University of Central Lancashire

IT Security Policy

September 2016 -
August 2017

STUDENT REGULATIONS AND POLICIES

uclan.ac.uk/studentcontract

Contents

1 INTRODUCTION

The University uses a large amount of information in order to operate effectively and the majority of this information is in electronic format and held on computers and in our IT systems. It is essential that this information is managed effectively so that it remains secure, accessible to authorised users and its integrity is protected. The IT Security Policy sets standards outlining the way electronic information and IT systems should be managed and operated to ensure the University complies with its obligations in relation to IT Security. The policy sets out how all users of University IT systems and the information they contain must act to ensure these standards and obligations are met.

The policy is divided into a number of sections. There is a section which contains information applicable to all staff and students and a section which contains information applicable to LIS staff and IT system administrators outside LIS. All employees and other users of the University's IT systems must read and comply with all sections relevant to them. A glossary of terms is available at the end.

2 SCOPE OF THE POLICY

The IT Security Policy covers all internal University systems and connections to wider networks. It sets out how information contained within or accessible via those IT systems should be handled to ensure it remains secure. It must be read in conjunction with the IT Security Incident Handling Guide which is available on the intranet.

All systems within the University and connections to outside bodies must conform to this policy. The University reserves the right to isolate any IT system or network which represents a potential or actual breach of security; to monitor information sent over its networks; and to deny user access to the universities IT systems.

3 POLICY STATEMENT

The University recognises the importance of keeping its information and IT systems secure and protected from unauthorised use. Through compliance with this policy, the University will ensure that all corporate information generated, used and held electronically in IT systems, networks, media and related forms is accurate, secure and available to authorised users for business purposes when needed.

4 RESPONSIBILITIES

This policy applies to all students, employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University.

The Chief Operating Officer (COO) has overall responsibility for ensuring the University complies with this policy. The COO is supported in their responsibility by LIS. Any questions or concerns about the operation of this policy should be referred in the first instance to LIS:

LISCustomerSupport@uclan.ac.uk or ext. 5355.

This policy is reviewed annually by LIS on behalf of the COO. Recommendations for any amendments should be reported to LIS Head of IT Security for consideration as part of the review process. UCLan will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

5 RELATIONSHIPS WITH EXISTING POLICIES

This policy must be read in conjunction with the following policies and guidance applicable to the user:-

The following are available at https://www.uclan.ac.uk/students/life/rules_regs.php

Rules for the use of the University's IT facilities

Email Use Policy

Data Protection Policy (and associated guidance)

Freedom of Information Policy

Rules for the Use of the Library

The following apply to staff only (see intranet):

Staff Handbook

Copyright information for staff

Bring Your Own Device Policy

UCLan Information Categories

Sharing Documents and Data

The following policy applies to all users and can be found via the link provided:-

Acceptable Use Policy of JANET (Joint Academic NETwork)

https://community.jisc.ac.uk/library/acceptable-use-policy

6 GENERAL - IT SECURITY POLICY FOR ALL STAFF AND STUDENTS

The information in this section of the policy is applicable to all users of the University's computer systems. All users must read and comply with this section and any other applicable sections.

6.1 KEEPING INFORMATION SECURE

Organisational information must remain secure at all times and must be protected from disclosures to unauthorised parties. Where organisational information is personal data, confidential or commercially sensitive, access to the information must be restricted to those individuals who have a legitimate need for it in order to do their job.

Individuals who use the University's computer systems to process personal data must comply with the requirements of the Data Protection Act 1998 as set out in the Data Protection Policy and associated guidance, which can be found on the Information Governance pages of the staff intranet.

For mobile devices such as tablet computers, PDAs, smartphones etc; the user must ensure the device PIN or password has been set and that the device is set to automatically lock after a short period of inactivity. This will help protect the device against misuse and is an extra safeguard for any personal contact details or any other confidential information held on the device should it fall into the wrong hands; however this does not replace the need for encryption. Any device without a PIN or password as a minimum security measure must not be used to hold any organisational information.

Users should note that if a device is lost or damaged, the information stored on it may not be recoverable. These types of devices should therefore never be used to store the only copy of information.

Where encryption is used, decryption passwords must be kept securely and separately. Information which is encrypted cannot be accessed without the encryption password.

A checklist for students has been published to provide guidance on safety and security when using mobile devices.

6.1.1 STAFF-SPECIFIC

All staff should follow the published University policy and guidance on Information Categories, Sharing Documents and Data, and Bring Your Own Device (BYOD). These documents are all located in the LIS Resource Centre and cover the following relevant points.

- Device security.
- User safety and security.
- Encryption.
- Sending documents by email.
- Storing and sharing documents "online".

Where possible, online services, Remote Access or UCLan-Global should be used to access University systems thus avoiding the need to store information locally, however temporary storage of information is acceptable provided that the information:

- is categorised as "Public", or "Internal".
- Is stored on the device/media only for as long as absolutely necessary.
- is encrypted.
- is deleted or removed from the device or media as soon as it is no longer required.

Users must not send or otherwise disclose to external parties photographic images of other individuals obtained from the University's email system or from any other electronic communication systems provided by the University.

Computers and other devices must not be accessible to anyone other than authorised users of the University's systems. Computers must be locked when unattended to ensure information is not accessed by anyone other than the user who is logged in. Computers must be logged out and shut down overnight to maintain security and ensure essential system updates are installed. Additional security guidance when working with personal data is available on the Information Governance pages of the staff intranet.

6.2 User accounts and passwords

Individual users will each be given a personal University account for which they are held responsible. The account is for the sole use of the authorised user for access to the University's IT facilities. Users must not permit their account to be used by anyone else and users must not use or attempt to use someone else's account.

User passwords must not be shared and only known to the user and the computer system. Managers, colleagues or computer system administrators do not need to know a user's password and must not ask for it. Passwords must not be written down or stored on or near a computer.

All users are required to register to use the self-service password service by going to the registration web page https://passwordregistration.uclan.ac.uk.

If a user forgets their password, they must go to the Self-Service Password Reset web page https://passwordreset.uclan.ac.uk where they will be asked to provide the answers to three of the questions they set up when they registered.

Users can change their own passwords without administrator intervention, either on University computers by using the Change Password application from the Start menu or through the self-service password service.

Users must follow good security practices when selecting passwords. Passwords should be at least eight characters in length and should include numbers, mixed case letters and symbols. They should not be made up of strings of the same characters, real words or common passwords such as family names, car registration numbers, telephone numbers and days of the week or other aspects of the date. These types of password are easy to crack and can lead to security breaches due to unauthorised access.

If users suspect that a password may be known to an unauthorised party, the password should be changed immediately and not used ever again.

It is good practice to use a different password for your university account than any personal/private accounts.

6.3 Working from home/Remote Working

Staff members who work from home and use their own home PCs to access the University's computer systems must ensure any personal data or other confidential business information remains secure at all times. The University's Home and mobile working guidance available on the Information Governance intranet pages, and the Bring Your Own Device policy must be complied with at all times. When working away from the campus, users who require access to organisational information must use Remote Access or UCLan-Global to access it unless this is not practically possible. This minimises the risk of theft or loss of information stored on removable media such as USB sticks. Any data associated with university business that needs to be stored on a laptop or removable media device

must be encrypted and stored no longer than necessary. Organisational information must always be stored in an appropriate network location and never on users' personal computers or devices.

Users must note that when using home PCs or other equipment at fixed locations outside the University, they are operating outside the University's IT security perimeter. In these situations, users must not assume their own PC equipment is protected by the same security measures as standard PC equipment routinely used at the University and directly managed by LIS. Users must be aware that weak security on home PCs used for home working could lead to University account passwords becoming known to unauthorised parties, which could lead to security incidents involving University IT systems. It is vital that PCs used for home working are themselves properly secured and it is the responsibility of users to ensure that is so (see list below). Users are responsible for safeguarding the equipment against unauthorised access, misuse, theft, or loss when in their home or in transit, for example on public transport or in their vehicle. Users are also responsible for ensuring that where the equipment is used by others (e.g. family members), no organisational information is accessible by such unauthorised parties.

Users must ensure that all reasonable protection measures are in place and operating where applicable, as follows: (LIS Customer Support are able to provide assistance and advice)

- The computer's local Firewall should be enabled
- Anti-virus software is set to automatically update itself
- Anti-spyware software to provide continuous protection against malicious software being downloaded
- Up to date security patches must be installed for both the operating system and applications when they are released by software vendors. Doing so will help protect the equipment against security vulnerabilities that have been identified.
- Wireless networks at home must be properly secured against eavesdropping and intrusion.

Users must comply with the security requirements of this document at all times and where personal data is being processed, they must also comply with the Data Protection Policy.

Users must not access internal or confidential/sensitive information over unsecured broadband or public wireless networks, including cyber cafes, as these present a security risk. Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

6.4 PHISHING, VISHING AND SPAM

Information security involves technical security measures but also requires users to ensure they act appropriately to maintain the security of computer systems and the corporate network. Attacks will be made on these systems and networks by unauthorised parties with the aim of obtaining organisational information or causing damage or disruption to that information or those systems by infecting them with viruses. Users must be aware of such attacks and be able to recognise them in order to stop them being successful. Attacks may involve phone calls from individuals trying to obtain confidential information by deception or may occur by email.

Users must ensure that organisational information is only disclosed by phone to callers who are authorised and entitled to receive that information. Further information can be found in the Data Protection Policy; this relates to personal data but can be applied to other organisational information as well.

Users must ensure that they do not click on links in spam or phishing emails or emails which appear to be such; attachments to such emails must not be opened. Users must never email their usernames and passwords in response to emails purporting to be from LIS; LIS staff will never ask for users'

passwords. Spam and phishing emails are becoming more and more sophisticated and plausible, if in any doubt, do not open the mail and delete it or contact LIS Customer Support on 01772 895355 for advice.

An increasingly common practice adopted by criminals attempting to gain access to passwords is by telephone call posing as a member of IT Support Staff. LIS Customer Support will never ask for your password. If you receive such a call **DO NOT** give your password, hang up and report it to LIS Customer Support on ext 5355, who will arrange for an IT Security investigation.

If users are in any doubt, they should contact LIS via LISCustomerSupport@uclan.ac.uk or 01772 895355 for advice.

6.5 CLOUD SERVICES

6.5.1 STAFF

Users must follow the University's Data Protection Policy and Information Categories when handling data. The only cloud storage service approved for the storage of non-Public categorised information is Microsoft OneDrive for Business, which is part of Office 365. A full security and compliance risk assessment has been undertaken of Microsoft's Online Services by UCLan.

Users of this service need to be aware of the following;

- UCLan has no direct control over the availability of this cloud service
- Responsibility for the availability, backup and recovery of the service lies with Microsoft.
- Deleted files can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost forever.
- Microsoft can and do carryout periodic updates and maintenance, which may result in a loss of service for that period.

It is recommended that important/critical documentation is kept on, or at least backed up to, the user's N: drive (home area) which is backed up daily by LIS, and in an emergency deleted files can be retrieved within hours.

6.5.2 STUDENTS

The only cloud storage service recommended by LIS is Microsoft's OneDrive for Business, which is part of Office 365. Other cloud providers are currently unable to provide assurances of where data would reside in the world, and with some (for example Dropbox) it is unclear who owned that data once it was on their servers.

Users of this service need to be aware of the following;

- UCLan has no direct control over the availability of this cloud service
- Responsibility for the availability, backup and recovery of the service lies with Microsoft.
- Deleted files can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost forever.
- Microsoft can and do carryout periodic updates and maintenance, which may result in a loss of service for that period.

It is recommended that important/critical documentation is kept on, or at least backed up to, the user's N: drive or home area which is backed up daily by LIS, and deleted files can in an emergency be retrieved within hours.

For further advice, contact LIS customer Support on ext. 5355 or by email at LISCustomerSupport@uclan.ac.uk

6.6 SECURITY BREACHES

All users must report all actual or suspected security breaches to the Information Security Team in LIS (LISCustomerSupport@uclan.ac.uk or ext. 5355) as soon as they become aware of it, whether they have caused the breach or they are informed of the breach by another party. LIS will ensure that any security breaches reported to them are acted upon promptly and will keep appropriate records and documentation, in line with the IT Security Incident Handling Guide. Corrective actions taken and other resolutions will be documented and monitored. In cases where an incident involves personal data, it must also be reported to the Information Governance Officer without delay, following which it will be managed and reported in line with the Information Governance Incident Procedure.

6.7 BACK-UP AND RECOVERY OF INFORMATION

All organisational information must be stored in a way which complies with the University's Information Categories, to ensure it is available for use, backed up and recoverable in the event of an incident. Users must not store organisational information on individual computers or devices unless exceptional circumstances apply, following advice from LIS and the Information Governance Officer (where personal data is involved). The system administrators cannot and do not back up files held off the network.

6.8 DESTRUCTION AND DISPOSAL OF EQUIPMENT

Any equipment or media used to store personal data or other organisational information must be disposed of securely, users should log a request with the LIS Customer Support team who will refer them to the relevant technician. No equipment or media containing or used to access organisational information must be disposed of or sent for resale without ensuring that all information has been removed and is irrecoverable. Any third parties who provide a destruction and disposal service under contract on behalf of the University must follow the agreed contractual procedures for removal of information. It must be noted that even though a third party may be contracted, the University is still ultimately responsible for the data and can be prosecuted should the Data Protection Act be breached.

6.9 ID CARDS AND ACCESS CONTROL CARDS

Lost or misplaced corporate identity cards present a security risk because the information they contain may, in some circumstances, allow an unauthorised user in possession of the card to gain access to live accounts. Consequently, it can also mean that in some cases, organisational information or other significant parts of computer systems are at risk. The loss of cards used for controlling access to buildings or secure rooms can potentially lead to a breach of physical security.

To guard against such events, if cards are lost or stolen, users must report its loss to the place of issue at the earliest opportunity but no later than 48 hours. If the card is used to access and administer university IT systems then the loss must be reported immediately to the LIS IT Security Manager. Administrators handling a report of a lost card must immediately disable the card and revoke any access privileges associated with it on the relevant systems. Users must follow relevant procedures for a replacement card to be issued.

When a lost card is found, the card must be handed in to the place indicated on it. The relevant user should be informed that the card has been found. If the loss has not already been reported, the user should also attend the relevant place for a new card to be issued. The lost card should never be returned to users; a new one must always be issued. The lost card must be disabled on the relevant systems for the reasons outlined above. To help protect the personal information held on such cards, the old card must be physically destroyed and not disposed of intact to ensure information contained in it is not accessible after it has been disposed of.

6.10 Social networking

Social networking services such as Facebook and Twitter are used for official University purposes as well as privately by employees in a personal capacity. Employees must not use their UCLan email addresses on their private social media accounts as this may compromise the security and privacy of the University's email system and the information it contains. The exception to this requirement is where accounts are used for interaction in genuine academic circles. For advice and assistance, contact LIS customer Support on extension 5355 or by email at LISCustomerSupport@uclan.ac.uk

6.11 Copyright

Copyrighted and licensed software must not be duplicated, removed or added by users unless it is explicitly stated that this is acceptable. Information about copyright is available to staff on the intranet. All copyright requirements must be complied with and declarations must be signed where appropriate.

The University's IT systems and network infrastructure, including wireless and Network-Lite must not be used for the downloading or streaming of copyrighted materials including but not limited to video and audio files, without the written consent of the owner or copyright-holder.

6.12 Wireless keyboards

Wireless (including Bluetooth) input devices are not approved for general use on the University network because they constitute a potential risk to information security. Wireless links offer little or no privacy and anyone within close proximity (30 metres) may monitor keystrokes and mouse movements. If there is a similarly-equipped PC within range it is possible that control of one PC may transfer to the other keyboard or mouse. On this basis, such equipment must not be used. If it is deemed not practical to use a keyboard connected with a cable, then only wireless keyboards using 128-bit encryption are approved. All other keyboards, including but not limited to unencrypted wireless keyboards and Bluetooth keyboards are prohibited.

Similar consideration should be given to the use of wireless input devices in the home environment. Individuals using such devices on personal PC equipment whilst remotely accessing corporate systems and/or information must be aware of the risks and take appropriate measures to protect against possible breaches of security.

6.13 Use of software

Copyrighted and licensed software may not be copied or distributed by users in contravention of the licensing agreement. Users are not permitted to trial software, for example from a removable disk on UCLan computers, and are not permitted to modify the operating system either manually or by downloading applications such as screensavers, themes etc.

Personal use of peer-to-peer networking and file sharing applications is not permitted on any of the University's systems. These applications use University resources for non-University purposes, they increase the risk of virus infection and spyware which compromise privacy and security and they involve legal risks regarding the storage of copyrighted material.

6.14 System planning

Proposals for new information systems or enhancements to existing information systems must be authorised by the Director of LIS or their nominee. This is subject to security risk assessments which must be made by suitably-qualified LIS staff.

Schools and Services must not contract digital services from external providers without the prior express permission of the Director of LIS or their nominee. Any external providers who have access

to UCLan's personal data will constitute a data processor under the Data Protection Act 1998, which means specific legal obligations must be met. See the Data Protection Policy for further information.

Project leaders and managers must ensure security (and data protection, where systems contain or are used to access personal data) is considered at all stages of projects relating to information systems. Data protection advice should be sought from the Information Governance Officer.

7 TECHNICAL - IT SECURITY POLICY FOR LIS STAFF AND SYSTEM ADMINISTRATORS

The information in this section of the policy is applicable to LIS staff and system administrators outside LIS. Responsibility for the security and integrity of the University data infrastructure lies with LIS or at certain formally-agreed locations, a party designated by it. This document and computer network security standards as implemented at the University must be complied with by all University computer systems.

All systems, except those designed for public open access, are required at their point of entry to have an auditable sign-on procedure with a unique, traceable identifier and password. All facilities remotely accessible must have approval from LIS. All external access will be audited to ensure traceability and responsibility and access and connection to selected wider networks will be restricted to authorised users only.

7.1 ACCESS CONTROLS

The computer system will have appropriate access controls. These controls will be defined for access to entire computer systems, specific data files, software applications, email and other resources. Access controls can be specific to individual users or to groups of users. Users will only be permitted access to those files and system resources they need to perform their job functions. In a computer system environment, considerations will include:

- Identification of the user to the computer system by Account Name and Password
- Access to *required* Files and Folders
- Account Restrictions
- Time Restrictions (set times of day between which the account may be used)
- Access to Databases and associated Applications Software
- Other Privileges

7.2 ACCESS CONTROLS ON USER ACCOUNTS

Individual users will each be given a personal account for which they are held responsible. Group accounts will be permitted where necessary for specific purposes but they will be suitably limited in function. By definition, a group account is used by more than one authorised person, which makes it harder to determine who performed any specific action. Users of any group account must understand their responsibilities for its security and only use it in the manner agreed. A group account may be withdrawn if, in the judgment of LIS, the account or the manner in which it is used is thought to present a security risk.

User accounts will be reviewed on a regular basis and any accounts that are no longer required will be removed. A user account will not be allowed more than one login session at a time except where absolutely necessary for specific work to be performed. Users will be given an appropriate restricted file store space for their work purposes. Users will be required to tidy this file store space on a regular basis by deleting files no longer current.

7.3 ACCESS TO FILES

User access to files will be granted according to individual or group need. By default, access will be denied unless it is shown to be required. Access to files containing confidential or sensitive information will be restricted. Only those users needing the information shall be given access to it.

7.4 ACCESS TO DATABASES AND THEIR ASSOCIATED APPLICATIONS

There will be access controls on databases and associated software in line with current best practice as recommended by the relevant software vendors. Third party support can obtain access to said systems through LIS Infrastructure Management who will manage a secure connection be that on site or over remote access. Access will be in office hours only. There will be occasions when out-of-hours access is required which must be agreed with LIS Infrastructure Management beforehand.

7.5 SYSTEM ADMINISTRATION

Sensitive system commands and software will be restricted to system administrators and security personnel. Accounts with enhanced file access rights or with high-level access to computer systems will be used only when necessary to perform tasks requiring such access. Excessive and unnecessary use will expose the computer system to increased risk of virus infection and damage to the file system and software.

7.6 PERMITTED USE

All users must be acquainted with and required to conform to current IT Facilities Rules as administered by LIS. These detail acceptable usage standards within the University. All users of IT facilities must adhere to the rules set out in this IT Security Policy and the Rules governing the use of the IT facilities and the Information Management Guide.

7.7 AUDIT CONSIDERATIONS

Computer logs are records of past events on a computer system. Logs can and are used to aid investigations into security incidents and misuse of the University's IT systems.

Types of information recorded in computer logs include (but are not limited to):

- The dates and times of account logins and logouts
- Internet use and email traffic
- The behaviour and health of the computer system itself.

Use of computer accounts and Internet usage will be logged and recorded in order to comply with our JANET contract. Software logs will be enabled as appropriate to comply with license conditions. Where appropriate, computer systems will always log user activity to provide an audit trail so that actions can be traced back to individual's e.g. When there is a case of suspected misuse. Attempts to breach security will be investigated immediately. If an attempted breach or an actual breach impacts on any corporate computer systems, staff discovering the problem must immediately notify LIS Customer Support. System administrators will regularly review computer logs to detect attempts to breach system security. Where checks of computer logs raise suspicions of attacks on the computer system, actual security breaches or other irregularities, system administrators will promptly investigate such concerns.

The corporate computer system will maintain correct time by automated reference to a nationally-recognised time source. All corporate systems will synchronise their clocks according to this time. The administrators of non-corporate systems will be responsible for ensuring the time on those systems remains consistent with the time on the corporate systems. LIS is registered with JANET for access to its NTP service and administrators should make use of this where possible.

The administrators of non-corporate systems will be responsible for retention of usage logs on those systems for periods prescribed by LIS in line with national best practice and legal guidelines.

7.8 BACK-UP AND RECOVERY

Back-up of server files will be automated and will be scheduled on a regular basis. The technologies for performing data back-ups and the schedules used must meet the business requirements of the University. Back-up media will be tested regularly to ensure the backup system and the media remain reliable.

Several generations of back-up files will be maintained. Back-up media will be stored in media safes, on and off-site. At least one back-up copy will be available on-site in case recovery is necessary and at least one other copy will be stored at an off-site location in case of a fire or some other contingency at the main site.

7.9 DISASTER PREVENTION

Disaster prevention is concerned with preventing a disaster from ever happening or at least minimising its effects if one does occur. The following precautions must be implemented by system administrators to mitigate disaster impact:

- Data back-up systems must be fully implemented, be tested regularly and be available for use if files need to be restored.
- The servers and networking equipment will be located in secure locked rooms to which access is restricted to authorised persons.
- Critical services will, where possible, be duplicated for resilience.
- Critical equipment must be covered by Uninterruptible Power Supplies to protect against power supply problems.
- Appropriate fire detection/prevention systems will be installed in the corporate computer rooms.
- University Security Personnel will respond to activations of intruder alarms and fire detection/prevention systems relating to the corporate computer room. Where appropriate the emergency services will automatically be notified of activations for the fastest response.

7.10 BUSINESS CONTINUITY PLANNING

A Business Contingency Plan has been formulated to ensure key personnel and resources are available to expedite recovery when a disaster does occur. The Business Contingency Plan covers all the essential and critical activities of the University. Key personnel will be made aware of the Business Continuity Plan, how it is to be executed and each understands their respective roles. The Business Continuity Plan is reviewed by the Business Continuity, Risk & Health and Safety Group and kept up-to-date with technical developments and the changing needs of the University and periodically tested to ensure the response options remain appropriate and adequate.

7.11 DOCUMENTATION

Computer system security controls must be adequately documented to allow for effective security and use of the network. LIS will prepare appropriate documentation for corporate systems. Administrators of non-corporate systems will prepare appropriate documentation for those systems.

7.12 MEDIA PROTECTION

Computer media will be stored and handled according to manufacturer's instructions. Media safes are available and should be used to store system back-up and vendor software on and off site as appropriate.

7.13 Network management/protection controls

7.13.1 Protection for the External Network Link

The external network link is managed by LIS to provide security, control and auditing of usage. Any computer systems using the external network link must have approval from LIS to do so. The administrators of such systems must ensure compliance with the security requirements of this document. Any broadband/ISDN access must not be connected to the main University networks but must connect through an LIS-managed or authorised firewall to avoid compromising security or must be completely standalone.

7.13.2 Firewalling for networks belonging to Schools and Services

All non-corporate networks belonging to schools and services must be authorised by LIS.

It is the responsibility of the individual school or service to ensure that its non- corporate network is not the source of any unsolicited intrusion (whether malicious or not) to the corporate network or the facilities of any other member of the JANET community.

Upon the reporting of suspicious activity by either Janet CSIRT or the non-corporate network administrator, LIS Infrastructure Management will provide assistance in identifying the source and taking appropriate action.

Failure on the part of the individual school or service to adequately police its non- corporate network will result in that network being immediately isolated by disconnection until such time as LIS is satisfied that there is no longer any risk. Each school or service with a non-corporate network must use the corporate, LIS-managed firewall to protect it from unsolicited external approaches.

7.13.3 User authorisation

The University will ensure that all computer system users are formally authorised to use the network and an audit trail of authorisation is maintained. Students are authorised through the enrolment process as being fee-paying students of the University. Staff are authorised by Human Resources and their line manager, with sensitive data access being specifically requested. External users are authorised by LIS and may be given access to computer systems where appropriate.

7.13.4 Hardware authorisation

LIS will maintain an inventory of authorised network equipment including network components, servers and workstations. Unauthorised hardware will be removed.

7.13.5 Controls on physical access to computer equipment

Physical access to the servers and related components will be limited to authorised personnel. The servers, back-up facilities, UPS, network hubs, etc. will be installed in locked areas which are only normally accessible to the computer system administrators and relevant technical support staff. Rooms used to house server and other sensitive system equipment will be kept locked and access to them restricted and monitored. Where workstations are located in public areas or areas that can be accessed by the public or students, consideration will be given to securing workstations and printers to desks and installing CCTV monitoring equipment.

7.13.6 Prohibition of non-standard hardware and software

All devices connected to the corporate network are to be standard hardware managed by LIS. Any non-standard hardware and software must be hosted on an existing non-corporate network behind firewall protection. Any exception to the above is by the prior express permission from the Director of LIS or nominee. This is subject to a security risk assessment which must be made by suitably-qualified LIS staff. The Director of LIS or nominee may refuse. Reasons for refusal are various, including but not limited to the following:

- In the judgment of LIS, the equipment might in any way interfere with, or be a risk to, the correct functioning of the corporate network or any approved systems.
- The equipment has inadequate protection against infection by malicious software.
- The equipment is not properly secured against unauthorised access and misuse.

7.13.7 Workstation client software protection

LIS will deploy security-related software patches and updates to the corporate computer systems following the guidance of the LIS system patching and update policies. The administrators of non-corporate systems will be responsible for the deployment of the relevant security related patches for those systems.

7.13.8 Protection of web-based services

Certain web-based services, for example access to University databases containing personal or confidential information, will have extra protection against eavesdropping on the Internet. SSL (Secure Sockets Layer) will be used to establish a secure connection between the client and server for transmission of information in encrypted form.

7.14 Risk analysis

Responsibility for conducting periodic risk analysis and security assessments will be formally assigned. The owner of the computer system is responsible for assigning responsibility for periodic risk analysis and security assessments of the computer systems. Risk analysis and security assessments will be conducted during the system design stages and at any other times when changes are made to the system design and/or components. Such analysis/assessments will measure the network's vulnerability to:

- Inadvertent error or improper disclosure of information
- Fraud or theft
- Financial loss
- Harm to individuals from infringement of privacy rights
- Loss of proprietary information and harm to organisational activity

7.15 Physical security

Physical security of the computer systems, including central servers and workstations, is a critical aspect of IT security. To maintain protection against intrusions, it is important that access to critical computer system components (such as the servers) is restricted to a small number of authorised individuals. Other considerations will include protection of equipment against theft, fire, and electrical hazards.

The corporate computer systems will be located in locked rooms to which access is restricted to authorised LIS staff. The corporate computer systems will have adequate backup power for critical components. Wiring closets housing network equipment will be kept locked at all times with access restricted to authorised LIS staff and approved third party companies e.g. data and electrical installers. Workstations in public access areas will be provided with appropriate physical security and be monitored by CCTV surveillance equipment where appropriate. Visitors to restricted areas should be supervised by authorised LIS staff. Security administration

Assigning administrative responsibilities for the computer system is absolutely necessary in order to maintain computer system security. Each system should have a lead person and a secondary. Assigning of administrative responsibilities must be approved by the lead person.

7.16 The System Administrator

The responsibility for the administration of the computer system, including security administration, will be assigned to knowledgeable individuals and authorised by the Head of LIS IT Systems. The administrator will be aware of their responsibilities regarding administration of the computer system as well as the security and integrity of the data and information stored and processed on the computer system. System administrators will be provided with the proper training, including training on security issues where required.

System administration external to the Computer Room will take place on secure workstations using secure IDs assigned to individual administrators as per the system administration rules. System administrators will be aware that operational shortcuts can lead to errors and reduce effectiveness of safeguards or even negate them. The University will maintain a representative on appropriate national and international security bodies (e.g. JANET Computer System Incident Response Team, CSIRT) to facilitate communication of current threats and countermeasures.

7.17 Server security considerations

System managers must consider the security of each individual server and types of server as part of the security of the computer system as a whole. All use of a server will be prohibited unless the user has entered a valid User ID and password. Web servers may be exceptions if they are required to be publicly visible but this will still depend on their exact purpose and content. Back-up systems will enable complete recovery of the entire server operating system, as well as data files in a timely manner.

Appropriate elements of hardware resilience (disk mirroring, server mirroring, load sharing on multiple servers) will be implemented for critical servers. A standard, secure build will be developed by LIS for each hardware/Operating System combination, and all will be built and maintained identically. All Operating System security patches will be applied in a timely manner and user-accessible servers shall have appropriate anti-virus protection operating continuously. Regular scheduled backups of the installed application software base will be taken to guard against file system corruption, damage, total loss and other contingencies.

7.18 User identification and authentication

User identification and authentication is the ability to identify the user of the computer system and to confirm the claimed identity of the users. The user identifies him or herself to the computer system by entering a User/Logon ID, usually consisting of his/her name. The user's identity is authenticated when the user enters a valid password.

7.19 User registration

The corporate computer system has user registration software for the creation of User IDs and allocation of resources to them. Users will be registered when proof of identity in the form of supporting documentation is provided according to user type.

- Staff – Letter from HR with proof of employment number
- Students – ID's generated automatically when students go through the enrolment process

7.20 User IDs

Each user will have one and only one user ID and the ID will be unique within the computer system. All user IDs will have expiry dates. Expired user IDs will have their access to computer systems suspended and deleted dependant on criteria according to user type. User types fall in to one of three categories: staff, student or external. The external category has an important subcategory of

'associate staff'. Staff accounts are expired at the end of employment and then deleted six months after the account expires. Student accounts are deleted when meeting all of the following criteria:

- The account has not been logged into for 12 months;
- The account is at least 12 months old; and
- The User who owns the account is not currently registered on the University's student records system.

External accounts are deleted 30 days after they expire. Accounts known as 'guest' accounts are merely external accounts with short lifetimes. Accounts known as 'associate staff' are external accounts with specific access rights granted to allow the authorised users, typically temporary staff or contractors, to perform their role functions.

7.21 PERIODIC CHANGES OF PASSWORD

Where technically possible, the computer system will require periodic changes of the user's password. Thirty days is the recommended password change interval. Where it is not technically possible to enforce periodic password changes, regular changes should be encouraged by user education. The user will be required by the computer system to choose a password different to the one previously used. Where technically possible, the user will not be able to use expired passwords as the new password when the system forces a password change. Authentication for critical services should include verification of token (e.g. SecureID) or biometrics. This is particularly important over remote access.

7.22 VIRUS PROTECTION

A virus infection may be, at a minimum, an annoyance to users of a personal computer; however in some instances, a virus may end up costing the user a lot of time through destruction of information or by preventing the user from being able to access the data stored on a hard drive. Increasingly likely is the possibility of a personal computer being infected but showing no outward sign. The compromised personal computer may behave in a way that impacts on its local network or may have effects on external sites by hijacking normal communication mechanisms for the virus' propagation or other unwelcome activities.

7.22.1 SYSTEM-WIDE EFFECTS OF VIRUS INFECTION

If an outbreak of virus infection is not well-contained there could be major disruption including:

- Denial of service due to network traffic congestion from infected computers. The congestion may reach the point where communication over the network is no longer viable, especially over slow links to remote sites.
- The possibility of re-infection. Without adequate protection in place, previously infected and cleaned computers may become re-infected from executing programs in the central file store which carry the virus.
- Implications for the System Administrator. The system administrator may unwittingly be a major source of infection due to possession of system level access to the computer system or even just extended access rights to its file store.
- Should the spread of infection extend far enough, effective loss of the entire file system may be the result. The computer system as a whole might be considered too badly compromised to be repaired.

7.22.2 PROTECTION MEASURES

Virus scanning and clean-up programs are installed on the system file servers and workstation clients. User files are scanned, on writing, to servers system wide to detect viruses. The workstation client ant-virus software is configured to scan on writing files to the local hard drive C:. Any other local

storage including secondary hard drives, floppy drives, CD/DVD drives and USB flash drives will be scanned on both reading and writing where technically possible.

The anti-virus software will be updated regularly in order that it may detect new viruses. Virus outbreaks will be monitored to determine if changed action is required as a result of a particular or new virus.

7.22.3 User awareness of virus issues

Users will be warned that virus scanners are not fool-proof and are largely reactive to new viruses, leaving a window of opportunity for new viruses before they are detected and incorporated in a scanner. Users will always be careful to verify the source of computer based information. If a file is discovered to be infected the onus is on the user to notify all sources and destinations of the file to prevent further spread (and maintain goodwill). Users must be particularly careful when distributing files, especially by email, to avoid spreading viruses. Unnecessary use of email attachments will be discouraged.

7.22.4 Responsibility for non-corporate University networks

The administrators of non-corporate systems will be responsible for anti-virus protection and scanning. In the event of non-corporate University networks becoming infected, LIS reserves the right to isolate such networks by disconnection if it is judged necessary to protect the corporate systems or external sites.

8 GLOSSARY OF TERMS

User	The individual who uses the computer systems
Computer systems	All campus networks, servers, workstations and network access devices
Organisational information	Information relating to the running of the University. This may be personal information about students, staff, external customers and contractors; information shared with the University by its business and research partners; or corporate information which is confidential or commercially sensitive.
Personal data	As defined by the Data Protection Act 1998: Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be an opinion (such as aspects of an employment reference). Information can be personal data without including a person's name. Personal data may also be referred to as 'personal information'.
Security incident/breach/violation	Any incident where the security of the computer system, corporate network or organisational information is compromised e.g. due to unauthorised access or disclosure.
Cloud services	Online storage areas hosted by commercial organisations external to UCLan where information can be stored and accessed via an individual user account e.g. Google Cloud.
Corporate network	Any and all infrastructure intended to support the corporate IT requirements.
Non-standard hardware and software	Any equipment which does not have an LIS-developed and maintained operating system. This is the case even if the equipment is funded by the Information Systems Panel.