UNIVERSITY OF WEST LONDON

Information Security Policy (including Acceptable Use Policy)

(Accessible Version)

Responsibility of: IT Services
Approval Date: October 2021
Review Date: October 2022
Approved By: IT Steering Group

For Everyone

1. Introduction

1.1. This Information Security and Acceptable Use Policy sets out what you must and what you must not) do in order to:

- Protect both your and the University's information from unauthorized people accessing, changing, or deleting it.
- Ensure that the equipment, services, systems and networks made available to students and staff to support them in their studies and research, and to administer the functions of the University, are used in a way that is acceptable, safe, and appropriate.
- Everyone should read and follow both this and the Data Protection Policy. If you have questions about either policy, contact IT Services for help – see below.

1.2. This policy is for Students, Staff, Managers, and System Owners.

1.3. If you have questions about this policy, or wish to report a security concern, call the IT Service Desk on 0300 111 4895. They are available 24 hours a day, 7 days a week.

2. Responsibilities for Information Security

2.1. We are all responsible for Information Security, for Data Protection, and for using University provided services and equipment responsibly.

2.2. Some people and groups in the University have additional responsibilities set out below:

- The Vice-Chancellor's Executive (VCE) has the ultimate accountability for implementing information security at UWL and owns the overall risk management process, including the prioritisation and acceptance of risks. This policy has the full support of VCE and all students and staff are expected to follow it.
- Heads of Schools and Central Service departments have responsibility for managing risks within their authority (or escalating) and operating in line with the expectations of VCE.
- Governance bodies like the Audit & Risk Committee of the Board of Governors (ARC), the Information Governance Group (IGG), the IT Steering Group (ISG) and IT Consultative Group (ICG), along with the Internal Audit programme, help identify risks to the University and provide advice to the Vice Chancellor's Executive.
- System Owners are responsible for ensuring that Information Security and Data Protection are baked into the systems they own by design and default.
- Managers of UWL staff are responsible for ensuring the data their teams work with and are responsible for is protected.
- The Information Security Manager leads the Information Security function with the support of the Chief Information Officer and colleagues in the IT Services team.

3. Reporting a security concern

3.1. All students and staff are responsible for promptly reporting any concern they have about Information Security.

3.2. Students should report concerns to the IT Service desk, their personal tutor, the Information Security Manager, or Student Services.

3.3. Staff should report concerns to the IT Service desk, their line manager, or the Information Security Manager.

3.4. To report a security concern, call the IT Service Desk on 0300 111 4895. They are available 24 hours a day, 7 days a week.

3.5. In you suspect there may have been a Personal Data Breach (see below) then you must follow the University Data Breach Reporting Process and report your concerns immediately to the Information Security Manager or Data Protection Officer. There are legal requirements for the University to respond very promptly to suspected Personal data Breaches.

3.6. Personal data is any data that is about a living person who can be identified. A personal data breach is any security incident where there is a risk that an unauthorized person accessed, changed, or destroyed personal data.

4. Infringement

4.1. UWL will investigate complaints received from both internal and external sources about any infringement of this or related policies. In support of this process a technical investigation may take place. UWL may choose not to investigate anonymous or verbal complaints.

4.2. If UWL believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency. If UWL believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

4.3. The involvement of external authorities will not prevent UWL from taking appropriate action in accordance with the university's regulatory framework.

4.4. All students must adhere to this policy. Serious breaches of this policy may be a breach of the student code of conduct and lead to disciplinary procedures

4.5. All staff must adhere to this policy. Any breaches may lead to disciplinary action. Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal.

For Students

5. Dos and don’ts for students

5.1. Do use a strong password: 3 random words in mixed case separated with punctuation

5.2. Do change your password if you think it is compromised, and at least once a year.

5.3. Do back up your important data e.g. to UWL OneDrive and a USB disk.

5.4. Do tell someone (personal tutor, IT Service Desk) if you have any security concerns.

5.5. Do check your email regularly for security advice and alerts from IT Services

5.6. Do watch out for phishing -online scammers pretending to be someone else

5.7. Do be considerate of fellow students and staff when using IT systems and equipment.

5.8. Do read and follow this policy (and the data protection policy).

5.9. Don’t tell anyone your password or write it down where someone could see it.

5.10. Don’t leave a UWL open access PC unattended while you are logged onto it.

5.11. Don’t get content from “dodgy” sources – they’re full of malware and other nasties.

5.12. Don’t waste resources, for example by printing unnecessarily or sending bulk emails.

5.13. Don’t attempt to bypass security systems, for example by turning off antivirus.

5.14. Don’t unplug, modify, move or remove any University equipment.

5.15. Don’t try to access, modify, or delete anyone else’s data without their permission.

5.16. Don’t assume Information Security is an “IT thing” – we all have a vital part to play.

5.17. If in doubt, contact IT Services

- Telephone 0300 111 4895
- Telephone 222 from any University phone
- Email ITServiceDesk@uwl.ac.uk

6. Personal activity, equipment, & services (students)

6.1. We recommend you do not use UWL services or equipment for personal use. Keeping University and personal activities and data separate will improve your work/life balance and is more secure.

6.2. But if you do, you must:

- Follow all University rules, regulations and policies, as well as the law.
- Keep personal use reasonable and to a minimum.

- Always give priority to University work.

6.3. And you must not:

- Expose the University to information security risks or excessive costs.
- Use UWL services or equipment for commercial or for-profit activities, or to compete with University business.

6.4. UWL does not accept any liability for damage or loss of any nature caused by the use of UWL services or equipment for personal activity. This exclusion does not apply where personal injury or death is caused by the university's negligence.

6.5. You may want to use your own personal devices for your University work. This includes mobile phones, tablets, and desktop and laptop computers.

6.6. If you do, you must:

- Protect your devices with a password, 6-digit PIN code, or biometrics.
- Run up-to-date and supported versions of your operating system and applications – turn automatic updates on.
- Use an antivirus product – both Windows 10 and Mac OSX have anti-virus built in.

6.7. But also, you must not:

- Plug any personal device into the UWL network – use Eduroam wireless instead.
- IT Services will help you get your personal devices connected.

6.8. UWL reserves the right to inspect personally owned devices that connect to our systems to ensure they are secure, and to deny access if they are not. This may require installation of a local device management agent. Users unhappy with this should not use their personal devices for UWL activity.

7. Prohibited Activities (students)

7.1. All students must follow the rules below at all times:

7.2. Do not access, create, download, store or transmit anything which is indecent, offensive, defamatory, or extremist.

7.3. Do not access, create, download, store or transmit anything which is discriminatory or encourages discrimination on the basis of racial or ethnic grounds, or on grounds of gender, age, sexual orientation, marital status, disability, political or religious beliefs.

7.4. Do not do anything that is illegal or with the intent to defraud.

7.5. Do not do anything with the intent to cause harm, annoyance, inconvenience, distress, or needless anxiety.

7.6. Do not do anything with the intent to disrupt or damage the work or data of other users or attempt to access or modify that data without their permission.

7.7. Do not jeopardise the integrity or security of UWL services, networks or equipment, for example by deliberately or recklessly introducing malware,

setting up or using unapproved servers, services, equipment or software, moving or reconfiguring existing UWL equipment, services, and networks, or trying to bypass any security systems or controls.

7.8. Do not infringe copyright or break license agreements.

7.9. Do not violate the policies of third-party services the University provides, such as Eduroam or Microsoft 365.

7.10. Do not do anything that unnecessarily takes up capacity or resources. That includes excessive emailing, unsolicited commercial or advertising emails, using excessive bandwidth, or wasting paper or electricity.

7.11. Do not use UWL services, networks or equipment for personal gain, or in a way which competes with the University's business.

7.12. Do not use UWL services, networks or equipment in a way that conflicts with your obligations to the university or with University rules, regulations, policies or procedures.

8. Passwords (students)

8.1. Your UWL network password is very important. It gives you access to services and equipment and protects your data throughout your time at the University. You are responsible for everything done using your UWL network account.

8.2. You must choose a good strong password.

8.3. You must keep it confidential at all times.

8.4. You must change your password:

- if you receive a temporary password from IT
- at least once a year
- immediately if you think someone might know it.

8.5. You must not tell anyone – even IT Services – your password.

8.6. You must not write your password down where someone else could see it. (you can store it in a secure password manager app).

9. Choosing a good password (students)

9.1. The easiest way to choose a good, strong password that is easy to remember is to pick three random words, using a mixture of upper and lower case, separated with a punctuation mark. For example: Horse-Battery-Staple.

9.2. Your password must:

- Be at least 10 characters long.
- Contain both upper and lower case letters.
- Contain at least one number or punctuation mark.
- Be entirely random.
- Have no connection to you or the University.
- Not be based on a single dictionary word.
- Not be used anywhere else.

10. Your data (students)

10.1. During your time at UWL you will create a lot of data. Keep it safe by regularly backing it up to your UWL OneDrive as well as copying to a USB disk or stick.

10.2. You retain all the ownership, copyright, and intellectual property rights of data you create with and store in university equipment and systems.

10.3. UWL monitors university networks, equipment and services:

- in order to detect, investigate, and resolve security incidents and system failures.
- in order to investigate alleged misconduct, misuse of facilities, breaches of policy and regulation, and risks of harm to staff or students.
- in order to comply with our statutory PREVENT duty to prevent people being drawn into terrorism.

10.4. Any data you store in UWL services will only be accessed by UWL for these purposes and with proper approval. UWL is acting as a data processor for such data.

10.5. UWL will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating, or preventing crime and ensuring national security.

10.6. You must not attempt to monitor or scan UWL networks, equipment or services yourself. If cyber security is the subject of your teaching or research, special arrangements will be made.

10.7. When you finish or defer your studies and leave UWL, your accounts will be automatically disabled after a grace period, and your data only kept for a short period after that, so it is important to make copies of anything you need to keep beforehand.

11. Web filtering

11.1. UWL strongly support the principles of academic freedom. We want our students to be able to use the web freely as part of their studies.

11.2. However, the university has responsibilities under the PREVENT duty, to safeguard children, and to protect UWL systems and data from harm and cyber-attack.

11.3. UWL blocks access to known malicious sites to protect the university from malware, phishing, crypto-jacking, and other forms of cyber-attack.

11.4. Apart from this, Higher Education (HE) students have unrestricted access to the web using UWL networks.

11.5. Further Education (FE) students may be under 18, so their web access is restricted using category-based filters.

11.6. Younger students, such as those attending Junior college, are not given UWL network accounts and so cannot access the web using the UWL network.

11.7. Remember that you must not use the web for anything on the list of prohibited activities, whether your access is blocked or not.

11.8. If you need access to a blocked site for your studies or research, ask your lecturer to contact the Information Security Manager to discuss.

11.9. Use of filtering in UWL is reviewed by the PREVENT committee on an annual basis.

For Staff

12. Dos and don’ts for staff

12.1. Do use a strong password: 3 random words in mixed case separated with punctuation.

12.2. Do change your password if you think it is compromised, and at least every six months.

12.3. Do back up your important data e.g. to UWL OneDrive and a USB disk.

12.4. Do tell someone (line manager, IT Service Desk) if you have any security concerns.

12.5. Do check your email regularly for security advice and alerts from IT Services.

12.6. Do watch out for phishing -online scammers pretending to be someone else.

12.7. Do be considerate of students and fellow staff when using IT systems and equipment.

12.8. Do read and follow this policy (and the data protection policy).

12.9. Don’t tell anyone your password or write it down where someone could see it.

12.10. Don’t leave your computer unattended while you are logged onto it.

12.11. Don’t get content from “dodgy” sources – they’re full of malware and other nasties.

12.12. Don’t waste resources, for example by printing unnecessarily.

12.13. Don’t attempt to bypass security systems, for example by turning off antivirus.

12.14. Don’t unplug, modify, move or remove any University equipment.

12.15. Don’t share personal data without taking a moment to “STOP, THINK, ASK”.

12.16. Don’t assume Information Security is an “IT thing” – we all have a vital part to play.

12.17. If in doubt, contact IT Services

- Telephone 0300 111 4895
- Telephone 222 from any University phone
- Email ITServiceDesk@uwl.ac.uk

13. Personal activity, equipment, & services (staff)

13.1. We recommend you do not use UWL services or equipment for personal use. Keeping University and personal activities and data separate will improve your work/life balance and is more secure.

13.2. But if you do, you must:

- Follow all University rules, regulations and policies, as well as the law.
- Keep personal use reasonable and to a minimum
- Always give priority to University work

13.3. And you must not:

- Expose the University to information security risks or excessive costs.
- Use UWL services or equipment for commercial or for-profit activities, or to compete with University business

13.4. UWL does not accept any liability for damage or loss of any nature caused by the use of UWL services or equipment for personal activity. This exclusion does not apply where personal injury or death is caused by the university's negligence.

13.5. You may want to use your own personal devices for work. This includes mobile phones, tablets, desktop and laptop computers.

13.6. If you do, you must:

- Protect your devices with a password, 6-digit PIN code, or biometrics
- Run up-to-date and supported versions of your operating system and applications – turn automatic updates on.
- Use antivirus – both Windows 10 and Mac OSX have anti-virus built in.

13.7. But also you must not:

- Plug any personal device into the UWL network – use Eduroam wireless instead.
- Use personal cloud services such as email, file storage, or video calling for UWL business.
- Store UWL data on a personal device.

13.8. UWL reserves the right to inspect personally owned devices that connect to our systems to ensure they are secure, and to deny access if they are not. This may require installation of a local device management agent. Users unhappy with this should not use their personal devices for UWL activity.

14. Prohibited Activities

14.1. All staff must follow the rules below at all times

14.2. Do not access, create, download, store or transmit anything which is indecent, offensive, defamatory, or extremist.

14.3. Do not access, create, download, store or transmit anything which is discriminatory or encourages discrimination on the basis of racial or ethnic grounds, or on grounds of gender, age, sexual orientation, marital status, disability, political or religious beliefs.

14.4. Do not do anything that is illegal or with the intent to defraud.

14.5. Do not do anything with the intent to cause harm, annoyance, inconvenience, distress, or needless anxiety.

14.6. Do not do anything with the intent to disrupt or damage the work or data of other users or attempt to access or modify that data without their permission.

14.7. Do not jeopardise the integrity or security of UWL services, networks or equipment, for example by deliberately or recklessly introducing malware, setting up or using unapproved servers, services, equipment or software,

moving or reconfiguring existing UWL equipment, services, and networks, or trying to bypass any security systems or controls.

14.8. Do not infringe copyright or break license agreements.

14.9. Do not violate the policies of third-party services the University provides, such as Eduroam or Microsoft 365.

14.10. Do not do anything that unnecessarily takes up capacity or resources. That includes excessive emailing, unsolicited commercial or advertising emails, using excessive bandwidth, or wasting paper or electricity.

14.11. Do not use UWL services, networks or equipment for personal gain, or in a way which competes with the University's business.

14.12. Do not use UWL services, networks or equipment in a way that conflicts with your obligations to the University or with University rules, regulations, policies or procedures.

15. Passwords (staff)

15.1. Your UWL network password is very important. It gives you access to services and equipment and protects your data throughout your time at the University. You are responsible for everything done using your UWL network account.

15.2. You must choose a good strong password.

15.3. You must keep it confidential at all times.

15.4. You must change your password:

- if you receive a temporary password from IT
- at least once every six months
- immediately if you think someone might know it

15.5. You must not tell anyone – even IT Services – your password.

15.6. You must not write your password down where someone else could see it. (You can store it in a secure password manager app).

16. Choosing a good password (staff)

16.1. The easiest way to choose a good, strong password that is easy to remember is to pick three random words, using a mixture of upper and lower case, separated with a punctuation mark. For example: Horse-Battery-Staple.

16.2. Your password must:

- Be at least 10 characters long
- Contain both upper and lower case letters
- Contain at least one number or punctuation mark
- Be entirely random
- Have no connection to you or the University
- Not be based on a single dictionary word
- Not be used anywhere else

17. Monitoring and data access

17.1. UWL monitors University networks, equipment and services:

- In order to detect, investigate, and resolve security incidents and system failures.
- In order to investigate alleged misconduct, misuse of facilities, breaches of policy and regulation, and risks of harm to staff or students.
- In order to comply with our statutory PREVENT duty to prevent people being drawn into terrorism.

17.2. Data accessed for one of the reasons above will be done by authorised persons only, and always in line with the Data Protection Policy and all relevant legislation. You must not attempt to monitor networks, equipment or services yourself without the explicit authorization of the Associate Pro Vice-Chancellor and Chief Information Officer.

17.3. Besides the monitoring described above, data stored in areas assigned to an individual staff member, such as their OneDrive or email inbox, will normally only be accessed with the staff members permission or with the authorisation of the University Secretary and Chief Compliance Officer or, in her absence, a nominated VCE colleague. In an emergency – for example if there is clear and immediate risk of harm to a student or staff member – authorization may be given by any member of VCE.

17.4. UWL will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating, or preventing crime and ensuring national security. If you receive such a request, direct it to the University Secretary and Chief Compliance Officer.

18. Mobile and remote working

18.1. As a UWL staff member you may be issued with a mobile device, such as a laptop, tablet, mobile phone, or portable storage device, allowing you to work off campus. Non-mobile devices such as desktop computers must only be taken off campus with the asset owner's permission.

18.2. Great care must be taken with such devices. In particular, the storage of confidential or personal data on such devices should be avoided as far as possible. When connecting devices to untrusted networks, such as public Wi-Fi, all UWL data MUST be encrypted in transit.

18.3. Portable storage devices must only be used when online storage services such as OneDrive or SharePoint cannot be used. They must be strongly encrypted and must never hold the only copy of any university data.

18.4. Mobile computing devices must have at least a 6-digit PIN or strong password set and should have full disk encryption enabled where possible.

18.5. Such devices must not be left unattended in public spaces or in open areas of the campus, even briefly. They must not be kept in full view in a vehicle, even for a short period of time, and must never be left in the vehicle overnight. When travelling by aeroplane, subject to airline regulations and applicable legislation, devices must be carried in the cabin and not checked in.

18.6. If a mobile device issued to you is stolen or lost you must notify the police, your line manager, and the IT Service Desk immediately.

18.7. When a mobile device is no longer required, or upon termination of the contract on the basis of which the device was issued, the device must without exception be returned to the line manager or asset owner.

19. Recording meetings

19.1. Online meetings should normally not be recorded unless there is a specific necessary purpose and approval has been given by the responsible Head of School, College, or Service.

19.2. The Chair or organiser must advise attendees in advance, and again at the beginning of the meeting, if it will be recorded.

19.3. Covert recordings must not be made – doing so may be a disciplinary offense.

19.4. If a recording is made to assist with the taking of notes or minutes – which should not be routine practice – it does not replace the formal record of the meeting.

19.5. Recordings should not be made to be shared with those who could not attend. A formal minute or oral update should be provided instead.

19.6. Meeting recordings by their nature are personal data. Retention periods of no more than 4 weeks must be set and a legal basis for processing must be determined.

19.7. They must be made with, stored securely in, and shared using UWL systems only. Sharing meetings should be exceptional and restricted only to specific people who need access.

19.8. Staff video training should normally be done as a standalone video rather than by recoding a live training session. Never use real or live personal data for training purposes.

19.9. See the UWL Lecture Capture Policy for recording of teaching.

19.10. See the UWL CCTV policy for the recording of video for the safety of students and staff.

20. Handling confidential material

20.1. In the course of your work at UWL, you may have need to handle confidential material. For example, commercially valuable information, personal data about students or colleagues, or sensitive information that must be restricted to only those staff who need to know it.

20.2. Be very careful when handling such material and always be sure to:

- Stop before you handle confidential material
- Think about how you will keep it safe
- Ask if you are unsure

20.3. Always put confidential papers in a drawer and either lock or log off your PC, even if only leaving your desk unattended for a moment. On Windows 10 PCs, press the Windows+L key combination to immediately lock your screen.

20.4. Always be aware of your surroundings when accessing or discussing sensitive, confidential, or personal information. Who can see your screen? Who can overhear your conversation?

20.5. Always remove confidential material from printers, scanners and copiers as soon as you are finished.

20.6. Always use encryption to protect confidential material when required.

20.7. Always dispose of confidential information safely when it is no longer needed, following the UWL records retention schedule. Secure waste bins are available in staff offices for the safe disposal of paper records. Contact IT Services for help with the secure deletion of confidential files.

20.8. Never leave confidential material visible at your workspace when you are not present.

20.9. Never access confidential material for any personal or unauthorized purpose.

20.10. Never allow students access to the Student Record system.

21. Local administrator access

21.1. Very exceptionally, it is sometimes necessary for a staff member to have local administrator access to their UWL issued computer.

21.2. Local administrator rights are a significant risk to the security of the University's infrastructure and must be handled with great care. It is essential that their password is strong, secure and unique, and if possible, local administrator rights should only be assigned temporarily to allow a staff member to carry out a specific task.

21.3. Requests for local administrator access rights must be made in writing. They must include a detailed justification and be approved by the staff members Dean of College, Head of School, or Head of Central Service Department, as well as by IT Services.

21.4. If you are granted local administrator rights, then you are responsible for ensuring you do nothing to compromise the security of the UWL network and IT infrastructure. In particular:

- You must not remove or modify UWL provided anti-malware and security software
- You must not remove or modify features which permit IT Services to manage or monitor devices
- You must not make changes to network configuration settings

21.5. IT Services will revoke local admin rights if necessary to protect the security of the UWL network and infrastructure.

For managers

22. Manager responsibilities

22.1. As a manager, you have additional responsibilities around Information Security.

22.2. You must identify the data and processes you are responsible for and accept accountability for their protection.

22.3. You must assess relevant business, legal, contractual, and corporate social responsibility risks to the activities of you and your team, ensure appropriate controls are in place to manage these risks, and regularly test these controls. Background verification checks on candidates and employees, as established by HR, must consider the sensitivity of the information they will access during their work, and the perceived risks of such access.

22.4. You must ensure you and your team understand fully your responsibilities regarding protecting systems and data, and have the skills needed to fulfil these responsibilities. These responsibilities must be part of employment contracts, including responsibilities that remain after termination or change of function.

22.5. You must actively, regularly and demonstrably verify what your reports are doing and how systems under their supervision are functioning (with the assistance of IT Services where appropriate).

22.6. When a member of your team leaves the University or changes their role, you must ensure that

- Any non-standard permissions or accesses that they had in their old role are removed
- Any data that your team needs to keep has been copied from their OneDrive, email, and computer.

23. Third parties and contractors

23.1. If, as a manager, you make use of third parties or contractors for a particular function, you must ensure that:

- The contractual arrangements with them set out their (and their organization's) responsibilities for information security and data protection, including responsibilities that extend beyond the end of the contract.
- Background verification checks, as established by HR, explicitly consider the sensitivity of information to be accessed and the perceived risks from such access.
- They meet all specified requirements for information security and data protection, both on selection and on an ongoing basis.
- They understand and accept their responsibility for their actions in these areas.
- Where a third party uses contractors or sub-contractors of their own, that they are also made aware of and accept their responsibilities in these areas.

23.2. If it is necessary to give third parties access to UWL systems, services, equipment or networks, then this must only be granted after

23.3. Suitable confidentiality and accountability clauses are included in the contract

- A due diligence risk assessment has been performed
- IT Services have approved the access
- IT Services have reviewed and approved the technical means by which it is delivered.

23.4. Where remote access is required to UWL systems in order to provide support, each individual access must require explicit authorization from a UWL staff member.

For system owners

24. System owner responsibilities

24.1. If you are the owner of a UWL data processing system, you are responsible for, and accountable for, that data's protection from harm.

24.2. That means:

- Ensuring that the system meets the requirements of this policy and the Data Protection Policy.
- Ensuring Information Security and Data Protection are built into the design throughout the lifecycle of the system.
- Ensuring that appropriate technical and organisational measures are in place to keep the system secure.
- Ensuring appropriate incident response and business continuity plans, aligned to the UWL Incident Management and Business Continuity Framework are in place for the system, and regularly reviewed and tested.
- Ensuring accounts - both regular and privileged - are managed properly and decommissioned when that user no longer has need of them.
- Ensuring the system complies with all legal and contractual requirements, such as the UK GDPR and PECR.
- Ensuring that systems and data are protected from damage, retained no longer than required, and securely disposed of when no longer needed.
- Co-operating with and supporting internal audit functions.

25. Security by design and default

25.1. When developing a new system, process, or service, information security and data protection are a requirement from the beginning. While much of the work may be delegated to IT Services or a vendor, the responsibility for defining security requirements and ensuring the system is protected remains with the system owner.

25.2. Systems must be designed so that:

- Users can only access the data and functionality they have been authorised for. (The "least privilege" approach)
- Accountability for usage is maintained by audit trails.
- Availability is addressed through suitable high availability, business continuity, and disaster recovery arrangements.
- Regular security testing and review is part of the business-as-usual operation of the system.

25.3. Each new service requires consideration of the unique risks it presents and the determination of necessary controls.

25.4. Systems must adopt the principle of defense in depth by having multiple resilient and redundant security controls in place that will continue to protect data even if one control fails or is bypassed.

25.5. Systems should never rely solely on perimeter or network defenses, such as the UWL network firewalls, for security.

25.6. The default or vendor recommended configuration of a system should be subject to review.

25.7. There should be separate development, test, and production environments for all business-critical applications, and attention should be given to the protection not just of live data but also test data and approved source/object code.

26. Web-based services

26.1. UWL has adopted a “cloud first” approach to new IT systems, so frequently a new service will be accessed via a web front end, accessible from the public internet.

26.2. Before deploying a new web service, systems owners must gain the approval of key stakeholders (such as IT Services and Marketing) and ensure that:

- Data protection legislation is complied with, and this has been recorded (via Form D or a DPIA as appropriate)
- The service meets the Public Sector Bodies Accessibility Regulations.
- The service meets the ICO’s age-appropriate Design Code.
- The service meets PCI/DSS requirements if required.
- Published content is licensed
- Content moderation is in place where user generated content is published.
- Due consideration has been taken of the impact of the web service on UWL’s reputation, branding, and Search Engine Optimization (SEO).

27. Managing User accounts

27.1. A user account is a set of credentials and associated data that allows a specific person to log in to one or more UWL services. The account is used both to authenticate the person (confirm who they are) and to authorise them (confirm what services and data they should have access to).

27.2. Access to systems should only be granted on a “need to know” basis, with users having the minimum access required to perform their work.

27.3. Systems should be designed so that all activity on the system can be linked to an identified individual’s account.

27.4. System owners need to ensure they have documented processes for approving and managing the creation, change, emergency suspension and deletion/decommissioning of accounts, and a mechanism for regularly auditing this process to confirm it is working.

27.5. All accounts in a system must be secured with a password or comparable authentication method.

27.6. Password strength rules should be implemented, requiring:

- Passwords be at least 10 characters long
- Passwords contain a mixture of at least three of upper-case letters, lower case letters, numbers, and special characters such as punctuation marks.
- Passwords do not contain the users name or username, or other common weak passwords.

27.7. Multi-factor authentication (MFA) should be enabled if available

28. Managing privileged accounts

28.1. A privileged account is one which has additional permissions above and beyond what is provided to a “normal” account on the system. By their nature they are higher risk and must be protected accordingly. All privileged access to systems must be traceable to an individual, and if technically possible, logged in a way that prevents the privileged account altering it.

28.2. Privileged accounts must never be used to perform tasks that a non-privileged account can do. if one staff member needs to perform both privileged and non-privileged then they should either have multiple accounts assigned, or if supported by the system use an account that is normally running without privilege but can be temporarily elevated when required.

28.3. Individuals with privileged accounts have been placed in a position of trust and must follow all applicable laws, regulations, policies, and procedures.

28.4. As with all accounts, there must be documented processes for approving and managing the creation, change, emergency suspension and deletion of privileged accounts, and a mechanism for regularly auditing this process to confirm it is working. Approval for a privileged accounts creation must be given by the system owner.

28.5. Systems are often supplied with pre-defined, generic privileged accounts, such as "admin", “superuser” or "root”. If possible, these should be disabled and separate privileged accounts, assigned to named administrators, used instead. Where these accounts must be kept active, their password must be immediately changed from the default, and if possible, the username should also be changed. If any member of staff who knows that password leaves, it must be immediately changed and recirculated.

29. Licensing and Patch Management

29.1. All software used in UWL (including free or open-source software) MUST be correctly licensed, supported (by either the vendor or a third party) and have security patches applied in a timely manner.

29.2. Patches whose severity is rated by the vendor as CRITICAL or HIGH MUST be installed within 14 days of release. Other patches MUST be installed within 28 days of release.

29.3. Where a vendor does not indicate severity with a CRITICAL-HIGH-MEDIUM-LOW ranking, reference may be made to the Common Vulnerability Scoring System (CVSS); but otherwise, such patches will be treated as CRITICAL.

29.4. If there is a business critical need to continue to run unsupported software, mitigating controls, such as network segmentation, MUST be put in place and documented in order to ensure that the University is not exposed to unacceptable risk.