Information Security Policy

Contents

Document Control
Reference: Information Security Policy
Issue No: 7
Issue Date: 19.05.2020
Author: Director of IT Services

Information Security Policy Statement

1.1 Introduction

1.1.1 The University is fully dependent upon the availability and integrity of its computer based information and IT services for many aspects of teaching, learning, research and administration. This makes it all the more essential to protect against the increasing risks facing the IT systems and infrastructure which form the basis of these essential services.

1.2 Objectives

1.2.1 The objectives of this Information Security Policy are to:

i. protect against the potential consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

ii. ensure that all the University's information assets and computing and network facilities are protected against damage, loss or misuse.

iii. ensure that all staff and student members of the University are aware of and comply with EU law (including General Data Protection Regulation) and UK law (including the Data Protection Act 2018) which applies to the processing of information.

iv. increase awareness and understanding across the University of the requirements of information security, and the direct responsibilities of users for protecting the confidentiality and integrity of the data which they themselves handle.

v. uphold the privacy principles and rights of the data subjects under data protection legislation.

1.3 Scope and Policy Structure

1.3.1 This document contains the high level policy which is seen as vital to protect the information assets.

1.3.2 This Policy is applicable to and is to be communicated to staff, students and other organisations or individuals who have access either to University 'restricted information' or 'highly restricted information', or to University computing and network facilities.

1.3.3 All staff / employees within the University are required to comply with this Information Security Policy.

1.3.4 The policy and associated General Conditions of Use of Computing and Network Facilities shall be reviewed and updated regularly to ensure they remain appropriate, for example in the light of any relevant changes in technology, the law, University policies or contractual obligations.

1.4 Risk Assessment and Management

1.4.1 Risks assessment and management is seen as a vital component of Information Security. To determine the appropriate level of security measures to be applied to information systems, it is important that a process of risk assessment is carried out for each system to identify the probability and impact of security failures. This will be done by IT Services with assistance from the appropriate manager.

1.5 Responsibilities for Information Security

1.5.1 Information security within the University is managed by IT Services. Responsibility for Information Security falls into the remit of the Registrar and University Secretary. IT Services' objective is to ensure that there is clear direction and visible support for security initiatives. The Registrar shall promote security through appropriate commitment and adequate resourcing.

1.5.2 The responsibility for ensuring the protection of information systems, and ensuring that specific security processes are carried out, lies with appropriate manager, or the owners managing that information system.

1.5.3 Specialist advice on information security shall be made available throughout the University from IT Services.

1.5.4 Individual staff and student members of the University also have specific responsibilities for Information Security, and these are made clear in this policy document and the associated General Conditions of Use of Computing and Network Facilities and BYOD policy.

2. Compliance

2.1 Intended Audience

This policy document applies to:

- All Users accessing Newman University systems, services and data
- Any auditor, internal or external, appointed to review the process

2.2 Assumptions and Constraints

Newman University ("the University") is a data controller, for the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018. It is assumed that all staff have an awareness of the data protection legislation and the consequences of the loss of University owned personal data, as data protection training is mandatory.

Compliance with the Information Security Policy, IT User Policies and BYOD Policy forms part of the Terms and Conditions of Employment of a member of staff, and also forms part of the General Academic Regulations.

2.3 Governance

IT management is regulated by the IT User Policies, including the Information Security Policy, General Conditions of Use of Computing and Network Facilities and the BYOD policy. They will be subject to regular review, in line with University guidelines, for effectiveness.

2.4 Statutory Duty

The University will ensure that Information Technology services are used to further the organisation's education and research, in accordance with the law.

The University has a statutory duty under section 26(1) of the Counter-Terrorism and Security Act 2015, known as the 'Prevent Duty', to have due regard to and aid the process of preventing people from being drawn into and supporting terrorism. It is part of the Government's counter-terrorism strategy with the aim of reducing the threat to the UK.
University members, staff or students must not create, download, store or transmit extremism related material with the intention of supporting or spreading terrorism. The University also reserves the right to block sensitive web sites, URLs and emails which are identified as supporting terrorism.

Use of University computer and computer network facilities is subject to the condition that users give express consent to the examination of any data stored in computers or computer systems or University devices. The University reserves the right to examine, monitor and intercept data, communications or the content of computers and devices for lawful purposes whenever it is deemed necessary, together with the authority to pass such data legally to third parties either as required by law or to fulfil the University's contractual obligations relating to the Network. This work is normally carried out by IT Services by the authority of the University Leadership Team on behalf of the University, in order to meet operational and security needs of the University and related investigatory activities.

2.4.1 All staff and students of the University and any third party with access to the University's information or computing systems will comply with the University's Information Security Policy, and where appropriate their compliance will be monitored.

2.4.2 The University will provide specific guidance on legal compliance, and line managers must also provide specific guidance on legal compliance to any member of staff whose duties require it.

2.4.3 Guidance documents will be made available to all computer users through the University's website covering the key aspects of the law of copyright, in so far as they relate to the use of information systems. Guidance will also available on the key aspects of computer misuse legislation, as well as providing a more general list of legal requirements.

2.4.4 The University will only process, disclose and share personal data in accordance with the requirements of the Data Protection legislation and the University's Data Protection Policy.

Personal or confidential information will only be disclosed in accordance with the privacy notices available to the data subjects. This includes sharing information with regulatory authorities, sharing information where we are compelled to by law, and sharing information to protect life.

2.4.5 Where personal data is being transferred to any external organisation then the guidance must be followed in the General Data Protection Regulation and can only be transferred using secured processes such as encryption, password protection or a multiple of authentication measures.

2.4.6 Retention and destruction of information must be in accordance with the Retention and Disposal Schedule - this defines appropriate lengths of time for different types of information to be held, taking into account legal obligations. Data will not be destroyed prior to the expiry of the relevant retention period and should not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

2.4.7 Access to information contained in information systems may be required for a variety of management purposes, including procedures where evidence is required, in which case the use of defined procedures needs to be observed in order to safeguard evidence and ensure legal compliance. Expert guidance will normally be sought.

2.4.8 The University requires procedures to be observed in the operation and administration of information systems, and will implement a regime of monitoring, enforcement, and where necessary interception, to ensure this.

3. Employee Compliance

3.1 Terms and Conditions

3.1.1 All employees must comply with the University's information security policies contained in this document, as well as the associated IT User Policies including the General Conditions of Use of Computing and Network Facilities, BYOD policy and Wireless Networking Policy. This requirement will be included in the Conditions of Employment.

3.1.2 If, after investigation in connection with a security incident, a user is found to have violated the University's Information Security Policy and/or IT User Policies or procedures, they may be disciplined in line with the University's formal disciplinary process.

3.1.3 In accepting employment with the University members are agreeing that 'restricted information' or 'highly restricted information' to which they will be given access as part of their responsibilities must be kept confidential (both during and after their employment with the University). As part of the induction process for new staff, managers must ensure that this is drawn to the attention of new staff who will be involved in the handling of 'restricted information' or 'highly restricted information'. All staff must undergo appropriate data protection training as defined by the Data Protection Policy.

3.2 Recruitment and Contracts

3.2.1 Where it is known that new University staff will be dealing with 'restricted information' or 'highly restricted information' as part of their duties, this should be referred to in their job description.

3.2.2 All external suppliers, contractors, temporary staff and casual workers who are contracted to supply services to the University, and who will thereby require access to the University's computing and network facilities or 'restricted information' or 'highly restricted information' - must agree to follow the Information Security Policy of the University. An appropriate summary of the Information Security Policy must be formally delivered to any such supplier prior to any supply of services. It is the responsibility of the manager involved to ensure that each individual involved in the supply of services is made aware of the issues relating to information security.

3.3 Leaving Staff and Students - Email accounts

3.3.1 When a member of staff leaves, their access to IT systems and computing facilities are withdrawn on the day that they leave; any exceptions to this must be authorised in advance by Human Resources. These exceptions will need to take account of staff that are likely to return. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges.

3.3.2 Once students have completed their studies at Newman and upon graduating – or leaving voluntarily, their Newman domain email address is retired. The only exception is for further post-graduate or research study. Those students who are later employed by Newman University either permanently or temporarily will be issued with new network and email credentials.

3.3.3 All email accounts operated from the Newman network – are the possession of Newman for University business and can be at any time backed-up, modified, interrogated or withdrawn.

4. Use of Computers and Access Control

4.1 Access Control and Management

4.1.1 Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff.

4.1.2 All users shall have a unique identifier (user ID) for their personal and sole use for access to one or more of the University's IT services. The user ID must not be shared with or

used by anyone else, and associated passwords must not be shared with any other person.

4.1.3 The user ID must not log anyone else, including children, into their computer profile.

4.1.4 Password management procedures shall be put into place to ensure the implementation of the requirements of the Information Security Policy. The selection of passwords, their use and management must adhere to best practice guidelines.

4.1.5 Access control standards must be established for all information systems, at an appropriate level for each system which minimises information security risks yet allows the University's business activities to be carried out without undue hindrance. Access control standards will be reviewed for each information system at appropriate intervals.

4.1.6 Access to all IT Services must be authorised by the Director of IT Services and appropriate manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted.

4.1.7 Procedures shall be established for IT services to ensure that users' access rights are adjusted appropriately and in a timely manner, whenever there is a change in business need, role change, or staff or students leave the University. Users' access rights will be reviewed at appropriate intervals.

4.2 Use of Computers

4.2.1 Managers and staff responsible for PCs and other IT equipment within the University must also be responsible for ensuring the equipment is safeguarded appropriately – especially when left unattended.

4.2.2 It is the responsibility of a member of staff to take reasonable precautions against theft of 'restricted information' or 'highly restricted information' from a device they are using, a device dedicated to their own use, or from the office where the PC is located.

4.2.3 Files or documents downloaded from the internet, email attachments, portable media or any other electronic source must be treated with appropriate care to safeguard against both malicious code and inappropriate material. All such files must be scanned for possible malicious code before being opened, as detailed in the Virus Management Policy.

4.2.4 Email must not be used to communicate 'restricted information' or 'highly restricted information' unless appropriate password protection measures have been taken to ensure confidentiality and that it is correctly addressed to the recipients who are authorised to receive it. Email Procedures regarding Data Protection are available on the intranet.

4.2.5 Any important information stored on devices such as a laptop or a PC's local disk must be backed up at an appropriate frequency. To facilitate this IT Services maintains regular back up procedures for the networked drives.

4.2.6 Users must not store any Newman data, whether 'ordinary', 'restricted' or 'highly restricted', on the hard-drive (e.g. C-drive) of a University owned desktop computer or laptop. This drive is located on the actual computer and is not backed up. If the device were to fail this data would be irretrievable. If this device were to be stolen the data may be able to be accessed and this would be a data breach.

4.2.7 Utmost care must be used when transporting files on removable media to ensure that version control is correctly maintained, i.e. valid files are not overwritten, and incorrect or out of date information is not imported.

4.2.8 Users are not permitted to install any software on to the University network; arrangements need to be made with IT Services.

4.3 Third Party Access

4.3.1 All external contractors or suppliers who are contracted to supply services to the University involving access to or use of the University's hardware, software or 'restricted information' or 'highly restricted information' must agree to follow the University's Information Security Policy. A summary of the Information Security Policy will be provided to any such supplier, prior to any supply of services. Due diligence on selected third parties will be carried out before engagement.

4.3.2 The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality (Non-Disclosure) agreement to protect its information assets.

4.3.3 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's Information Security Policy.

4.3.4 Any facilities management, outsourcing or similar company with which the University may do business must be able to demonstrate compliance with the University's Information Security Policy.

5. Information Handling

5.1 Inventory and Asset Classification

5.1.1 An inventory will be maintained of all the University's major information assets and the ownership of each asset will be clearly stated in the 'Data Asset Classification Register'

5.1.2 Information and outputs from systems producing data must be appropriately labelled according to their level of classification. i.e. Restricted, Highly restricted.

5.2 Disposal of Equipment with 'Restricted Information' or 'Highly Restricted Information'

5.2.1 When permanently disposing of equipment containing storage media, all 'restricted information' or 'highly restricted information' and licensed software will be irretrievably deleted either before the equipment is moved offsite, or by utilising an approved 3rd party off-site service.

5.2.2 Damaged storage devices containing 'restricted information' or 'highly restricted information' will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the permission of IT Services.

5.2.3 In addition, Desks and screens on which 'restricted information' or 'highly restricted information' is processed or viewed should be appropriately sited in such a way that they cannot be viewed by unauthorised persons.

5.2.4 Computer users must lock their screens when unattended.

5.2.5 Any third party used for external disposal of the University's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with the University's Information Security Policy.

5.3 Handling Confidential Data and Documents

5.3.1 If removal off site of the University's 'restricted information' or 'highly restricted information' assets becomes imperative because of critical operational reasons applying to either print or storage media (incl: USB or Hard Drive), in line with 'Encryption of Data clause 5.5.3' this should first be approved by the manager and authorised with the Director of IT Services. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out by those requesting to remove 'restricted information' or 'highly restricted information' assets off-site.

5.3.2 All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the privacy, confidentiality, integrity and availability of such files.

5.3.3 'Restricted information' or 'highly restricted information' should only be accessed from equipment in secure locations.

5.3.4 All employees are required to be made aware of the risk of breaching confidentiality associated with the copying (including photocopying or other duplication) of 'restricted information' or 'highly restricted information'. Authorisation for copying such documents should be obtained from the appropriate manager.

5.3.5 All hardcopy documents of 'restricted information' or 'highly restricted information' are to be shredded or disposed of as confidential waste when no longer required. Approved software deletion methods must be employed for similar electronic documents.

5.3.6 Prior to sending 'restricted information' or 'highly restricted information' /documents to third parties, not only must the intended recipient be appropriately authorised to receive such information, but the information security measures adopted by the third party must also continue to assure the confidentiality and integrity of the information.

5.3.7 'Restricted information' or 'highly restricted information' may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured – and only in encrypted form when transferring to hosted services.

5.3.8 Staff participating in conference and videoconference are expected to be aware of the information security issues involved and are expected to maintain appropriate confidentiality both during and after a phone / video meeting.

5.3.9 Staff need to ensure that work conversations and meetings cannot be overheard, whether these conversations are in person or on a phone call / video call. When participating in a phone / video call it is recommended to use a headset / earphones to prevent anyone nearby overhearing the other people on the call.

5.4 Communication by Email and Telephone

5.4.1 Email addresses should be checked carefully prior to transmission, especially where the information content is 'restricted information' or 'highly restricted information', or where the disclosure of email addresses or other contact information to the recipients is a possibility.

5.4.2 The identity of recipients or requesters of 'restricted information' or 'highly restricted information' over the telephone must be verified and they must be authorised to receive it.

5.4.3 Email should only be used for business purposes in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the classification of the information being sent and checking that the attachment is password protected in accordance with the Email Procedures regarding Data Protection available on the intranet.

5.4.4 University-provided devices (including but not limited to desktop computers, tablets, laptops and phone handsets, whether landline / VOIP / mobile) and IT systems (including but not limited to email, Moodle, lecture capture, MyNewman, and SITS) are for work use and therefore the University reserves the right to access the stored content on those devices and systems.

5.5 Use of Encryption

5.5.1 Encryption will be utilised where data is moved to hosted services to provide appropriate levels of protection to 'restricted information' or 'highly restricted information' whilst ensuring compliance with statutory, regulatory and contractual requirements.

5.5.2 Automated processes shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

5.5.3 Removable Storage media containing 'restricted information' or 'highly restricted information' must be encrypted with inbuilt encryption or software such as 'Bitblocker' or password protected before being removed off-site.

6. Network Management

6.1.1 The University's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security issues.

6.1.2 The network must be designed, configured and operated to deliver high performance, reliability and availability to meet the University's needs whilst providing a high degree of flexibility to maintain security controls and a range of appropriate levels of quality of service.

6.1.3 The network should be segregated where appropriate into separate logical sub-networks taking account of security requirements, with routing and access controls operating between the sub-networks. Appropriately configured firewalls and other security mechanisms where appropriate shall be used to protect the sub-networks supporting the University's business critical systems.

6.1.4 Access to resources on the network must be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to the network, and all computing and information systems and peripherals shall be restricted unless explicitly authorised.

6.1.5 Devices may only be connected to the network with the prior approval of an authorised member of staff within IT Services. It must also first be registered with IT Services before being connected.

6.1.6 Moves, changes and other reconfigurations of network access points will only be carried out by staff authorised by the Director of IT Services according to agreed procedures.

6.1.7 Implementation of new or upgraded network software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to business critical systems or network components. All changes must be tested and authorised before being implemented in the live environment.

6.1.8 The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

6.2 Remote Access/ Remote Working

6.2.1 The same level of professionalism and confidentiality must be maintained when working off-site / remotely as when working on campus.

6.2.2 Persons who will be doing part or all of their computing work at a location outside the University footprint must be authorised to do so by an appropriate manager and information owner.

6.2.3 Remote access to resources on the network will be made available only through authorised entry points, normally through the site firewall and using a RDP portal. Remote access to non-public resources will be subject to authentication and other security mechanisms

6.2.4 Those using their own devices, as defined by the Bring Your Own Device (BYOD) Policy, for remote working must follow the agreed security procedures at all times as specified in the BYOD Policy, which advises users how remote computing equipment should be used in order to conform to the University's Information Security Policy.

6.2.5 Personal data as defined by the GDPR / DPA 2018, which includes personal data in the 'ordinary', 'restricted' and 'highly restricted' categories of the Information Classification Table, must not be stored on personal cloud services, with the exception of the University provided 'OneDrive'. Bear in mind that the University provided 'OneDrive' facility is not backed up so documents that could not be replicated if corrupted, should not be stored on 'OneDrive'. It is recommended you should use the University provided storage (currently the S-drive and Z-drive). This is constantly under review and other cloud services may be appropriate in the future at which point this policy will be updated to reflect this.

6.2.6 The University has a secure encrypted virtual desktop, using remote desktop protocols (encrypted data traffic). Remote Desktop Connection (RDC) is available to staff to provide a direct connection to their Newman computer profile whilst working on a different internet-connected device e.g. for example when off campus. Through this staff can access their Outlook, Z-drive, desktop, the S-drive, other shared drives you have access to, iTrent etc. Working through RDC reduces the need for duplicating documents on USBs, external storage, OneDrive or emailing documents to themselves. If that is unavailable on their device staff need to use an external storage device e.g. a USB / flash drive which is password protect or uses a Bitlocker program to protect the files containing personal data. The files containing personal data should remain on the USB / flash drive

and not be copied or stored on their own device. The files should be on the USB / flash-drive for the least length of time required and after that time must be securely deleted.

6.2.7 It is advised that 'restricted information' or 'highly restricted information' is only sent by email when necessary. Email Procedures regarding Data Protection must be followed. The recommended method of password protecting documents (and therefore attachments) is 7-zip. Guidance on how to set up these measures is available from the online IT Services Helpdesk pages currently on SharePoint and the intranet.

6.2.8 Hard-copies of 'restricted' or 'highly restricted information' should only be taken off site when necessary, for the minimum time necessary, stored securely in transit and stored securely at home / where you are taking it to.

6.2.9 Breaches of electronic or hard-copies of 'restricted' or 'highly restricted' information need to be reported as a matter of urgency in accordance with the Data Breach Reporting Procedure.

6.2.10 Users need to familiarise themselves with and follow the Instructions for Working Off-site and Zoom Guidance: how to use Zoom well.

7. Systems Operation and Management

7.1 Operations Policy

7.1.1 Offices and other areas where 'restricted information' or 'highly restricted information' or critical information is processed shall be given an appropriate level of physical security and access control.

7.1.2 All persons, whether staff or contractors, with authorisation to enter areas where 'restricted information' or 'highly restricted information' or critical information is processed are to be provided with information on the potential security risks and the requirement to comply with the Information Security Policy.

7.1.3 The procedures for the operation and administration of all systems and activities forming part of or related to the University computing and network facilities must be documented by those responsible for them, with the procedures and documents being reviewed and maintained at appropriate intervals. Where practical to do so, the users of the procedures should be involved in this review process.

7.1.4 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and computing and network facilities. Mechanisms shall be in place to monitor and learn from those incidents.

7.1.6 Continual reviews of operational procedures must be assessed to ensure ongoing compliance with the requirements of information security and the protection of data.

7.1.7 Development and testing facilities for business critical systems shall be separated from operational facilities where economically feasible, and the migration of software from development to operational status shall be subject to formal change control procedures.

Exceptions to this will be specifically approved by the Director of IT, and documented with reference to the level of risk which has thereby been accepted.

7.1.8 The security risks to the information assets of all system deployment and development projects shall be assessed and access to those assets shall be controlled. This will include all aspects of integration with existing systems.

7.1.9 An audited Disaster Recovery Plan and Business continuity plan is documented and annually tested for existing and new operational systems, software and services. Penetration tests are scheduled annually and evaluated for any weakness.

7.1.10 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

7.2 System Management

7.2.1 The University's systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with IT Services. All systems management staff shall be given relevant training in information security issues.

7.2.2 Within the information inventory each system or service will be classified according to its criticality in terms of impact in the event of loss of system on the University's business, as reflected in the 'IT Business continuity plan'.

7.2.3 Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the appointed manager of the system or application. A record of access permissions granted must be maintained.

7.2.4 Access to all information systems, excluding publicly accessible data sources, shall use a secure logging-on process. Access to information systems is to be logged and monitored where appropriate to identify potential misuse of systems or information.

7.2.5 Password management procedures shall be put into place to meet the requirements of the Information Security Policy.

7.2.6 Only authorised staff will be permitted to perform systems administration or management functions. Use of commands to perform these functions should be logged and monitored where it is considered appropriate and feasible to do so.

7.2.7 Formal change control procedures, with audit trails, shall be used for all changes to business critical systems. All such changes must be risk assessed and authorised by the Director of IT before being moved to the live environment.

7.2.8 Capacity demands of systems supporting business processes shall be monitored where practical, and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

7.2.9 Security event logs, operational audit logs and error logs must be reviewed and managed by qualified staff.

7.3 System planning

7.3.1 New information systems, upgrades to existing systems or hosting services (cloud) must be authorised jointly by the manager(s) responsible for the information and IT Services. The authorisation process must take account of security requirements and data protection measures.

7.3.2 Equipment supporting the University's systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

7.3.3 Equipment supporting the University's systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

7.3.4 Access controls for all information and information systems are to be set at appropriate levels in accordance with the value of the information assets being protected.

7.3.5 Prior to acceptance, all new or upgraded systems shall be tested and the results documented to ensure that they comply with the University's Information Security Policy requirements for ongoing information security management. A Data Protection Impact Assessment (DPIA) must be carried out on all new or upgraded systems involved in the processing of personal information.

8. Business Continuity Management (as detailed by the Disaster Recover Policy)

8.1 The University will maintain a co-ordinated approach to the assessment of business continuity requirements across the University, and the identification of appropriate areas for further action.

8.2 A formal risk assessment exercise is regularly conducted to classify all systems according to their level of criticality to the University and to determine aspects of Data security.

8.3 A Business Continuity Plan is regularly reviewed and audited with provision for each system or activity identified in 8.2 where the need has been established. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.

8.4 All relevant staff will receive appropriate training to be able to carry out their roles with respect to Business Continuity Plans.

8.5 IT Services is responsible for backing up business critical systems, users should ensure that they maintain a suitable backup for non-critical data. The Director of IT, with the assistance of the Network Team is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the University and its business interests.

9. Compliance Sanctions and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the University's disciplinary policy.

10. Equality and Diversity

This Policy has been reviewed for accessibility and inclusion purposes.

11. Feedback and Further Information

The University welcomes feedback on this Policy. If you would like to comment or need further information, please contact the IT Helpdesk or the Director of IT Services.

12. Related Policies and Procedures

This policy is related to the following policies and procedures:

Access Control Policy
Bring Your Own Device (BYOD) Policy
Computing and Networking Facilities: General Conditions of Use
Confidential Paper Waste Procedure
Data Breach Reporting Procedure
Data Protection Impact Assessment (DPIA) Screening Questions Checklist and DPIA Template
Data Protection Glossary
Data Protection Internal Information for Staff

Data Protection Lawful Basis Explanations
Data Protection Policy
Data Protection Posters – practical actions
Email Merge from Excel Instructions
Email Procedures regarding Data Protection
Guidance for Handling Personal Data Off-Site
Guidance for Management of Research Data
How to encrypt a memory stick using Bitlocker
Information Classification Table
Instructions for Working Office-Site (inc. IT, data protection)
New Project Development Procedure – Data Protection
Password Policy
Password Protecting Attachments using 7-Zip
Password protecting documents in Microsoft Office
Reviewing Contracts – Data Protection Clauses
Virus Management Policy
Wireless Networking Policy
Zoom Guidance: How to use Zoom well