IT and Cyber Security

UPR IM20 Appendix II version 02.0

Policies superseded by this document

This document replaces version 01.0 of UPR IM20 Appendix II, with effect from 3 January 2023.

Summary of significant changes to the previous version

Minor amendments have been made for clarification purposes and to reflect changes in organisational structures.

Glossary

A glossary of approved University terminology can be found in **UPR GV08**.

Table of contents

1 IT and Cyber Security

1.1 This appendix to UPR IM20, IT and Computing Regulations, must be read in conjunction with the whole UPR and its other appendices. The substantive UPR lays out the regulations for general users of IT systems – the appendices determine the regulations under which these systems will be managed and operate.

1.2 All notifications to the Chief Information and Digital Officer required under these regulations should be made through the Helpdesk.

1.3 The University's IT systems will be configured, monitored and managed in accordance and compliance with the UK HM Government Cyber Security Essentials Scheme:

https://www.cyberessentials.ncsc.gov.uk/advice/

1.4 The Chief Information and Digital Officer may, in exceptional circumstances, deny an individual access/usage to University IT facilities. Such cases must be reported by the Chief Information and Digital Officer to the Vice-Chancellor.

2 Computer Network Performance and Security

2.1 Internal computer network connections

2.1.1 All connections to the University's computer networks must conform to the protocols defined by the Chief Information and Digital Officer (or nominee) and with the requirements that apply to IP addresses. Abuses of, or failure to comply with, these requirements will result in immediate disconnection from the network and the withdrawal of the individual's user privileges. Such instances will be reported by the Chief Information and Digital Officer to the Vice-Chancellor.

2.1.2 All cabling installations must be in accordance with the standards agreed by the Chief Information and Digital Officer and the installation work must be approved by the Department of Estates, Hospitality and Contract Services. Requests for the installation of cabling must be made using the appropriate University request procedure.

2.1.3 Only staff authorised by the Chief Information and Digital Officer are permitted to install and maintain active network equipment including hubs, switches, routers, line-of-sight and wireless network units connected to the University's network. The specification of any equipment must be agreed by the Chief Information and Digital Officer.

2.1.4 'Public access' equipment may only be connected to the student network.

2.1.5 Equipment connected to the staff network, located outside of the University Data Centres, will not be set up to offer services to other users (for example, to act as servers) unless the prior written consent of the Chief Information and Digital Officer (or nominee) has been obtained. This consent will normally exclude all external access.

2.1.6 Equipment connected to the staff network must be located in 'staff only' areas. For the purposes of this document, a 'staff only' area is defined either as an area which students may not enter or, exceptionally, an area which students may not enter unless they are accompanied at all times by a member of staff or unless they are research students authorised by the Chief Information and Digital Officer to use that area.

2.1.7 Authorised use of IT equipment connected to the staff network is restricted to those Members of the University in Membership B (see UPR GV06[2]) and Postgraduate Research students who share research facilities with staff, and who must have entered into an appropriate confidentiality agreement with the University and formally agreed to comply with the University's policies and regulations.

2.1.8 The staff network is linked to the student network by a 'firewall'. This 'firewall' permits access from the staff network to the services and systems, including the internet, connected to the student network. The Chief Information and Digital Officer will establish appropriate mechanisms for monitoring the 'firewall'.

2.1.9 Equipment will be connected either to the staff network or to the student network, but never to both.

2.2 External data communications

2.2.1 All external data communications will be conducted through the University's Janet connection, or other approved links.

2.2.2 No other external network connections, including use of ISDN lines, on premises owned, managed or occupied by the University or its wholly-owned subsidiary companies, may be made without the prior written consent of the Chief Information and Digital Officer (or nominee).

2.2.3 Off-campus access over the internet and on-campus wireless network access to the University's networked services is available for Members of the University via the University's secure access service (VPN). These routes provide authenticated access to designated information systems and services using the individual member's normal University username and password. Approved suppliers for whom off-campus access has been identified as essential by the appropriate Head of Strategic Business Unit and notified in writing to the Chief Information and Digital Officer (or nominee), will also be granted access.

2.3 Boundary firewalls and internet gateways

2.3.1 The default administrative password for any firewall (or equivalent network device) should be changed to an alternative, strong password.

2.3.2 Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall) should be subject to approval by an authorised individual and documented (including an explanation of business need).

2.3.3 Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), should be disabled (blocked) at the boundary firewall by default.

2.3.4 Firewall rules that are no longer required (e.g. because a service is no longer required) should be removed or disabled in a timely manner.

2.3.5 The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.

2.3.6 In situations where the administrative interface needs to be accessible from the internet (e.g. because it is supported by a remote administrator or external service provider) the interface should be protected by additional security arrangements, which include using a strong password, encrypting the connection (e.g. using SSL), restricting access to a limited number of authorised individuals, and ultimately 2-factor authentication for the most sensitive data and only enabling the administrative interface for the period it is required.

2.4 Domain Name Services and Internet Protocol (IP) addresses

2.4.1 All Domain Name Services (DNS) activity will be managed and monitored centrally, for the whole University, by the Chief Information and Digital Officer (or nominee).

2.4.2 The Chief Information and Digital Officer is responsible for all University IP address range applications, and for the management, allocation and use of IP addresses.

2.4.3 All equipment connected to the University's computer networks must be assigned a unique IP address from within the University's official range of IP addresses. IP addresses must not be re-assigned to other items of equipment without the prior written consent of the Chief Information and Digital Officer (or nominee).

2.4.4 Members of staff must notify the Chief Information and Digital Officer of cases where an IP address is no longer required.

2.5 Additional or changed equipment

2.5.1 The Chief Information and Digital Officer (or nominee) must be advised, in advance and at the earliest opportunity, of any plan to add items of equipment to or to replace or to re-locate equipment that is connected or may require connection to the University's computer network, or of any plan involving a new use, a change of use or addition to the University's computer networks that might impact on the performance or security of the computer networks, such as wireless networks, video conferencing, the use of networked multimedia applications and document imaging systems.

2.5.2 The Chief Information and Digital Officer (or nominee) will assess the likely impact on the University's computer networks of the proposed change. The Chief Information and Digital Officer (or nominee) will give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change MIGHT cause.

2.5.3 All new or changed uses of the computer networks must be approved by the Chief Information and Digital Officer (or nominee).

2.5.4 Prior to their installation in the 'live' situation, major network developments should be 'soak-tested' in off-line simulation.

2.5.5 For up to two (**2**) months after the live installation of the new development, the network provision that it is to replace should, wherever possible, remain in place as a 'fall-back' in the event of any subsequent failure of the new development when it is subject to actual user demand.

2.6 Computer network provision in new and refurbished buildings

2.6.1 Network provision for new and refurbished buildings will normally be in accordance with the specification ('the standard specification') published from time-to-time by the Chief Information and Digital Officer.

2.6.2 The standard specification will be reviewed annually by the Chief Information and Digital Officer.

2.6.3 Where the network requirements of a specialist area or activity need a network provision that exceeds the standard specification, the Head of Strategic Business Unit concerned will advise the Chief Information and Digital Officer and the appropriate Project Manager of these requirements at the earliest opportunity.

2.6.4 The Project Manager will seek advice from the Chief Information and Digital Officer (or nominee) concerning the technical use and cost implications of the proposal. This information will form part of any submission, by the Project Manager, for additional funding to meet the costs of the enhanced network provision that is required.

3 Security of Data Centres, Communications Rooms and Cabinets

3.1 Access to Computer Network Equipment and Data Centres

3.1.1 All data centres, communications rooms and cabinets will be kept locked at all times.

3.1.2 Other than in an emergency, access to data centres, communications rooms, cabinets and their contents and computer network equipment is restricted to persons authorised by the Chief Information and Digital Officer (or nominee). All other entry and interference with computer network equipment is strictly prohibited.

3.1.3 In the event of fire or other emergency, Security Staff and/or staff of the Department of Estates, Hospitality and Contract Services and/or the emergency services and/or agreed University contractors, may enter a Data Centre or Communications Room without prior permission, to deal with the incident. The Chief Information and Digital Officer (or nominee) must be notified of such entry as soon as reasonably possible.

3.1.4 For regular authorised access to Data Centres, a person must complete a Data Centre Access Request Form and obtain an authorised access card from the Chief Information and Digital Officer (or nominee).

3.1.5 All persons granted authorised access to Data Centres must undertake the required training and comply fully with Data Centre security requirements and all relevant University policies and regulations.

3.1.6 Access control standards must be established for all Data Centres which minimise security risks yet allows the University's business processes to be carried out without undue hindrance. Procedures for managing the registration and de-registration of the authorisation of persons requiring access to Data Centres locations will be established to ensure that all users access privileges match their authorisations. Authorisations and access privileges will be reviewed at regular intervals. The Chief Information and Digital Officer will identify the authorised officers to manage and implement these procedures.

3.1.7 Where a University post has designated specific Data Centre responsibilities, this will be made clear in the Job Description and staff appointed to such posts must receive an appropriate briefing and training as part of their induction.

3.1.8 Where computer network equipment is housed in accommodation used for another purpose, the arrangements for access by another user of that accommodation will require the prior written consent of the Chief Information and Digital Officer (or nominee). This consent will specifically exclude access by the other user to any communications cabinets or computer network or systems equipment located in the shared accommodation.

3.2 Contractors and visitors

3.2.1 All contractors requiring regular and agreed access to Data Centres must follow the requirements of 3.1 above and sign in and out of the Data Centre on each occasion.

3.2.2 Contractors undertaking equipment maintenance, computer network services and information systems work must have obtained the prior approval of the Chief Information and Digital Officer (or nominee) and must also have obtained the appropriate authorisation and the necessary Contractors' badge in accordance with the procedures established by the Director of Estates, Hospitality and Contract Services and the requirements of the University's security regulations and procedures (see UPR HS05[1]).

3.2.3 Contractors who fail to comply with these requirements may be challenged and may be asked to leave University premises if they are unable to produce a valid badge and the necessary authorisation.

3.2.4 Contractors must be advised of their obligation to observe any specific access conditions which apply within the areas in which they will be working.

3.2.5 Other contractors and visitors requiring ad hoc access to Data Centres must be escorted at all times by an authorised person nominated by the Chief Information and Digital Officer (or nominee); comply with the provisions of this University policy and regulation and comply with any specific instructions given by the authorised person during the course of their visit to the Data Centre

3.2.6 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University's Data Centre or Communications Room environment must agree to comply with the Data Centre and Communications Room Security arrangements set out in this document and with all other relevant University policies and regulations.

3.3 Compliance

3.3.1 Data Centre and Communications Room management processes must enable the University to comply with its legal, statutory and contractual obligations and any national agreements that it has entered into.

3.3.2 Data Centres must be safeguarded appropriately, especially when left unattended. Controls will be established to ensure the safety and security of the Data Centre environment.

3.3.3 It is the responsibility of each individual working within a Data Centre or Communications Room to ensure compliance with agreed good Health and Safety practices. To limit their exposure to personal Health and Safety risks, Members of the University working within Data Centre environments will comply with the following Code of Practice:

---

[1] UPR HS05 'Security and Public Access'

a no food or drink may be brought into University Data Centres;

b packaging and/or waste materials must never be left inside;

c furniture must not be brought into any Data Centre without the express permission of the Infrastructure Development Manager, and must be fire resistant;

d aisles and exit routes must not be obstructed;

e cabinet keys must not be left in the racks (a key safe is provided for storage);

f power extension cables must never be used;

g the correct equipment for the job, for example, tile lifters or stepladders must always be used;

h the door to the Data Centre must never be propped open;

i no one must be allowed to 'tail-gate' behind another person entering a Data Centre legitimately.

3.3.4 The risk to human life associated with the fire suppression system must be fully understood and training undertaken in the emergency evacuation of the Data Centre.

3.3.5 All authorised persons with access to Data Centres are required to participate in annual refresher training in the safe and secure use of Data Centres. Access to Data Centres may be revoked where authorised users fail to undertake the required refresher training.

3.3.6 All authorised persons with access to Data Centres must comply with health and safety requirements for lone working, working in confined spaces, electrical safety and hazardous chemicals.

3.3.7 Any contracts with facilities management or outsourcing companies must have incorporated within them agreed service levels consistent with the regulations set out in this document so that Data Centre and Communications Room security and compliance issues are addressed.

3.4 Operations

3.4.1 To ensure on-going compliance with Data Centre security requirements, changes to operating procedures will require the prior written approval of Chief Information and Digital Officer (or nominee).

3.4.2 The specification of any equipment to be installed in a Data Centre or Communications Room and the arrangements for the installation of that equipment must have the prior written consent of the Chief Information and Digital Officer (or nominee).

3.4.3 Acceptance criteria for new information systems, upgrades and new versions will include reference to the sustainability of those systems within the University's Data Centres.

3.4.4. The Chief Information and Digital Officer (or nominee) will:

i determine and disseminate procedures for the reporting of incidents, security breaches and potential security weaknesses in the University's Data Centres;

ii implement monitoring arrangements to inform Data Centre management;

iii determine and disseminate procedures for the reporting of Data Centre equipment malfunctions and faults;

iv require that all faults and malfunctions are logged and monitored and that corrective action is taken in a timely manner.

3.4.5 The Infrastructure Development Manager must be informed of all breaches of Data Centre security through regular reporting channels and in emergencies. The Infrastructure Development Manager must report major breaches immediately to the Chief Information and Digital Officer.

3.5 Planning and Changes

3.5.1 Changes to equipment supporting critical business systems must be planned in advance to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment will be correctly maintained.

3.5.2 The implementation of new systems or related projects must be agreed by the Chief Information and Digital Officer (or nominee) prior to installation into the Data Centre.

3.5.3 Equipment supporting critical business systems will be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

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

4 Information Security

4.1 Development and support of information security processes

4.1.1 This policy should be read in conjunction with the University's Data Management Policy (UPR IM16[2]) and its appendices.

[2] UPR IM16 'Data Management Policy'

4.1.2 It is the policy of the University to implement processes to protect the security and confidentiality of its management and administrative information. These processes will:

i identify who may be permitted to access the University's management and administrative information;

ii stipulate the extent to which these individuals may be permitted to manipulate the University's management and administrative information;

iii make clear the obligation placed on authorised workers to maintain security and confidentiality;

iv specify the arrangements for the release of information;

v establish mechanisms to secure management and administrative information against loss, damage, corruption or unauthorised access or use.

4.1.3 The University will address security issues during the purchase and implementation of all new management and administrative information systems. All management and administrative information systems purchased or implemented by the University will, therefore, be capable of compliance with these regulations.

4.1.4 Heads of Strategic Business Units will develop and maintain local management and administrative information security policies which are consistent with this policy for those areas for which they are responsible. They will ensure that members of staff receive training on information security policies that may apply and any amendments that may be made to these subsequently.

4.1.5 The Learning and Organisational Development team will ensure that the induction programme for all new staff includes specific information and advice concerning this policy and local management and administrative information security policies.

4.1.6 Compliance

Information management processes must enable the University to comply with its legal and statutory obligations and any contractual obligations and national agreements it has entered into.

4.2 Outsourcing and Third-Party Access

4.2.1 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University’s information resources must agree to abide by the relevant UPRs. UH staff must proactively monitor contractors to ensure that the abide by those UPRs and any other requirements and take appropriate action in the event of a breach. Access rights for suppliers must be terminated as soon as that access is no longer required, and password changes made where there are staffing changes within that supplier.

4.2.2 Any contracts with facilities management or outsourcing companies must include service levels that address information security issues and conform to this policy.

4.2.3 Any contracts which provide services that are hosted off-site (in "the cloud") must include service levels and contractual obligations that address information security and data protection issues, have a data access agreement in place and conform to this policy.

4.3 User Management

4.3.1 Access to all systems must be authorised by the Information Asset Owner as defined in UPR IM02[3]) and/or manager responsible for the information system and a record must be maintained of such authorisations, including the appropriate access privileges and user roles granted.

4.3.2 Procedures will be established for all information systems to ensure that the access privileges of Members of the University are adjusted appropriately, and in a timely manner, whenever there is a change in business need or role or the Member leaves the University. Members' access privileges will be reviewed at regular intervals.

4.3.3 Termination of Membership or change of Membership status within the University will result in a modification of information system access privileges as stipulated in UPR.

4.3.4 Where a post has a specific Information Security responsibility this will be made clear in the job description. All Members of the University should have a clear understanding of their responsibilities under the Information Security Policy and should receive an appropriate briefing at induction.

4.3.5 The Chief Information and Digital Officer will maintain a list of all authorised Information Asset Owner and their nominees and their respective areas of responsibility (see Appendix I, UPR IM16[4]).

4.4 Systems Administrators and users with special privileges

4.4.1 The Information Asset Owner (or nominee) designated for the management and administrative information concerned, is responsible for the authorisation of special access privileges and user roles for use of the management and information system through an authorisation process agreed with the Chief Information and Digital Officer. These should be restricted to a limited number and reviewed on a regular basis.

4.4.2 All authorised access privileges and user role(s) for Members of the University will be notified to the Chief Information and Digital Officer who will arrange for their recording and secure implementation using an individual University username and password for each authorised person.

4.4.3 Administrative accounts should only be used to perform legitimate administrative activities.

---

3 UPR IM02 'Information and Data Management Principles'

4 Appendix I, UPR IM16 'Master Sources with Assigned Data and Document Steward Responsibilities'

4.5 Procedures

4.5.1 The security risks to the information assets of all system development projects will be assessed and access to those assets will be controlled.

4.5.2 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have appropriate management approval.

4.5.3 The procedures for the operation and administration of the University's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

4.5.4 Duties and areas of responsibility will be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.

4.5.5 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information processing systems. Mechanisms will be in place to monitor and learn from those incidents.

4.5.6 Procedures will be established for the reporting of software malfunctions and faults in the University's business critical information processing systems. Faults and malfunctions will be logged and monitored and timely corrective action taken.

4.5.7 Development and testing facilities for business-critical systems will be separated from operational facilities and the migration of software from development to operational status will be subject to formal procedures.

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

4.5.9 Procedures will be established to control the development or implementation of all business-critical operational software. All systems developed for or within the University must follow, as a minimum, the University's Project Management Guidelines.

4.6 Secure Information handling

4.6.1 The creation and management of records must conform to the University's record management policy (see UPR IM11[5]).

[5] UPR IM11 – 'Records Management'

4.6.2 An inventory will be maintained of all the University's business critical information assets and the ownership of each asset will be clearly stated. Each asset will be classified according to sensitivity using the University's agreed information security classification scheme.

4.6.3 When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site.

4.6.4 Areas and offices where sensitive or critical information is processed will be given an appropriate level of physical security and access control. Members of the University with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

4.6.5 Screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

4.6.6 Individuals responsible for business-critical systems must ensure that appropriate backup and system recovery procedures are in place.

4.6.7 Backup of the University's information assets and the ability to recover them is an important priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the University.

4.6.8 Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files, especially where such files may replace files that are more recent.

4.6.9 Prior to sending sensitive information or documents to third parties, the intended recipient must be authorised to receive the information and the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

4.6.10 Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured.

4.6.11 All parties/participants are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

4.6.12 The identity of recipients or requesters of sensitive or confidential information via the telephone must be verified and they must be authorised to receive the information requested.

4.6.13 No University computer should store credit card or debit card data. The use of credit and debit cards to pay on-line for University services should only be via a University-approved payment agent and with the prior agreement of the Group Finance Director (or designated deputy).

4.7 Mobile computing

4.7.1 Members of the University accessing information systems remotely to support business activities must be authorised to do so by an appropriate authority within the University. A risk assessment, based on the criticality of the information asset being used, must be carried out. Where technically feasible, all access should be through the VPN.

4.7.2 The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the University's information security policy and other good practices.

4.8 Systems Development and Changes

4.8.1 The implementation of new or upgraded software must be planned and managed carefully and any development for or by the University must always follow the University's Project Management Guidelines.

4.8.2 Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

4.8.3 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment. Changes to vendor supplied systems must be approved by the vendor. All software will be checked before implementation to protect against malicious code.

4.8.4 Prior to acceptance, all new or upgraded systems will be tested to ensure that they comply with the University's information security policies, access control standards and requirements for on-going information security management.

4.8.5 New information systems or enhancements to existing systems must be authorised jointly by the manager(s) responsible for the information and the Chief Information and Digital Officer. The business requirements of all authorised systems must specify requirements for security controls.

4.8.6 Business requirements for new software or enhancement of existing software will specify the requirements for information security controls. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the University's record management policy (see UPR IM11[5]) and a risk assessment undertaken to identify the probability and impact of security failure.

4.8.7 Equipment supporting critical business systems will be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment will be correctly maintained.

4.8.8 The implementation of new or upgraded software and/or data loads by external suppliers and third-party organisations is subject to prior planning and agreement with the University through the relevant trained and qualified systems management staff.

4.9 Systems management and maintenance

4.9.1 The University's systems will be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff will be given relevant training in information security issues.

4.9.2 Access controls will be maintained at appropriate levels for all systems and applications by on-going proactive management. Any changes of access permissions must be authorised by the Information Asset Owner and/or manager of the information system or application and a record of the access permissions granted must be maintained.

4.9.3 Access to operating system commands and system administration functions on servers is to be restricted to those persons who are authorised to undertake these operations as part of their job description. Server administration accounts should only be used to perform legitimate administrative activities and should not be granted access to email or the internet. Server administration account passwords should be changed on a regular basis.

4.9.4 Where feasible, inactive connections to the University's business systems will shut down after a defined period of inactivity to prevent access by unauthorised persons.

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

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

4.9.7 System clocks must be regularly synchronised between the University's various processing platforms.

4.9.8 Equipment supporting critical business systems will be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

4.10 Information Security Reporting

The Chief Information and Digital Officer must be informed of all breaches of information security immediately. The Chief Information and Digital Officer should bring major breaches to the notice of the University's Data Protection Officer within the Office of the Vice-Chancellor.

5 Computer Virus and Malware Protection Management

5.1 Virus and malware detection software

5.1.1 The Chief Information and Digital Officer is responsible for the distribution, installation and updating of the approved virus detection software on all University systems, services and computing equipment across the University.

5.1.2 Where appropriate, the Chief Information and Digital Officer will arrange for the approved virus detection software to be available to designated authorised persons who will then be responsible for distributing and/or installing the software and any subsequent updates to it, on all computer systems for which they are responsible.

5.1.3 All approved virus detection software that is in use within the University, by its wholly-owned subsidiary companies or their wholly-owned subsidiaries, must be updated at least daily.

5.1.4 All new IT equipment and mobile devices or those which have be re-commissioned should be installed without a network connection until virus detection software has been installed and the equipment is ready to have security updates applied.

5.1.5 Malware protection software should be configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser).

5.1.6 Malware protection software should be configured to perform regular scans of all files (eg daily).

5.1.7 Malware protection software should prevent connections to malicious websites on the internet (eg by using website blacklisting).

5.2 Patch management

5.2.1 Software running on computers and network devices that are connected to or capable of connecting to the internet should be licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.

5.2.2 Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner.

5.2.3 Out-of-date software (i.e. software that is no longer supported) should be removed from computer and network devices that are connected to or capable of connecting to the internet.

5.2.4 All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner.

5.3 Secure configuration

5.3.1 Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.

5.3.2 Any default password for a user account should be changed to an alternative, strong password.

5.3.3 Unnecessary software (including application, system utilities and network services) should be removed or disabled.

5.3.4 The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).

5.3.5 A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.

Sharon Harrison-Barker
Secretary and Registrar
Signed: **3 January 2023**

Alternative format
If you need this document in an alternative format, please email us at governanceservices@herts.ac.uk or telephone us on +44 (0)1707 28 6006.