Information Security Policy

Status: Approved by Executive December 2015

Version:

Date: December 2015

Reviewed: Every twelve months

Classification: Public

Which Sections are likely to be relevant to me?

Policy Section	**Undergraduate**	**Post Graduate/ Researcher / Academic**	**Technical / System Owners**
Information Security Policy	√	√	√
Information Security Policy – Executive Summary	√	√	√
Section 1 – Relevant Legislation to Information Security Policy	√	√	√
Section 2 – Authorised Officers			
Section 3 – Additional requirements	√	√	√
Section 4 - Outsourcing and Third Party Compliance		√	√
Section 5 - Human Resources			√
Section 6 – Internet Filtering, Recording and Retention.			√
Section 7- Information Handling		√	√
Section 8 - User Management			√
Section 9			
Section 10 - System Planning and Development			√
Section 11 - System Management			√
Section 12 - Network Management			√
Section 13 - Software Management			√
Section 14 - Mobile and Remote Working		√	√
Section 15 – Cloud Storage		√	√
Section 16 - Encryption		√	√
Section 17 – Security Sensitive Research (Approval and Storage)		√	√
Section 18 - Investigation of Computer Use		√	√
Section 19 - Passwords	√	√	√
Section 20 - Guidelines for system and network administrators			√
Section 21 - Guidelines for Security and Penetration Testing			√

Contents

Information Security Policy – Executive Summary

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 mobile devices of their own to connect to those systems.

The policy is modular. Please familiarise yourself with those sections that directly concern you. 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.

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, whilst most will be public and open, not all will
- 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
- 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 IT 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 IT 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 HR
- 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 IT 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
- Software that creates significant risks to the network such as Games, Instant messaging and Dropbox are not appropriate
- Mobile working is permitted from both personal and university owned devices. These devices must be password protected and secure. All new issue 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 IT 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

Please familiarise yourself with the sections of the policy that apply to you. We need to ensure our teaching and research is underpinned and supported by effective Information protocols and that our systems are compliant, robust and fit for purpose for all Aston staff and students

If you wish to comment on this document and the policy sections, please get in touch with the Director of IT Services

Information Security Principles

The following principles underpin this Policy:

1. Information will be protected in line with all applicable legislation and relevant University policies, notably those relating to data protection, human rights, prevent and freedom of information.
2. 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
3. Information will be made available solely to those who have a legitimate need for access.
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Breach of this Information Security Policy may be considered gross misconduct and compliance will be enforced accordingly.

Introduction

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.

Purpose

An effective Information 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.

Scope

The documents in the Information Security Policy and sections apply 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.

The documents in the Information Security Policy and sections apply to all information which the University processes, irrespective of ownership or form.

The documents in the Information Security Policy and sections apply to all members of the University and any others who may process information on behalf of the University.

Acceptable Use

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 IT Services are subject to this policy.

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 IT 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.

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 and
- 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, 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).

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 a University network must be managed effectively this includes

- Up to date antivirus
- 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.

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.

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 IT 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 IT Services.
- Failing to comply with a request from an authorised person for you to change your password.

Penalties for misuse

Minor breaches of policy will be dealt with by the IT Director. 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

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.

Purchasing of equipment

Software and hardware must only be purchased via the contracts established by procurement and administered by IT services, to make sure that everything being purchased is compatible with the University systems.

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 IT, users will not be reimbursed for the costs involved for unauthorised purchases.

Section 1 – Relevant Legislation to Information Security Policy

Introduction

The University must comply with certain legislation and associated regulations in relation to the use, storing and handling of information. When this policy was approved, this legislation includes but is not limited to the following statutory instruments referred to for the purposes of this document as "applicable laws"

Data Protection Act 1998

Freedom of Information Act 2000

Privacy and Electronic Communications 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 of Operations and Estates.

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.

Section 2 – Authorised Officers

Authorised Officers

For the sake of brevity and clarity the document refers to the Director of IT, this is the Director of Library and IT Services, and in his absence the IT Technical Director or IT Support Director will have the same authority as the IT Director (Director of Library and Information Services)

Section 3 – Additional requirements

Listed below are additional requirements the University has to comply with

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.

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.

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 brought other than via IT services.

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 Document Retention Policy.

.

Section 4 - Outsourcing and Third Party Compliance

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.

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.

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 IT, 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.

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.

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 the Universities Information Security Policy
- Compliance with the University's Data Protection 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; and
- 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 legal services (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 Legal Services to ensure the information security requirements are being satisfied. Advice should be sought from the Data Controller (Director of Governance), Head of Legal Services and/or Procurement in relation to contractual arrangements.

Personal Data

A Privacy Impact Assessment (PIA) must be completed at the outset of any project that will potentially involve personal data being accessed by a third party. 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.

If the outsourcing involves the transfer of personal data outside the European Economic Area (EEA), it must only be to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Information Commissioner's Office (ICO) provides a list of countries it has deemed to provide an adequate level of protection. Transfers to the USA are problematic following the ruling regarding the US EU Safe Harbour scheme. Please contact Legal Services for advice in relation to any proposed agreement where data could be transferred to the USA.

Informal outsourcing

There are extensive IT 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 the Data Protection Act 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 IT Services and/or the Director of Governance.

University staff must not configure their University email account automatically to forward incoming mail to third party services with which the University has 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.

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.

Section 5 - Human Resources

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

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.

Employment contract terms

All Employees sign terms of employment which bind them to comply with the University`s Policies

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.

IT usage monitoring and access

The Chief of Operations & Estates 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 Section 18 - the Investigation of Computer Use Policy

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 with the investigations policy.

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

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.

Section 6 – Internet Filtering, Recording and Retention.

Introduction

This 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.

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 (Approval and Storage).

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

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.

Section 7- Information Handling

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.

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.

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 disclosable 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, and any information which are not explicitly classified will be classified as open, by default.

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.

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. Advice can be obtained from the Estates & Capital Development Helpdesk.

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 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.

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.

There is other data that we handle on behalf of users such as Research Councils, NHS, European Union and Social Care organisations all of which the University must handle in line with its own and national policies for these areas.

Using personally owned devices

Any processing or storage of University information using personally owned devices must be in accordance with Section 14 - Mobile and Remote Working.

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.

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 a week, weekly backups that are kept for 12 weeks, and quarterly backups that are retained for a minimum of 24 months.

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

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 4 – 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 or above unless they are authorised to do so.

Reporting losses

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset to the information security team (mailto: dp_officer@aston.ac.uk) who as required will engage with the Legal Services team.

Section 8 - User Management

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.

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.

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 there status.)
- Members of Council (who will be recorded in the HR Systems).

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.

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 IT Services.

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.

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 the University's Information Security 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 users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. 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.

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.

Creation of User Accounts

User accounts can only be created from automated feeds from either the University HR 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.

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 IT may request that an account is suspended immediately).

When a member of staff`s system end date is reached (or passed) they will lose access to remote access to desktops (thereby freeing up the machine) and servers immediately. Access to other University resources such as email will be read only and the ability to send emails removed, three months after the end date the account will no longer be accessible. 12 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 deleted much sooner as the machine will be wiped before being passed to another user. If this needs to be a more flexible arrangement, it has to be approved by the Executive in line with Internal Audit recommendations.

Where leavers are not automatically deleted from systems, HR 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 HR.

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 setting etc. Some software by its nature requires these elevated user rights to run and so therefore some users may need these privileges. 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 & IT Services stakeholder group and to the University Audit 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 IT 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 the large majority of cases IT Services expect to retain full control of computers e.g. 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.

General Principles for granting Local Administrative Rights

IT 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 there is a strong case.

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 and IT 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.

Elevated User Rights will be withdrawn if a particular threat is identified or, for example, machine hardware is repeatedly corrupted. Appropriate notification will be given to staff depending on the threat posed to data security.

Section 9

Left intentionally blank

Section 10 - System Planning and Development

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 IT department).

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 integrated together

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

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.

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 its 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 IT Services Change Advisory Board (CAB)

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 server this functionality needs to be tested
- Business continuity plans must be in place for users of the system
- IT services must be informed and they must update their plans including the overall priority of recovering this system In the overall recovery plan of University systems.

Section 11 - System Management

Introduction

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

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.

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 the University's Information Security policy in its entirety and must always abide by the 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 IT 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 & IT 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 (see Section 7 - Information Handling Policy). 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 IT 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 Section 18 - Investigation of Computer Use" policy and the associated "Guidelines for system and network administrators" document.

System managers must immediately report any information security incidents to the IT Security Team (or, if unavailable, by email to abuse@aston.ac.uk)

Change management

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

File integrity monitoring software should be used where possible to help detect unauthorised system changes.

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.

Access must only be granted in strict accordance with Section 8 - User Management.

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.

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.

Vulnerability scanning

All systems should be 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 should be subject to regular (at least annual) penetration testing by an approved external assessor.

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.

Section 12 - Network Management

Introduction

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

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).

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 the University's Information Security policy in its entirety and must always abide by the policy.

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 the University's Section 18 -Investigation of Computer Use 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).

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.

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.

Change Management

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

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 malware
- A Supported operating system
- Capable of reporting centrally to IT on the current state of its patches and versions
- Must not introduce additional risk to the Universities 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.

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 IT Services.

Network addresses (IPv4 or IPv6) assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

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.

IT 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.

Section 13 - Software Management

Introduction

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

Definitions

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.

General software management principles

All software, including operating systems and applications must be actively managed. This function is normally managed by IT 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

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.

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.

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.

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

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 system or network security is prohibited unless authorised by the Director of IT.

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.

Software maintenance

All changes to computer systems are subject to IT 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 IT services will have upgrades installed on them automatically, and users are advised that overnight never to leave their machines with unsaved data, as IT 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 IT 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 IT director is authorised to remove on Utilitarian grounds.

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.

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 IT 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 IT helpdesk, along with a justification for access which will then be considered by the Director of IT on a case by case basis.

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.

Prohibited Software / Protocols

Certain software is not appropriate to have on the University network as it creates additional risks that cannot be effectively managed or can have unintended consequences that could affect the University systems.

- Sniffing software
- Instant messaging software (except those approved by IT)
- Games
- Software that allows remote access to PC`s other than that provided by IT 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.

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 IT Director)
- Torrent applications (Only for accessing Linux distributions etc. that are non-copyrighted material)
- Penetration testing software (Only where authorised by the Director of IT)
- Virtual Private Network Connections (Only where authorised by the Director of IT)

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.

Section 14 - Mobile and Remote Working

Introduction

This Section sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are not located on University premises when these devices are used to access University information assets with a classification of confidential or above.

While recognising the benefits to the University (and its members) of permitting the use of mobile devices and working away from the office, the University also needs to consider the unique information security challenges and risks which will necessarily result from adopting these permissive approaches. In particular, the University must ensure that any processing of personal data remains compliant with the Data Protection Act.

Definition

A mobile computing device is defined to be a portable computing or telecommunications device which can be used to store or process information. Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices (such as Google Glass).

Scope

This policy applies to all members of the University except for undergraduates and taught postgraduates (It is assumed that these groups will not have access to any material that is not already in the public domain) and covers all mobile computing devices whether personally owned, supplied by the University or provided by a third party. Personally owned, University owned or third party provided non-mobile computers (for example desktops) which are used outside of University premises are also within scope.

Personally owned devices

Whilst the University does not require its staff or postgraduate researchers to use their own personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to the following requirements and guidelines are followed. Users must at all times give due consideration to the risks of using personal devices to access University information and in particular, information classified as confidential or above:

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- Mobile devices must be encrypted. (Some older devices are not capable of encryption and these should be replaced at the earliest opportunity.)
- An appropriate passcode/password must be set for all accounts which give access to the device.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “auto lock” after a period of inactivity (no more than 10 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.
- Devices which are at risk of malware infection must run anti-virus software.

- All devices must be disposed of securely and any university information or data securely removed.
- The loss or theft of a device must be reported to IT Services.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to restricted University information assets.

In addition to the above requirements, the following recommendations will help further reduce risk:

- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (e.g. by “jail breaking” or “rooting” a smartphone).
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against “shoulder surfing”.
- Minimise the amount of restricted data stored on the device and avoid storing any data classified as strictly confidential.
- Access restricted information assets via the University’s remote access facilities (the “remote staff desktop”) wherever possible rather than directly.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching the Data Protection Act by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

University owned devices

The University may at times provide computing devices to some of its members. When it does, it will supply devices which are appropriately configured so as to ensure that they are as effectively managed as devices which remain within the office environment.

Devices supplied by the University must meet the minimum security requirements listed above for personally owned devices.

In addition, the following are required:

- Non-members of the University (including family and friends) must not make any use of the supplied devices
- No unauthorised changes may be made to the supplied devices
- All devices supplied must be returned to the University when they are no longer required or prior to the recipient leaving the University, irrespective of how they were purchased (for example, grant funding, pasa etc.)
- No attempt must be made to change the Universities standard configuration include the configuration of anti-virus and system updates.

Members should also follow the additional recommendations listed above for personally owned devices.

Third party devices

In general, members should not use third party devices to access restricted University information assets. This includes devices in public libraries, hotels and cyber cafes.

On occasion, staff and research postgraduates may be supplied with computing devices by third parties in connection with their research. These devices must be effectively managed, either by the third party or by the University or by the end user. In all cases, the device must meet the minimum security requirements listed above for personally owned devices.

Reporting losses

All members of the University have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any University information asset to the information security incident response team (abuse@aston.ac.uk).

Section 15 – Cloud Storage

Introduction

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

The University is currently investigating a Cloud Storage supplier that will mitigates many of the risks of Cloud Storage, in the interim please contact the IT Helpdesk if you need any advice.

Definition

For this Section, the phrase "cloud storage" refers to third party online storage services such as Google Drive, Dropbox and SkyDrive. 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.

Risks

Many people are now using public cloud storage in their private lives. This allows convenient access to their files and data from a number of different devices. If employed in a work context however, such services also introduce risks to the security, privacy, copyright and retention of University data. Before using cloud storage for work, users of the University computing environment must consider if the usage is appropriate and follow the policy guidance in this document to limit the risk imposed on University data.

The main risks when files are stored in public cloud storage are that:

- The University can no longer guarantee the quality of access controls protecting the data, access control becomes the responsibility of the user (default is often open to all)
- Backup / recovery of data (not normally done on cloud services)
- The location where the data is stored may not be guaranteed as remaining in the European Economic Area (EEA) so are unlikely to meet Data Protection Act requirements for personal data and the prospective European regulations.
- In many cases, public cloud storage requires that files be associated with an individual's personal account. Should that individual suddenly become ill, be absent for other reasons or leave, the University will lose access to the data
- Cloud services generally limit their liability for negligence, resulting in little or no recourse should the provider misuse, lose or damage information stored in the cloud
- Few cloud providers guarantee they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights
- Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment
- If they have financial difficulties a cloud storage provider may end the service with little or no notice, leaving users with no access to files or decide to charge elevated prices beyond

our ability to pay. We need to be mindful of the risk that there may be for the University to provide the storage to bring this data back in-house from a third party.

Requirements

The following policy requirements aim to mitigate the risks above.

All staff have a responsibility to protect the University's data, particularly data about individuals. Staff must familiarise themselves and adhere to the following University policies, guidance and information:

Working Off-Campus: Guidance on Data and Records

The University provides undergraduates with one drive storage, however this is not suitable for research or sensitive personal data. There is a supplier that enables us to make sure that data is appropriately secured, backed up and meets the terms of relevant UK and European legislation and regulation. Those that need Cloud storage (other than undergraduates) should contact IT in the first instance for help with their particular requirements and they will work with you to get this setup

There may be some circumstances when other services and providers may need to be considered for example when collaborating with other institutions which have a different service in place, such as Dropbox or Google Drive. If other services are considered then staff must evaluate the Terms of Service for each provider and ensure that the risks above are avoided. This evaluation must be recorded and authorised by the Appropriate Executive Dean or Director.

The following points relate to both University and externally provided services:

- Do not use cloud storage to store files containing information about individuals or other sensitive information. Please refer to the University Data Protection Policy for more information on this.
- The only exception permitted is in the case of external collaboration, only if no other secure alternative is available. Each exception must be approved by local management and recorded. Encrypting information about individuals or other sensitive information prior to uploading is mandatory. Further guidance is available in Section 16 - Encryption. The use of strong passwords on any encrypted files or folders is mandatory and is to be in accordance with Section 19 - Passwords.
- Do not use cloud storage for the long-term retention of University documents or files even for instances when you work with non-sensitive information. Use alternatives such as SharePoint and shared network drives provided by IT services.
- If you are 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.
- The University does not support or allow to be installed on its systems cloud storage clients or apps, such as those available for Dropbox.
- Do not store the only copy of a file in cloud storage
- You must 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.

Scope

This policy applies to all staff, data processors, partners, suppliers and contractors and other authorised users. Any exceptions must be documented and approved.

Section 16 - Encryption

Introduction

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

Definition

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.

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.

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 IT Services, IT 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.

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 IT Services and the University's Information Security website.

UK, EU and US Export Regulations. Law

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 contact Legal Services for further guidance on this matter.

Travelling abroad

When travelling abroad you are unlikely to encounter problems.

It is good practice however, to plan in advance and check everything is operational before you go.

The best information available changes regularly. For the most up-to-date information on the country or countries you are intending to visit, please check the latest Foreign Office Advice and Crypto law. A number of countries are specially banned from taking our encryption software to restrictions in place due to sanctions etc.

If you are stopped at a border and asked to log on to your laptop, just do as they say. They are unlikely to realise that your device is encrypted. You would just login as normal if asked.

If you are visiting a country where there is a high risk of your device being hacked, consider taking a small, cheap and blank device for use during that visit.

If you are visiting a country that you suspect will object to your encrypted device, it is not advisable to de-crypt your device for the visit. That is likely to coincide with a high-risk of your device being hacked.

Aston students based overseas whilst they access our systems securely remotely, this access may be blocked in a small number of countries. If this is the case such as access from China or Iran for example, please contact the IT security team for assistance ITsecurity@aston.ac.uk

In addition to what has been written above about export regulations, you should also be aware that government agencies in any country may require you to decrypt your devices or files on entry or exit from the country. If you are travelling abroad with encrypted confidential data this means that there is a risk that the data may have to be disclosed and you should consider the consequences of this. Wherever possible, do not take confidential data with you when you travel (keep the data at the University and access it using the University's secure, remote access facilities).

Particular attention should be paid to the possible inadvertent export of data subject to the Data Protection Act to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling

Laptop Encryption

All newly issued University laptops will from 1st October 2015 be issued with encryption software, and as machines are replaced or repaired encryption will be added.

Laptops that are used by students such as in the cabinets in the Library are exempt from this, providing that they are “deep frozen” and reset to their original state each time they are used.

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 PC`s are at elevated risk of being stolen.

Machines in the following areas or categories will always be encrypted (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
- Counselling
- Anyone accessing security sensitive research.

Section 17 – Security Sensitive Research (Approval and Storage)

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 Universities Ethics Committee who will authorise the Director of IT 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 Universities firewall.

If in the opinion of the Director of IT 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.

Storage

Any research data in these areas must only be stored on the dedicated storage space provided by IT 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.

Section 18 - Investigation of Computer Use

Introduction

This Section is part of the Information Security Policy and 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 IT.

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 IT Director(in conjunction with the Director of HR) in order to ensure that such requests are free of bias and are not malicious. Investigations of this kind are sensitive and time-consuming.

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 IT Services are subject to this policy.

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:

- to ensure the operational effectiveness of its services (for example, the University may take measures to protect its systems from viruses and other threats)
- to 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)
- to investigate or detect unauthorised use of its systems
- to 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)
- to comply with information requests made under the Data Protection Act or Freedom of Information Act (individuals would in normal circumstances be notified).

The Powers of Law Enforcement Authorities to Access Communications

A number of other non-University bodies and persons may be allowed 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.

Covert Monitoring

Covert monitoring of computer use will only be authorised in exceptional circumstances by the Chief of Operations and Estates (in consultation with the Head of Security and Director of IT) 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.

Procedure

Requests for investigation under this policy may be made by any member of staff or student under the speak-up policy, although typically the request will come from a head of department, school or directorate. Occasionally requests are made from outside of the University, for example by the police. The request should be made to the Director of IT and 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 Director of HR and the Director of IT, will be reported to the Chief of Operations and Estates whom if he concurs, may not be investigated.

Section 19 - Passwords

Introduction

This Section is part of the Information Security Policy and outlines the requirements for permissible passwords access to IT accounts, systems etc.

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 document 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.

Purpose

This policy establishes a minimum standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

Guidance

When creating strong passwords users need to ensure that they:

- are a minimum of 8* characters
- 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

* 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.

# 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.

Helpdesk and Passwords

The IT Department will never ask for full 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.

Section 20 - Guidelines for system and network administrators

Introduction

This Section is part of the Information Security 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 document 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 document.

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 IT 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, the Data Protection and the Human Rights Acts. You must therefore obtain such authorisation promptly in all circumstances, and records must be kept to help to protect you and the University from any charge of improper actions.

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 work within the University's information security and data protection policies, and should seek at all time to follow professional codes of behaviour

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 of Operations and Estates, who has delegated these rights to the Director of IT 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 of Operations and Estates has delegated these rights to the Head of Legal Services. You have both a right and a duty to be duly authorised by an appropriate person to undertake the activities set out in these guidelines.

If you are ever unsure about the authority you are working under you should stop and seek advice immediately as otherwise there is a risk that your actions may be in breach of the law.

Permitted activities

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. You are acting to protect the operation of the systems for which you 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.

You may also play a part in monitoring compliance with policies which apply to the systems. These policies include those implicitly or explicitly set out in the University's Information Security Policy and the JANET Acceptable Use and Security Policies. In these cases the 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 administrator should be clear, before undertaking any action.

Operational activities

Where necessary to ensure the proper operation of networks or computer systems for which you are responsible, you 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, you should act with due respect for users' reasonable expectations of privacy and adopt as light a touch as possible. Do not unnecessarily browse log files, for example, when you are looking for something specific.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, you must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file.

You 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.

Policy activities

Administrators must not act to monitor or enforce 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. (Automated system activities are exempt from this requirement).

Provided 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 (see Modification of data below)
- 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. Do not unnecessarily browse log files, for example, when you are looking for something specific.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, you must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file.

You 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.

Disclosure of information

You are required to respect the confidentiality of files and correspondence.

During the course of your activities, you 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

You must be aware of the need to protect the privacy of personal data and sensitive personal data (within the meaning of the Data Protection Act 1998) that is stored on your systems. 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 University's Data Protection Officer.

Modification of data

For both operational and policy reasons, it may be necessary for you 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.

You 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.

Modification of systems

All changes to a system no matter how minor must go through the Universities 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 the IT Service Director.

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.

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 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

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.

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, you are asked to carefully consider the following in conjunction with all subordinate legislation at all times while conducting your role.

- Regulation of Investigatory Powers Act (2000)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Data Protection Act (1998)
- Human Rights Act (1998)

If you have any questions regarding the detailed application of these applicable laws, please contact the Director of IT in a first instance who will seek legal advice as required.

Section 21 - Guidelines for Security and Penetration Testing

Introduction

This Section is part of the Information Security Policy and outlines the requirements for penetration testing.

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

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 Universities infrastructure, configuration or any other items that may pose a risk to the Universities IT Security.

Penetration Testing on Hosted Systems

Where possible we will work 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

Penetration Testing on University Systems

Penetration testing focused at a particular application particularly systems defined as key systems by the University (Student Administration, HR, Finance) and other that are critical to the University operation need to be tested to make sure they give us the maximum protect 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.

Internal Scanning

A number of tools exist (e.g. OpenVAS) to identify weakness that could be exploited by hackers etc to compromise University system, 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.

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

Annual Plan

The Annual plan for this testing with be agreed with the Library & IT Services engagement group after consultation with key users across the university including the Library & IT services engagement group.

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 system 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 IT and Chief of Operations and Estates in the first instance, before being communicated to the strategy board at its next meeting.

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

Acknowledgements

The 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.

Structure

The Information Security Policy document set 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 document includes a number of sections for ease of use, these sections are part of the policy which together constitute the Information Security Policy of the University. All of these documents are of equal standing although in the event of any inconsistency within the document, the overarching policy and any of the sections, the overarching policy will take precedence.

The sections of the Policy only 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.

Compliance

This policy document was approved by the University’s Council on TBC and any substantive changes may only be made with the further approval of Council.   The Council has delegated authority to approve any changes to the University’s Executive. Before approving any Section, the Executive will consult with the IT Strategy Board, , IT Services’ User Group and/or other groups as may be appropriate such as Campus Trade Unions (at the discretion of the Chief of Operations and Estates or his nominated alternate).

The IT Director will ensure that this policy is reviewed annually and has responsibility to ensure that this policy is and remains internally consistent.

Any substantive changes made to any of the documents which make up the policy will be communicated to all relevant personnel.

NOT PART OF POLICY BUT THE ACTION PLAN

Action Plan for IT Security Policy

Brief all University Systems Owners on policy

Information shared with all Staff

Popup on log requiring acceptance of policy before access is granted

Produce a project plan to fully implement this policy which will be monitored by the Library and IT services engagement group (including)

- Timetable of penetration testing of internal systems
- Progress in encryption desktops
- Progress in reviewing elevated user rights
- Progress on moving all storage onto University managed Servers
- Identification of secure remote access to files
- Progress on roll out of web filtering
- Progress on providing storage for Security Sensitive Research

Brief Library & IT engagement group on progress including informing of any decisions to grant

- Elevated user rights
- Reviewing Actions and Outcomes from Penetration Testing Reports

Which Sections are likely to be relevant to me?

Policy Section	**Undergraduate**	**Post Graduate/ Researcher / Academic**	**Technical / System Owners**
Information Security Policy	√	√	√
Information Security Policy – Executive Summary	√	√	√
Section 1 – Relevant Legislation to Information Security Policy	√	√	√
Section 2 – Authorised Officers			
Section 3 – Additional requirements	√	√	√
Section 4 - Outsourcing and Third Party Compliance		√	√
Section 5 - Human Resources			√
Section 6 – Internet Filtering, Recording and Retention.			√
Section 7- Information Handling		√	√
Section 8 - User Management			√
Section 9			
Section 10 - System Planning and Development			√
Section 11 - System Management			√
Section 12 - Network Management			√
Section 13 - Software Management			√
Section 14 - Mobile and Remote Working		√	√
Section 15 – Cloud Storage		√	√
Section 16 - Encryption		√	√
Section 17 – Security Sensitive Research (Approval and Storage)		√	√
Section 18 - Investigation of Computer Use		√	√
Section 19 - Passwords	√	√	√
Section 20 - Guidelines for system and network administrators			√
Section 21 - Guidelines for Security and Penetration Testing			√