IT Services Policy

University of East London

Information Security Policy

1 Introduction

Information is a vital asset to any organisation, and this is especially so in a knowledge-driven one such as the University of East London (UEL) where information relates to learning and teaching, research, administration and management. This policy is concerned with the management and security of the University's Information and the use made of this Information by its members and others who may legitimately process University information. The policy must be read and understood by all users of UEL IT Systems.

The Data Protection Policy and the Information Security Policy (ISP) are the overarching documents of UEL's Information Security and Information Assurance Frameworks. The ISP is intended to provide an overview of Information Security best practice. It should be read in conjunction with the Frameworks' other policies and guidance, some of which fall outside the scope of IT Services.

This and other Information Security Policies will be subject to an annual review and update, or in response to any significant changes that may impact the overall security posture of the University. Such changes will be announced to all users via the Intranet, direct communications or both. As usual, supporting information will be provided when users are required to use a new feature or change behaviour.

2 Purpose

The purpose of this policy is:

- To provide guidance to university staff, students and other users as to the controls and support that are available to ensure information and the applications used by the University remain secure.
- To protect the University's IT assets and services against unauthorised access, intrusion, disruption or other damage.
- To ensure the confidentiality, integrity and availability of Information used within the University is maintained.
- To ensure compliance with applicable legislation and regulations, allowing the University to meet security standards, including Cyber Essentials (the National Cyber Security Centre backed security certification for organisations) and Payment Card Industry – Data Security Standards Compliance (PCI-DSS).
- To protect personal information and intellectual property owned by the University, its staff and students from loss, exposure or corruption.

3 Scope

This policy applies to anyone using UEL IT facilities (hardware, software, data, network access, third party provided services, and other online services) provided or arranged by the University of East London. It also applies to all information created, received or retained as a result of University business, which must be protected according to its sensitivity, criticality and value, regardless of the media or location the data is stored or accessed from. Guidance on sensitivity marking and information handling can be found in the University of East London: Data Classification Policy**.**

4 Policy Statement

This policy is in place to reduce the risk of Information Security events that impact the ability of the University's staff, students and other users to carry out their legitimate activities. Awareness of what to do and what not to do, to minimise those risks, is also valuable in helping all our users be more aware of the Information Security threats they face in their personal lives.

5 Responsibilities

Director of IT: Has ultimate accountability for implementing Information Security at UEL.

Head of IT Security: Is responsible for ensuring that all information and information systems which are of value to UEL are adequately protected against adverse effects of Information Security breaches.

Heads of Schools and Services: Are required to implement this policy and are responsible for ensuring that staff, students and other authorised persons comply with associated policies.

Individual users of UEL IT equipment/services: Are responsible for adhering to this and any associated policies alongside having a duty to report any breaches of this policy, information security threats or known vulnerabilities.

To assist in the understanding and usefulness of this policy, this document is broken down into three responsibility areas; those of the users of the UEL IT Systems, those of both the users and providers of UEL IT Systems and those of the providers of UEL IT Systems.

5.1 User Responsibilities

5.1.1 Handling Sensitive Information

Users of UEL IT services will handle a variety of information and some of it will be sensitive. Information may well be marked with its security classification, but this may not always be the case. See University of East London: Data Classification Policy for definitions. In such circumstances the information should be considered as Sensitive, and handled appropriately if it contains;

- Personal Information (PI) or Personally Identifiable Information (PII), including names, addresses, performance observations;

- Sensitive Personal Information (SPI), including health records, political associations, sexuality, criminal records;

- Potentially valuable Commercial information, such as research, business plans;
- Card Holder or bank details for individuals or organisations;
- User account credentials, including your own (your user Identity and password);
- Configuration details of the University's information Systems.

Staff who process Payment Card Data must read and be familiar with the Payment Card Data Protection Policy.

5.1.2 Conduct

Users of UEL IT services are expected to follow reasonable conduct and this is outlined in the **Acceptable Use Policy**. Key aspects of the expected conduct are:

- You must not use UEL IT equipment to cause unwarranted offense or distress to others or perform actions that would be in breach of legislation including but not limited to the Computer Misuse Act (1990), the Data Protection Act (2018), the Regulation of Investigatory Powers Act (2000) or UEL's Data Protection Policy.
- You must not send spam (unsolicited bulk email).
- You must not produce material or electronic communications that brings the university into disrepute, causes offence or otherwise damages the university's reputation. This includes the use of Social Media, both UEL official accounts and your personal account.
- You must not create, download, view, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Any such activity may constitute a criminal or civil offence and will be reported to the authorities accordingly.

5.1.3 Disciplinary Action

Violation of the standards, policies and procedures presented in this and associated documents by an employee or student may result in disciplinary action, from warnings or reprimands up to and including termination of employment or being removed from a course. Claims of ignorance, good intentions or using poor judgment will not be acceptable as excuses for non-compliance.

5.2 User and UEL's Join Responsibilities

5.2.1 Access to Sensitive Data

UEL has introduced access control mechanisms to protect sensitive data. These provide both physical and logical controls. For both, UEL provides the minimal access required for users to perform their duties and to protect sensitive data from unauthorised access. For these controls to be effective, users must follow the advice contained in this and associated policies, in particular, the Acceptable Use Policy and Payment Card Data

Protection Policy – owned by Finance (in production), where appropriate to their role and the Account Provisioning Policy.

5.2.2 Data Loss Prevention

UEL applies Data Loss Prevention (DLP) controls. The objective of these is to reduce the risk of accidental or deliberate exposure, compromise or loss of UEL data assets and is an aspect of UEL's efforts to meet Information Security obligations under DPA 2018 and GDPR. Further enhancements are being carried out through 2020.

These controls apply to the exposure or leaking of the more sensitive information held by UEL, including PI and SPI. These controls are or will be applied to such services as email, SharePoint and Teams.

The changes being introduced will result in users being notified that an action they have taken or attempted has been detected as a potential breach of DLP controls. In these cases, the user may be asked to justify their actions, for example when sending an email which contains PI or SPI to an external recipient. Communications will be issued before these changes are made so that users are aware of the DLP controls and how to deal with them.

- Staff and Students must be careful that they do not expose personal Information beyond the UEL network, or to internal users without a right to see it. This can occur accidentally through forwarding an email to an external recipient or by making a SharePoint or Teams file or folder widely available by making it 'public'.

- Auto Forward of UEL mailboxes is not allowed. This can result in sensitive information leaving the network. For this reason, Auto Forward of emails will be removed when detected.

Monitoring of these activities is already in place with notices being sent to the Information Assurance and IT Security Teams.

5.2.3 Physical Security

The Physical Access Control Policy describes the controls in place and responsibility of staff, students and visitors in meeting the policy. In general:

- Staff and students should observe physical security controls, not allow "tailgating" through access-controlled doors and barriers;

- Wear their UEL passes at all times while on campus and/or present it virtually when requested to do so by University staff;

- Visitors must always be escorted by a trusted employee when in areas that hold sensitive (including cardholder) information and equipment;

- Procedures must be in place to help all personnel easily distinguish between employees, students and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees, other personnel such as partners and examiners, and consultants who are "resident" at UEL sites. A "visitor" is defined as a vendor, guest of an

employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day;

- Employees need to follow UEL's **Clear Desk policy** to prevent physical media and paperwork being exposed to unauthorised access and loss.

5.2.4 Protection of Data in Transit

Where sensitive data is to be transmitted, it must be protected using strong encryption. There are particular requirements for payment card data and these are to be identified in the Payment Card Data Protection Policy (in production). Please refer to the Data Classification Policy for handling advice for the 4 categories of data: Public, Internal, Confidential and Strictly Confidential.

5.2.5 Disposal of Stored Data

All data must be securely disposed of when no longer required, regardless of the media or application type on which it is stored.

Where on-line material has been marked for deletion by a user or process, it must be permanently deleted at that point or after a set retention period.

Data stored on media must be securely destroyed via an approved and certificated destruction process.
Hard copies of data must be securely destroyed via Shredding. Note that hard copies of payment card data must be destroyed by cross-cut shredding to specific dimensions. They must not be placed in confidential waste bins to be shredded by a third party if this is executed out of sight of UEL staff responsible for the protection of the data. See the Payment Card Data Protection Policy for more details, when available.

5.2.6 Security Awareness and Procedures

All users must be aware of this policy and those listed below to ensure Information Security is maintained at the University. To support awareness of policy, procedures and guidance, supporting material is available on the IT Services intranet page. All staff are required to complete the mandatory IT Security training programme (course) prior to passing probation and are subject to completing the IT security yearly refresher training.

5.2.7 System and Password Policy

Password strength will be assessed by Microsoft when a new network password is created. Any password deemed too weak or common will be rejected and the user asked to submit an alternative.

For staff and student IT accounts the password must:

- Be at least 8 characters, Admin accounts are set to be longer.

- Include at least 3 of these 4 character types -Upper and lower alpha, numeric and special characters (symbols and punctuation).

- Not include a single dictionary word or 'common' passwords.
- Not include all or part of your username or obvious link to you, such as a pet or relatives name.
- Be unique to your UEL account and not used by you for any personal accounts.
- Be changed promptly after the user or UEL knows or suspects an account has been compromised.
- Not be disclosed to anyone, including IT staff. This includes you never disclosing MFA codes.
- Not be written down so that they may be available to others.
  Note. Passwords may be held in an IT Services approved password management tool.
- An account will be locked out after 6 unsuccessful attempts for a day, it can be reset using the Self-Service Password Reset (SSPR) service but enrolment in SSPR is required prior to this, click here to be taken to the SSPR.
- Multi Factor Authentication (MFA) is in place for all Staff accounts when off site, this has been introduced when on site too for staff tech accounts.
- MFA has been introduced for all student accounts, except for specific managed exceptions.

During the COVID-19 Pandemic and UK lockdown, the need for all staff and students to work remotely has been supported by a temporary suspension of the need to reset password every 90 days. This suspension has been reviewed and password ageing is being re-introduced.

5.2.8 Anti-Virus Policy

All UEL build devices will be configured with Malware protection. UEL also incorporates email and web filtering to reduce the risks of users allowing viruses to affect their devices.

Users are not able to alter the Anti-Virus software settings, which are designed to provide:

- Protection that is kept up to date by at least daily updates.
- Scanning of files upon access and automatically scanning external media upon inserting into a UEL device.
- Web sites are scanned before allowing access in addition links included in emails are verified to be safe, those which are not are listed as suspect by internet providers and/or security services.

For PCI-DSS compliance logs from the Anti-Virus product must be maintained online for 3 months and archived to maintain a 12 month record.

Bring Your Own Device (BYOD): Where a non-UEL device is used for work purposes, it is the user's responsibility to ensure that the same level of AV protection is provided on their device.

It is not permissible to use a non-UEL owned and managed device while working on certain activities and projects. This currently includes devices used to handle **card payments or** for the **Babcock/MPS** project.

5.2.9 Patch Management Policy

All software used on devices and the network must be licensed and supported by the vendor. When no longer supported, software must be removed.

Wherever possible all systems software must have automated updates enabled for systems patches released by the vendor.
Software and OS patches must be applied within 14 days where the product vendor describes the patch as fixing a vulnerability rated as “critical” or “high risk”. Where not marked “critical” or “high risk”, all security patches must be applied within a month of release.

When using their own devices, users take on the responsibility identified in this section. If they are unable to meet these patch management requirements, they must not use their own device for UEL activities.

UEL operates change freezes during critical business periods and where IT resources are limited. During these freezes patches and updates to OS and application software to address critical and high risk security issues will still be applied to the above schedules, unless there is good evidence that to do so would introduce a greater risk to service continuity or security than from the security risk being addressed.

5.2.10 Use of Privileged Account

When using an account with higher privileges, such as a technical account or domain admin account, you as a user need to be additionally wary of the risks associated with the higher privileges should you be lured by an attacker. You must avoid using email and browsing with these accounts, unless you are engaging with a recognised supplier, or performing a task that requires access to Azure for example. Cyber Essentials requires that higher privilege accounts do NOT have access to email or the internet. It is therefore necessary to use such services to the bare minimum.

5.2.11 Administration Access to a Device

UEL provided laptop, tablets and desktop computers will allow user access to the functions of the device, but without the user having administrative privileges on the device. It will be possible for a user to be granted admin privileges to their device, but only for a specific purpose, for example the installation of approved software. The admin privileges will be revoked after a set period. Requests are currently made via a TOPdesk ticket raised by the user. The process has been amended so that the user needs to provide a reason for the need for admin privileges and to identify how long the escalation is required, which will be limited to a week at most.

There will be allowed exceptions to this policy, for example where technicians in schools have responsibilities to manage the devices used in labs by those schools and where lecturers require the ability to install software related to coursework.

All devices currently issued with administrative privileges are to be reviewed and brought in line with the above stated policy.

5.2.12 Secure Application Development

Software used by UEL for business purposes must be approved for use by IT Services. All products used for business purposes must be provided by recognised and approved providers with attention to Information Security included in requirements and product specifications. Evidence of Secure Application Development must be available as part of the Software Development Lifecycle (SDLC).

5.3 User and UEL's Join Responsibilities

5.3.1 Remote Access Policy

Remote access for staff and students must be secured so as not to introduce new security risks.

Remote access is secured with Multi Factor Authentication (MFA) for all off site access. MFA is achieved mainly using a PIN sent by text to a previously registered device or using the Microsoft authenticator app. All admin accounts use MFA for UEL on site access too.

Any remote access for staff, students, contractors, vendors and agents must be removed when no longer required. This will be carried out by IT Services staff disabling or removing accounts and disabling any remote access solutions provided. In some cases, this may require notification to third parties such as Microsoft and AWS for Cloud Service Partners no longer engaged.

5.3.2 Vulnerability Scanning and Management Policy

UEL IT Services will run regular internal and external scans of the network using recognised tools. These tools will identify the risk ranking using industry standards.

PCI-DSS specific requirements will be met and will be described in the Payment Card Data Protection Policy, when available.

UEL will run scans on all new server and user device builds, so as to provide assurance of the build security before use, as well as regular scans into the network to detect vulnerabilities, including those believed to have been remediated following previous scans.

5.3.3 Configuration Standards

UEL IT Services will manage the University network to meet specific standards;

- Devices used to transmit network traffic will be configured to meet specific standards. These standards will be held in documentation which is subject to regular review and update.
- Network devices will be configured to meet these standards before deployment to the network.
- Where possible automated configuration management tools will be used to ensure consistent configuration is achieved.

5.3.4 Change Control Process

UEL IT Services run a Change Management system. The Change Management process is documented in the Change Management Policy. The process ensures that all changes are documented, assessed, authorised and tested before formally executed in the live environment.
A weekly CAB (Change Advisory Board) meeting is undertaken within IT Services to ensure all system changes scheduled meet the above stated process requirements and, on that basis, either approved or rejected to proceed. CAB requests and approvals are stored within IT Services Teams site.

5.3.5 Audit and Log Review and Monitoring

UEL reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic within its domain for any purpose. See the University of East London: Monitoring Policy for more details.

Logs of user activity, including logging in/out, access to applications and Office 365 services are kept and archived. These logs are held to meet regulatory and compliance requirements but are subject to retention schedules and deletion as part of required housekeeping.

5.3.6 Penetration Testing

UEL will arrange penetration testing of our systems to a schedule required for compliance with security standards necessary for PCI-DSS and Cyber Essentials (the National Cyber Security Centre backed security certification for organisations). This will be arranged with third party providers and will be executed so as not to cause capacity or availability issues for UEL services.

5.3.7 Security Incident Response Plan

As part of its Major Incident response plan, UEL has developed a Security Incident Response Plan, this is supported by a number of process documents designed to ensure a standard approach to dealing with specific security events.

More detail on the responsibility for reporting incidents relating to Payment Card Data will be held in the Payment Card Data Protection policy.

5.3.8 Security Incident Response Plan

All accounts providing access to UEL information systems are managed through defined processes and in line with the Account Provisioning Policy. These processes cover activities for Joiners, Leavers and Movers as well as in-life reviews of access. They cover Staff, Contractors, Researchers, Hourly Paid Lecturers. Students are also covered.

The basic principles applied include:

- Formal processes are in place for all user types, access cannot be provided until initial verification and vetting (where required) are completed.

- Each user is granted a unique User Identify and must have a Password meeting complexity rules.

- Each account grants the least privileges required for a user to execute their responsibilities.
- Additional access privileges are subject to formal request and implementation.

- The segregation of duties is applied to reduce the risk of misuse and fraud.

- Group or shared accounts are not allowed other than for tightly managed exceptions which must be agreed by the Head of IT Security.

- Service accounts are allowed for specific Information System functions.

- All remote access will be subject to Multi Factor Authentication.

- Those with higher privileges and technical accounts are subject to MFA when on site.

- Currently, a VPN is required for remote access to specific 'high risk' applications when off site.

All users are expected to be familiar with the Information Security Policy and related policies, enabling them to follow appropriate on-line behaviour.

5.3.9 Wireless Policy

UEL operates wireless networks for staff and students. These are segregated to protect UEL information. UEL also offers EDUROAM access, allowing access from other educational establishments back into UEL's Network.

For PCI-DSS compliance, those who are handling Payment Card Transactions must NOT use the UEL internal Wi-Fi service to process payments.

6 Other Relevant Policies

a) University of East London: Acceptable Use Policy
b) University of East London: Account Provisioning Policy
c) University of East London: Cloud Services Policy
d) University of East London: Data Classification Policy
e) University of East London: Data Protection Policy
f) University of East London: Data Retention Policy
g) University of East London: Social Media Policy
h) JANET: Acceptable Use Policy
i) JANET: IT Security Policy

7 Reporting

Any actual or suspected breach of this policy should be reported to IT Services immediately upon discovery. Any device in breach of this policy can be brought to IT Services who will rebuild the device to ensure compliance with the policy.

8 Failure to Comply

Failure to comply with this policy, or its subsidiary regulations, may result in withdrawal of access to University ICT Systems and may result in disciplinary action.

We appreciate your cooperation in complying with University policy and the Law and helping to keep your device, our network and services, as well as those of our partners and third-party suppliers, safe and secure. If you are in any doubt, please contact the **IT Services Service Desk** or the IT Security team at infosec@uel.ac.uk

Policy ID:	Information Security
DOC VERSION NO:	Version 3.1
DOC VERSION DATE:	January 2021
DOC AUTHOR:	Jake McMahon, Tim Moore
APPROVED BY:	Amanda Niblett
APPROVED DATE:	08/01/2021
REVIEW DATE	19/11/2021