University of Central Lancashire

IT Security Policy

Effective September 2017

-

August 2018

STUDENT REGULATIONS AND POLICIES

uclan.ac.uk/studentcontract

Contents

1 INTRODUCTION....3
2 SCOPE OF THE POLICY....3
3 POLICY STATEMENT....3
4 RESPONSIBILITIES....3
5 RELATIONSHIPS TO OTHER POLICIES....4
6 GENERAL – IT SECURITY POLICY FOR ALL STUDENTS....6
6.1 PERMITTED USE....6
6.2 USER AUTHORISATION....6
6.3 USER ACCOUNTS AND PASSWORDS....6
6.4 ID CARDS AND ACCESS CONTROL CARDS....7
6.5 KEEPING INFORMATION SECURE....7
6.6 PHISHING, VISHING AND SPAM....7
6.7 BACK-UP AND RECOVERY OF INFORMATION....8
6.8 CLOUD SERVICES....8
6.9 SOCIAL NETWORKING....9
6.10 WORKING FROM HOME/REMOTE WORKING....9
6.11 COPYRIGHT....10
6.12 USE OF SOFTWARE....10
7 NETWORK MONITORING....10
7.1 AUDITING....10
7.2 SECURITY BREACHES....10
8 GLOSSARY OF TERMS....11

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.

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 Rules for the use of IT facilities and Wireless Network Fair Usage and Security Policy which is available on the Student Support pages of the University website.

All internally and approved externally hosted systems must conform to this policy. The University reserves the right to isolate any IT system including externally hosted service or networks, which represents a potential or actual breach of security; to monitor information sent over its networks; and to deny user access to the universities, approved 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, guests in Office 365 and 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 the Learning and Information Services department (LIS). Any questions or concerns about the operation of this policy should be referred in the first instance to the LIS Customer Support Team:

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. The

University will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

5 RELATIONSHIPS TO OTHER 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 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 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 PERMITTED USE

All users of IT facilities must adhere to the rules set out in this IT Security Policy. Users are also required to conform to the current Rules for the use of IT facilities and Wireless Network Fair Usage policies.

6.2 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. Guest access for Microsoft's Office 365 Groups is authorised and the responsibility of the Office 365 Group owner.

6.3 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.

Passwords must not be shared, 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.

6.4 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. The reported lost card will immediately be disable. 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 will 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 will never be returned to users; a new one will always be issued. To help protect the personal information held on such cards, the old card must be physically destroyed to ensure information contained in it is not accessible after it has been disposed of.

6.5 Keeping information secure

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.

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. Encrypted information 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.

6.6 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.

6.7 Back-up and recovery of information

Students are advised to use their allocated Home Area (N:\) for storing of files as Home area drives are backed up daily by LIS systems. 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 LIS system administrators cannot and do not back up files held away from the University network.

6.8 Cloud services

Users must follow the University's Data Protection Policy when handling data. The only cloud storage service approved for the storage of non-Public categorised information is Microsoft Office 365 Services. This includes but not limited to;

- Microsoft OneDrive for Business
- Microsoft Exchange Online
- Microsoft SharePoint Online

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 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

6.9 Social networking

Students should 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

6.10 Working from home/Remote Working

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.

6.11 COPYRIGHT

Copyrighted and licensed software must not be duplicated, removed or added by users unless it is explicitly stated that this is acceptable.

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 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.

7 NETWORK MONITORING

7.1 AUDITING

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. System administrators 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.

7.2 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.

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 University.