people.

15.3 Purpose

This Policy defines the University's position on the use of cloud storage as it relates to storage of University data. The Policy sets out a clear definition of cloud storage and the types of University data which may be stored together with additional safeguards, which must be adhered to, in order to:

- Ensure compliance with national and international laws governing the storage and guardianship of data.
- Ensure that University employees and other partners understand the University's requirements relating to the storage and guardianship of data.

15.4 Scope

This Policy applies to all University data i.e. information which arises in University teaching, research and administration, and applies to all staff, post graduate students and other parties who have access to University data.

This Policy does not apply to personally-owned data (i.e. unrelated to University work).

- Considerations about who actually owns the data and therefore has full rights over it. Some cloud providers may assert ownership of any data stored in the provider's cloud, or reserve the right to do so in future.
- The financial stability of Cloud Storage providers should be considered to avoid a potential end of service with little or no notice.

15.5 Cloud storage for University use

The University provides undergraduates with Microsoft OneDrive storage, and Box storage for all staff and post graduate students.

Under no circumstances must University data be stored on other cloud services such as Dropbox or Google Drive, as they do not offer the protections required for this data. Any historical University data that has inadvertently been placed on other cloud storage must be migrated **immediately** to our approved providers, then deleted from the previous location.

In addition to allowing uploading and editing a variety of file types, BOX also allows users to:

- Add collaborators to folders.
- Sync Box with desktop folders for one-step editing.
- Include Box file links in the place of email attachments for more efficient collaboration.
- Link Box accounts to third-party apps and services for easy content management and surfacing.
- Track account activity via notification subscriptions.
- View account content and activity on mobile devices from any location. Box accounts provide users with free unlimited storage.

Important: Box **must not** be used to store and share information with an information classification of **Secret**. Any information that is classified as **Confidential** or **Highly Confidential** must have extra security measures to be saved to Box. For more information regarding recommended storage locations for specific data classifications set out in this Policy.

Box offers unlimited storage, includes a range of file viewers, supports adding metadata (to help with managing/finding data) and data can be retained when staff leave the University - this is critical to ensure that research teams do not lose data when a team member, for example a PhD student, leaves.

The University recommends Box for data generated, processed and analysed as part of your research. Box makes it easy to share data and offers automated backup to ensure your valuable research data is not lost. Box has a wealth of collaborative features in comparison to Dropbox. Compare BOX and Dropbox.

Digital Services offer a short course '**Box cloud storage – An Introduction'** which can be booked through Core HR. It is recommended all users complete this course as it contains important information regarding its features such as sharing documents and how to remove such shares when no longer needed.

When using Cloud Storage for collaboration with others, either from within the University or elsewhere, only grant access to files or folders that are required for the collaboration to take place. Access to personal data should be given on a strictly need to know basis to comply with the data protection legislation and regulation and strictly in accordance with the University's Privacy Policy and associated procedures.

It is essential to ensure that there is a suitable level of encryption on any mobile or portable device used to download any data about individuals from cloud storage. Such a device must be password protected.

16. ENCRYPTION

16.1 Introduction

This section sets out the principles and expectations of how and when information should be encrypted.

16.2 Definition

The following term applies to this section 16:
Encryption is the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

16.3 When to use encryption

Encryption must always be used to protect strictly confidential information transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing strictly confidential information (for example, in emails).

Where confidential data is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders) the devices themselves must be encrypted (using "full disk" encryption), irrespective of ownership.

Where strictly confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should be handled (stored, transmitted or processed) in accordance with the organisation's specified encryption requirements.

16.4 Key management

In most cases, encryption keys will be in the form of a password or passphrase. Losing or forgetting the encryption key will render encrypted information unusable so it is critical that encryption keys are effectively managed. When devices are encrypted by Digital Services, Digital Services will take responsibility for the secure management of the keys. In all other cases, it will be the individual member's responsibility to manage the keys. It is advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

16.5 Encryption standards

There are many different encryption standards available. Only those which have been subject to substantial public review and which have proven to be effective should be used. Specific guidance is available from Digital Services.

16.6 Export regulations

Export regulations relating to cryptography (encryption) are complex. Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes a provision whereby certain "public authorities" (including, but not limited to law enforcement agencies) can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK. Please refer to the Export Controls and Trade Sanctions Policy for policy information and further guidance.

16.7 Travelling abroad

Please refer to the IT Remote Working Policy for policy information and further guidance.

16.8 Laptop encryption

Since 1st October 2015 all University laptops have been issued with encryption software, there has been a program to encrypt all remaining laptops. From 1st January 2018 no University staff member may use an unencrypted University laptop. Any such laptops should be handed to the Digital Services helpdesk immediately to be encrypted.

Laptops that are used by students such as in the cabinets in the Library are exempt from this, providing that they are ‘deep frozen’ – A process that resets the machine to its original state each time they are used, thus doesn’t contain any data.

16.9 Desktop encryption

Desktops where sensitive personal data or data that is classified as sensitive or above must have their hard drives encrypted. This will also apply to all machines in departments where in the opinion of the University’s Head of Security or departmental manager the PCs are at elevated risk of being stolen. From 1st October 2017 new machines in the following areas or categories will be encrypted by default (except where by system enforced policy nothing can be saved to the local machines hard drive).

- Aston Medical School;
- Patient Data;
- Human Resources;
- Biomedical Sciences;
- Finance Department;
- Registry and Counselling;
- Anyone accessing security sensitive research.

17. SECURITY SENSITIVE RESEARCH

17.1 Introduction

This section outlines the process for how the handling of security sensitive research is handled and management from an information security perspective. The Counter Terrorism and Security Act 2015 establishes certain activities that should not be accessed except by those undertaking research in these areas.

To enable the University to meet its statutory duty any research in the following areas will need to be first approved by the University's Ethics Committee who will authorise the Director of Digital Services both to allow access and also to provide dedicated secure storage for these research materials to be stored and managed, as well as allow access through the University's firewall.

If in the opinion of the Director of Digital Services that the material should only be accessed from a specific or dedicated PC this request must be complied with.

Research in the following areas needs to follow this process:

- Work commissioned by Ministry of Defence.
- Animal rights research.
- IT encryption design.
- Terrorism.
- Extremism.
- Child pornography.
- Extreme pornography.

17.2 Storage

Any research data in these areas must only be stored on the dedicated storage space provided by Digital Services, who will make sure that only those who need access to such materials have access. To enable liaison with the Police and other security services the Chair of the Ethics Committee, and University (IT) Ethics Officer will have access to monitor compliance with this Policy.

18. INVESTIGATION OF COMPUTER USE

18.1 Introduction

This section is the Policy outlines the circumstances in which it is permissible for the University to access the IT accounts, communications and other data of its members.

The University respects the privacy and academic freedom of its staff and students and recognises that investigating the use of IT may be perceived as an invasion of privacy. The University may however, carry out lawful monitoring of its IT systems when there is sufficient justification to do so and when the monitoring has been authorised by the Director of Digital Services.

Staff, students and other members should be aware that the University may access records of use of email, telephone and other electronic communications, whether stored or in transit. This is in order to comply with applicable laws and regulations, and to ensure appropriate use of the University's IT systems.

Decisions to access the IT accounts, communications and other data of members will be taken by the Director of Digital Services (in conjunction with the Executive Director of Human Resources and Organisational Development) in order to ensure that such requests are free of bias and are not malicious. Investigations of this kind are sensitive and time-consuming.

18.2 Scope

All members (staff, students and associates) of the University together with any others who may have been granted permission to use the University's information and communication technology facilities by the Director of Digital Services are subject to this Policy.

18.3 The University's powers to access communications

Authorised University staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the University and may examine the content of these files and any relevant traffic data.

The University may access files and communications for the following reasons:

- Ensure the operational effectiveness of its services (for example, the University may take measures to protect its systems from viruses and other threats).
- Establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person).
- Investigate or detect unauthorised use of its systems.
- Ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the University's business.
- To monitor whether or not communications are relevant to the business of the University (for example, checking email accounts when staff are absent on holiday or on sick leave to access relevant communications).
- Compliance with information requests made under data protection law or Freedom of Information Act (individuals would in normal circumstances be notified).

18.4 The powers of law enforcement authorities to access communications

Certain non-University bodies and persons may be permitted access to user communications under certain circumstances. Where the University is compelled to provide access to communications by virtue of a Court Order or other competent authority, the University will disclose information to these non-institutional bodies/persons when required as permitted by the applicable laws. For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding issues of national security, the prevention and detection of serious crime or the safeguarding of the economic well-being of the UK.

18.5 Covert monitoring

Covert monitoring of computer use will only be authorised in exceptional circumstances by the Executive Director of Human Resources and Organisational Development (in consultation with the General Counsel and Director of Digital Services) where there is reason to suspect criminal activity or a serious breach of University policy and regulations and notification of the monitoring would be likely to prejudice the prevention or detection of that activity. The period and scope of the monitoring will be as narrow as possible to be able to investigate the alleged offence and the monitoring will cease as soon as the investigation is complete. Only information gathered in relation to the alleged offence will be retained. This information will

only be viewed by those for whom access is strictly necessary, for example in relation to potential disciplinary proceedings.

18.6 Procedure

Requests for investigation under this Policy may be made by any member of staff or student under the Whistleblowing Policy, although typically the request will come from an Executive Dean or Head of Department. Occasionally requests are made from outside of the University, for example by the police. All such requests will be addressed in accordance with the Whistleblowing Policy and when reported to the Director of Digital Services should include the following information:

- The name and department of the student or staff member whose computer or computing activity you wish to be investigated.
- The reasons for the request.
- Where computer misuse is alleged, the evidence on which this is based.
- The nature of the information sought.
- Any other relevant information, for example, that the request relates to ongoing disciplinary or grievance procedure.

In order to monitor the number and type of requests made, the University will keep a record of the requests that have been made and those which were acceded to. Repeat or malicious requests in the opinion of the Executive Director of Human Resources and Organisational Development and the Director of Digital Services, will be reported to the Chief Operating Officer whom if he concurs, may not be investigated.

19. PASSWORDS

19.1 Introduction

This section is of the Policy and outlines the requirements for permissible passwords access to IT accounts, systems etc.

19.2 Purpose

Passwords are an important aspect of computer security and the failure to use strong passwords may lead to the compromise of information and information systems.

This section defines the password policy for all users of IT Systems and has been implemented to safeguard information, comply with external business requirements and adhere to best practice. It establishes a minimum standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

19.3 Guidance

When creating strong passwords users need to ensure that they:

- Are a minimum of 8 characters. Mobile devices such as smartphones/tablets should have access controls activated but these may be a minimum of 6 characters (or an equivalent pattern-matching/biometric strength) and do not need to adhere to the above complexity rules but must be as strong as possible.
- Do not contain the user's account name.
- Do not contain 2 consecutive characters of the user's full name.
- Contain characters from 3 of the following 4 categories:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)

- Numbers (0-9)
- Special characters (for example, !, $, #, %)

- Are changed at least every 12 months.
- Are not reused for at least six changes.
- Do not contain common words found in a dictionary.
- Are not shared or disclosed.
- Are not used for personal 'non-business' systems.

Passwords/PINs used to access mobile devices (smartphones/tablets) do not need to be changed every 12 months but must be changed if the device has been compromised.

19.4 Helpdesk and Passwords

Digital Services IT Service Desk engineers will never ask for details of your password or other security credentials (unless you have self-initiated a password reset with the Service Desk), and therefore, you should never provide these either over the phone or in an email message.

20. GUIDELINES FOR SYSTEM AND NETWORK ADMINISTRATORS

20.1 Introduction

This section of the Policy and outlines the requirements for system and network administrators across the University.

System and network administrators, as part of their daily work, need to perform actions which, at times, may result in the disclosure of information held by other users in their files, or sent by users over the University's communications networks. This section sets out the actions of this kind which authorised administrators may expect to perform on a routine basis, and the responsibilities which they bear to protect information belonging to others. Administrators also perform other activities, such as disabling machines or their network connections that have no privacy implications; these are outside the scope of this Policy.

On occasion, you may need to take actions beyond those described in this document. Some of these situations are noted in this document itself. In all cases you must seek individual authorisation from the Director of Digital Services for the specific action that you need to take. Such activities may well have legal implications for both the individual and the University, for example under the Regulation of Investigatory Powers, data protection law and the Human Rights Act. Any such authorisation must be promptly obtained in all circumstances, and records must be kept to demonstrate the proper discharge of the relevant officer's duties.

System and network administrators must always be aware that the privileges they are granted place them in a position of considerable trust. Any breach of that trust, by misusing privileges or failing to maintain a high professional standard, not only makes their suitability for their role doubtful, but could also be considered by the University as gross misconduct. Administrators must always comply with this Policy and the Privacy Policy and should seek at all time to follow professional codes of behaviour.

20.2 Authorisation and authority

System and network administrators require formal authorisation from the 'owners' of any equipment they are responsible for. The law refers to "the person with a right to control the operation or the use of the system".

In the University this person is the Chief Operating Officer, who has delegated these rights to the Director of Digital Services who is therefore usually the appropriate authority to grant authorisation to system and network administrators for routine activities. For non-routine activities, the Chief Operating Officer has delegated these rights to the General Counsel.

System and network administrators are to contact the Director of Digital Services or the General Counsel for further advice as required.

20.3 Permitted activities

In accordance with Policy, the activities covered by these guidelines can be classified as operational or policy. Operational activities are undertaken to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. System and network administrators are acting to protect the operation of the systems for which they are responsible, for example, investigating a denial of service attack or a defaced web server is an operational activity as is the investigation of crime.

System and network administrators also play a part in monitoring compliance with policies which apply to the systems. These policies include those implicitly or explicitly set out in this Policy and the JANET acceptable use and security policies. In these cases, the system administrator is acting in support of policies, rather than protecting the operation of the system. The law differentiates between operational and policy actions, so the system administrator should be clear, before undertaking any action. System and network administrators are to contact the Director of Digital Services or the General Counsel for further advice as required.

20.4 Operational activities

Where necessary to ensure the proper operation of networks or computer systems for which system and network administrators are responsible, they may:

- Monitor and/or record traffic on those networks.
- Examine any relevant files on those computers.
- Rename any relevant files on those computers or change their access permissions (see Modification of data below).
- Create relevant new files on those computers.

When undertaking any of these activities, system and network administrators should act with due respect for users' reasonable expectations of privacy and adopt as light a touch as possible. Any work is completed in line with what's reasonable for the task in hand and no unnecessary or ancillary tasks would be permissible.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, system and network administrators must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file. If emails are marked as private or are contained in a folder marked as 'private and confidential' then permission must be obtained from the user to access the content.

System and network administrators must take all reasonable steps that these activities do not result in the loss or destruction of information. If a change is made to user file store then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

20.5 Policy activities

System and network administrators must not act to monitor or enforce this Policy unless they are sure that all reasonable efforts have been made to inform users both that such monitoring

will be carried out and the policies to which it will apply. If this has not been done through a general notice to all users then before a file is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or all the parties involved in a network communication. Please note that automated system activities are exempt from this requirement.

Provided system and network administrators are satisfied that either a general notice has been given or specific permission granted, they may act as follows to support or enforce policy on computers and networks for which they are responsible:

- Monitor and/or record traffic on those networks.
- Examine any relevant files on those computers.
- Rename any relevant files on those computers or change their access permissions or ownership in accordance with section 20.7 - Modification of data.
- Create relevant new files on those computers.

When undertaking any of these activities, you should act with due respect for users' reasonable expectations of privacy and adopt as light a touch as possible. Any work is completed in line with what's reasonable for the task in hand and no unnecessary or ancillary tasks would be permissible.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, system and network administrators must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file. If emails are marked as Private or are contained in a folder marked as 'Private and Confidential' then permission must be obtained from the user to access the content.

System and network administrators must ensure that these activities do not result in the loss or destruction of information. If a change is made to user file store then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

20.6 Disclosure of information

System and network administrators are required to respect the confidentiality of files and correspondence.

During the course of their activities, the University acknowledges that they are likely to become aware of information which is held by, or concerns, other users. Any information obtained must be treated as strictly confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation. This means that:

- Information relating to the current investigation may be passed to managers or others involved in the investigation.
- Information that does not relate to the current investigation must only be disclosed if it is thought to indicate an operational problem, or a breach of local policy or the law, and then only to management for them to decide whether further investigation is necessary.

System and network administrators must be aware of the need to protect the privacy of personal data and sensitive personal data that is stored on your systems in accordance with the Privacy Policy. Such data may become known to authorised administrators during the course of their investigations particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the Data Protection Officer.

20.7 Modification of data

For both operational and policy reasons, it may be necessary for system and network administrators to make changes to user files on computers for which you are responsible.

Wherever possible this should be done in such a way that the information in the files is preserved:

- Rename or move files, if necessary, to a secure file store, rather than deleting them.
- Instead of editing a file, move it to a different location and create a new file in its place.
- Remove information from public view by changing permissions (and if necessary ownership).

Where possible the permission of the owner of the file should be obtained before any change is made, but there may be urgent situations where this is not possible. In every case the user must be informed as soon as possible of any changes which have been made and the reasons for the changes.

System and network administrators may not, without specific individual authorisation from the appropriate authority modify the contents of any file in such a way as to damage or destroy information.

20.8 Modification of systems

All changes to a system no matter how minor must go through the University's Change advisory Board (CAB) which meets regularly and all requests for change must be submitted to, or in extra ordinary cases emergency change controls can be approved. Documents related to the change control board are available from Digital Services.

20.9 Granting access to systems

Each area must have its own guidelines for granting access to systems, and in particularly on giving users the minimum of access to systems to enable them to undertake their role, as well as making sure they are both trained technically on the systems, as well as understanding the legislation or local guidance on the use of those systems. System Administrators must logon to Servers / Management consoles with secondary accounts only. Whilst logged in with these accounts, high risk or day to day activities such as accessing external emails or browsing the internet must not be carried out.

20.10 Privacy policies

In a spirit of openness and transparency all services should have an associated privacy policy published. Each policy should be written in plain English and should be readily accessible to all users of the service. The relevant policy should provide users with the following information:

- Details of all of the information collected as a result of them using the service.
- The uses made of the information collected (the purposes of the collection).
- The retention period for the information collected.
- Details of who will have access to the information collected.
- The circumstances under which the information collected will be disclosed to others.

20.11 IP addresses

As any IP address assigned to the University (or otherwise used within the University) can, in association with other data held by the University, be used to identify individual users, the University considers such IP addresses to represent personal data within the meaning of the data protection legislation and regulations. As such, any processing involving University IP addresses must be held in accordance with such legislation and regulations.

20.12 References

The JANET website has examples of how these guidelines would apply in a variety of situations, while it is not possible to list all the applicable laws that apply to the work of system and network administrators, they are asked to carefully consider the following in conjunction with all subordinate legislation at all times while conducting your role. If system or network administrators have any questions regarding the detailed application of these applicable laws, please contact the Director of Digital Services in a first instance who will seek legal advice as required.

21. GUIDELINES FOR SECURITY AND PENETRATION TESTING

21.1 Introduction

This section of the Policy and outlines the requirements for penetration testing. Only authorised members that have explicit permission are permitted to conduct any form of penetration testing or port scanning on the University infrastructure. Any unauthorised user attempting to conduct any security relating testing will be subject to disciplinary measures.

21.2 External penetration testing

External penetration will take place at least annually (by an external company), and will attempt using their skills and knowledge, to see what University systems or infrastructure they can access remotely.

21.3 Internal penetration testing

Internal penetration will take place at least annually (by an external company), and will attempt using their skills and knowledge to see what university systems or infrastructure they can access whilst connected to the University network, identifying weakness in the University's infrastructure, configuration or any other items that may pose a risk to the University's IT security.

21.4 Penetration testing on hosted systems

Where possible the University works with companies hosting our systems to arrange annual penetration testing of their systems, or to gain access to penetration testing they commission on their systems or accreditation that they hold for their security.

21.5 Penetration testing on University systems

Penetration testing focused at a particular application particularly systems defined as key systems by the University (Student Administration, Human Resources, Finance) and others that are critical to the University operation need to be tested to make sure they give us the maximum protection possible from unauthorised access. Systems will always be tested on the following occasions:

- Testing new applications on go live.
- Testing new application on a major upgrade.
- A three year cycle to test all University applications software.

21.6 Internal scanning

A number of tools exist (for example, OpenVAS) to identify weaknesses that could be exploited by hackers etc. to compromise University systems, therefore a number of checks will be implemented, as follows:

- Termly scans of the whole Aston infrastructure.
- Monthly scans of the critical Infrastructure.
- Scans on specific servers or infrastructure following any change or new installation.
- Services before they go live.

21.7 Critical infrastructure

Criteria for high risk infrastructure is defined as follows:

- System exposed to the internet.
- System where access and privileges are not managed by active directory.
- Systems that hold sensitive personal information.

21.8 Annual plan

The annual plan for this testing with be agreed with the Library & Digital Services engagement group after consultation with key users across the University.

21.9 Follow up

Where the testing is undertaken by University staff it is expected that issues identified should be fixed as quickly as possible, particularly for systems that are not yet live this should be immediately, with all other issues being resolved ideally within five days, but longer where third parties need to make changes.

Where issues are highlighted as part of testing by our external company, an action plan should be produced within 14 days of the final draft being received, with actions being completed with a further 14 days. Anything out of these times scales will need to be agreed between the Director of Digital Services and Chief Operating Officer in the first instance, before being communicated to the strategy board at its next meeting.

If, in the opinion of the Director of Digital Services, a risk is identified that is so serious that it requires immediate action, he can authorise this up to and including the removal of an application, device or server from the University network.

Aston University
Birmingham
B4 7ET, UK

+44 (0)121 204 3000
aston.ac.uk

UNIVERSITY OF THE YEAR 2020 The Guardian

POSITIVE ABOUT DISABLED PEOPLE

Race Equality Charter
RACE CHARTER