IT SECURITY POLICY

Introduction and Overview

It is the policy of Northumbria University ("the University") to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information and equipment. The University is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets and equipment to ensure that legal, regulatory, operational and contractual requirements are fulfilled. The University wishes to support its staff and students in using IT and information systems safely and securely, in addition cybercrime poses a real and growing threat for the University and it isn't something that should be ignored. Preventing both internal and external threats, the University recognises that the ability to protect systems and data is a fundamental enabler for the University's wider strategy. Promoting an effective security culture will therefore be beneficial to both the institution and the individuals within it.

Policy Acceptance and Authority

This policy is owned by the University Director IT Services and reviewed by the Information Governance Group, it is a sub-policy of the Information Governance Policy Framework.

Scope and Applicability of this Policy

This policy is applicable to, and will be communicated to, all Northumbria University employees, students, third parties who interact with information held by the University whether processed on site or externally and the information systems used to store it. This policy supports and underpins the University's IT Strategy and other relevant strategies.

Section A: Definition

A1.1 This security policy is intended to ensure the confidentiality, integrity and availability of data and resources through the use of effective and established IT security processes and procedures.

Section B: Responsibilities

B1.1 The Information Governance Group chaired by the Senior Information Risk Owner (SIRO) is responsible for reviewing and approving information security policy and responsibilities, reviewing and monitoring security incidents and approving major initiatives to enhance information security.

B1.2 The Northumbria University IT Security Manager is responsible for managing information security within the University. This includes implementing and supporting University wide security initiatives, developing contacts with internal and external security specialists, keeping up with industrial trends, monitoring standards and advising on security issues. In addition to conducting investigations into any alleged computer or network security compromises, incidents and/or problems.

B1.3 University managers must ensure that staff within their management control area are made aware of this and other relating policies and security mechanisms. Managers must make all efforts to incorporate security procedures into staff briefings and training programs. Where applicable ensure computer and communication system security measures are observed. Managers must report promptly all significant changes in User duties or employment status to the local administrators responsible for user accounts. In addition managers are expected to ensure their staff receive appropriate training and guidance to manage information security.

B1.4 Individual users of Northumbria University IT equipment are expected to have some basic computer knowledge and should understand and adhere to University security policies and procedures. Users must protect against the misuse of computer system accounts issued to them, select and maintain good passwords and provide the correct identity and authentication information when requested. Standard facilities should be used for securing access to their workstation when left unattended, users must also notify the helpline or line management if a security violation or failure is observed or suspected. Users must not exploit system

weaknesses or attempt to assume another party's identity.

B1.5 Service administrators are expected to support and enforce applicable security policies and procedures including managing all user access privileges to data, programs and functions. Maintain and protect server software using available and approved security mechanisms. Monitor all security related events and following up on any actual or suspected violations where appropriate and report in line with section H of this policy.

B1.6 Network administrators are responsible for enforcing University security policies as they relate to technical controls in hardware and software. This includes developing appropriate procedures and issuing instructions for the prevention, detection and removal of malicious software. All data and software should be backed up on the systems/networks on a timely basis and critical programs and data archived if applicable. Network administrators should also ensure the network environment within the site and interfaces to outside networks are secure, control access to and protect network physical facilities, conduct timely audits and monitoring of server logs, incident logs and reports and report where applicable. Emergency events must be responded to in a timely and effective manner and the Information Security Manager promptly notified of all computer security incidents.

B1.7 Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are expected to comply with this IT Security Policy regarding their designated systems specifically Section E. Further guidance regarding the Information Asset Register and responsibilities can be found in the Information Asset Register Handbook.

B1.8 Contractual partners and contracted consultants must abide by Northumbria University's policies and procedures including the Acceptable Use Policy prior to accessing University systems and services. The IT System owner is responsible for ensuring that this is implemented.

B1.9 External Service Providers must abide by Northumbria University's policies and procedures when accessing University systems and services or data. The System owner is responsible for ensuring that this is implemented. Consultation with External Service Providers must be done in conjunction with the External Service Provider policy.

Section C: Physical and Environmental Security

C1 Secure Areas and Equipment

C1.1 All University network equipment must be physically secured with appropriate access control in place to ensure that only authorised personnel have access. Local area servers must be placed in locked cabinets in areas of public access or locked computer rooms.

C1.2 Wherever practical as determined by IT Services; equipment must be sited in a suitable environment to prevent loss, damage, or compromise of service and interruption to business activities.

C1.3 The IT Security Manager is responsible for approving physical access to University Data Centres.

C1.4 All persons accessing University IT areas should be prepared to produce University or third party ID cards on demand, ID's cards must not be transferred to a third party or to colleagues. Visitors must be escorted in secure areas if applicable.

C1.5 All external doors and windows must be closed and locked at the end of the work day.

C1.6 Controls should be adopted to minimise the risk or potential threats to the physical equipment including theft, fire, dust, liquid damage, electrical interference or failure, chemical effects or environmental hazards.

C1.7 Users are responsible for ensuring the security of their own belongings and for the IT equipment associated with the work station they are operating from where 'Hot Disking' arrangements are in place. Computers and laptops must not be left logged on when unattended, and must be protected by passwords and screensavers. Screens can be locked by the user when leaving their computer terminal, however, at the end of a work session, devices must be shut down and not locked so that the device can be used by other users.

Section D: Network

D1.1 This section sets out the requirements for the protection of the confidentiality, integrity and availability of the University network. The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected

together using the University local and wide area network and wireless networks.

D1.2 The Network is owned by Director IT Services and administered by IT Services Infrastructure team. The security of the network is the responsibility of IT Security Manager.

D1.3 The University network is protected by key controls such as Firewalls, Intrusion Prevention System, Mail and Web Filtering, Anti-Virus, VPN, Access Control Lists as well as further underlying security controls to prevent the network from both internal and external threats.

D1.4 The Director of IT, on the advice of the IT Security Manager, will co-ordinate the delivery of an annual programme of penetration testing on areas of the network based on risk, impact and priority. Penetration testing might be conducted by an external specialist provider and/or internal audit or through use of internal expertise.

D1.5 Computer and network resources must not be wilfully or negligently used to attempt to breach the security of the University or security of other sites. There should be an inventory containing all equipment connected to the University's wired networks and all access to Northumbria University's networks should be logged.

D1.6 Where the software allows, computer and communications systems handling sensitive, valuable, or critical University information must securely log all significant security events.

D1.7 The connection of any major non University owned IT equipment to the University network must be approved by IT Security Manager and carried out by suitably technically qualified support staff.

D1.8 When using a device connected to the University network, users must log in with a user name and password supplied by IT Services.

D1.9 Computer or communications systems attached to the University network must include sufficient automated tools to assist the administrator in verifying the systems' security status. These tools must include mechanisms for the recording, detection, and correction of commonly encountered security problems.

D1.10 Usernames and Passwords for users accessing the University domain or secured web pages from an external source must have security in place to protect authentication details. No Usernames and Passwords should be sent in clear text format. This would include access by wireless technology.

D1.11 System users must respect the physical network configuration of University owned networks and must not extend the physical network on which their system resides.

Section E: Access Control

E1 Creating, Controlling and Managing User Accounts

E1.1 Written procedures for access control and passwords based on business and security requirements must be in place. Password procedures should contain password requirements such as frequency of change, minimum length, character types which may or must be utilised and regulate password storage.

E1.2 Users accessing systems must be authenticated according to University procedures. Users should have unique combinations of usernames and passwords and are responsible for any usage of their usernames and passwords. Users must keep their passwords and system passwords confidential and not disclose them.

E1.3 Users should only have access to the services they are authorised for, access to information systems should be granted on a "need to know" basis and take into account access rights, associated privileges and be authorised in accordance with the system owners. Access to privileged accounts and sensitive areas should be restricted. Users should be prevented from accessing unauthorised information.

E1.4 Remote access to the University's computer equipment and services is only permitted if the IT Security and Acceptable Use Policy has been read and understood. All remote access from external suppliers must be risk assessed and authorised by the IT Security Manager.

E1.5 Remote access to the University's network may only take place through security solutions approved by the IT department.

E2 Granting and Revoking Systems Privileges

E2.1 Requests for a user account, access privileges and email system access must be granted only by a clear chain of authority. Approval must be obtained from the user's line manager before a service administrator grants access privileges.

E2.2 The ability to create and allow access to servers, services or applications is limited to employees with relevant authority. System and network privileges of all users, systems and programs must be restricted to the lowest level required to meet business needs. Excessive

privileges granted to users must be avoided.

E2.3 All original staff account documentation must be retained and stored securely and may be used in the event of possible legal and/or disciplinary matters. In such an event, the IT Security Manager will be given access to these documents via the University Interception and Monitoring Policy.

E2.4 All user-accounts must automatically have the associated privileges revoked after a certain period of inactivity. The recommended period is one hundred and fifty (150) days.

E2.5 On written (Email) application of appropriate management or Human Resources staff, user accounts and associated privileges will be suspended immediately.

E2.6 All user accounts must be disabled on cessation of employment. This is to include any access to shared mailboxes which may fall outside of the user's normal logon details.

E2.7 All users must be able to produce University or appropriate identification prior to being able to use any University multi-user computer or communications equipment. Positive identification for University networks involves both a username and a password.

E2.8 Log-in banners on multi-user computers must include a notice stating:

- This system is to be used only by authorised users.
- Continuing to use this system requires compliance with University conditions of use.
- Log-in banners must have physical input to continue.

E3 Password Control

E3.1 The following password measures should be implemented on all University systems and networks:

- All server accounts must be password protected, user account passwords may not be shared with or revealed to anyone. Where applicable different passwords should be used for different systems.
- User account passwords must not be written down and left in a place where unauthorised persons might discover them.
- Passwords should be at least 8 characters in length, contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z), have at least one numerical character (e.g. 0-9) and contains at least one special character (e.g. ~ ! @ # $ % ^ & * ( ) - _ + =), passwords should be changed every 60-90 days.
- All vendor supplied generic accounts and default passwords must be changed.
- Non-personal accounts must be assigned to a named person, who will be held responsible for that account and should maintain an audit trail of said account.
- No employees leaving the organisation on termination of employment should retain access to non-personal accounts, account passwords should be changed.
- Multi-user accounts and passwords must not be used unless strict password management is in place.
- System accounts and passwords should be secured and used only in emergencies.
- All passwords must be changed immediately if they are suspected of being disclosed, or known to have been disclosed to anyone. Whenever system/network security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the relevant local administrator should immediately reassign all relevant passwords, and broadcast a message to all concerned telling them to change their passwords.

E4 Monitoring of System Access and Usage

E4.1 Access and use of IT systems should be logged and monitored in order to detect unauthorised information processing activities. Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system. The IT department should register substantial disruptions and irregularities of system operations, along with potential causes of the errors. Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.

E5 External Third Party Access to University Assets

E5.1 External parties include customers, consultants, auditors, developers and suppliers. Assets include information (databases, data files, etc.), software, hardware (including removable media) and services.

E5.2 No third party IT must be installed on Northumbria University's corporate network without explicit consent from the IT Services department. Access to the University network, servers, or information systems by third parties must be controlled. Access requirements of any third party will be risk assessed by the IT Security Manager or approved project manager. Access

will not be granted until the successful outcome of an assessment. Access provided to third party organisations must have formal agreements or contracts in place.

E5.3 Technologies for connectivity to Northumbria assets include VPN clients, Citrix thin-client, SFTP and approved web applications. This list is not definitive, however connection by other technologies will only be approved on the basis of a successful full risk assessment

E5.4 Third party accounts must be configured to automatically disable after the period defined in the contract.

Section F: Safeguarding Data, Backup and Encryption

F1 Safeguarding Data

F1.1 Users of University desktop PCs where possible should always save data to their network share (U Drive). Users are not encouraged to saved data to the local PC hard disk where no back up may exist and hard disk failure may occur.

F1.2 All University servers must be served by or fitted with a suitable back up device.

F1.3 Users must only be added to the workstation administrators group if authority has been granted by the IT Services department or IT Security Manager.

F1.4 University PC's should not be used to host business critical services, where possible services should be deployed to servers and data backed up to network shares.

F1.5 Changes to network configuration (IP number, Machine name etc.) must only be carried out by IT Services technical staff.

F1.6 Local PC administrator accounts must not be disclosed to users. Changes to PC administrator accounts must only be carried out by authorised IT Services staff.

F1.7 PC firewalls may be installed only with the approval of the IT Security Manager.

F1.8 IT Services department must ensure the documentation of physical and virtual servers, services hosted, protocol usage and available ports must be in the possession of relevant core administrators.

F1.9 Firewall technology must be made available, and utilised on systems identified as requiring such a level of security.

F1.10 All computers, IT devices and servers connected to the University network where applicable must run a version of the Operating System and installed applications with the latest available security patches and updates, all computers and servers must have approved and up to date virus-scanning software enabled. No exceptions should be placed in antivirus software without consent from IT Services. Users must notify IT Services immediately if they suspect their PC has become infected. Any PC service or system suspected of being infected must be isolated from the network immediately.

F1.11 Appropriate technical and organisational controls for physically securing media including but not limited to computers, removable electronic media, receipts, paper reports, and faxes to prevent unauthorised persons from gaining access to personal data, cardholder data or organisationally sensitive data must be in place.

F1.12 Cardholder and personal data is susceptible to unauthorised viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal and cardholder data and against accidental loss or destruction of, or damage to such data.

F1.13 User education, training and awareness is available, a package of training materials has been made accessible to employees via the corporate intranet to help ensure that staff are appropriately trained and educated on information and IT security matters.

F2 Backups and Recovery

F2.1 Specialist computer staff will install, or provide technical assistance for the installation of back-up hardware and/or software. Ensuring adequate controls and procedures are in place for the backup of University data is the responsibility of the IT Services department and the systems administrator involved in the back-up process.

F2.2 All sensitive or confidential, valuable, or critical information resident on University computer systems and networks must be regularly backed-up.

F2.3 Department managers or data owners should define which information and which machines are to be backed-up, the frequency of back-up, and the method of back-up.

F2.4 Where possible backup procedures should be automated and not require manual processes.

F2.5 If the system supports more than one individual and contains data that is critical to the day-to-day operation within the University, then back-up is required daily.

F2.6 Back-ups for critical business functions should be stored off-site in suitable secure conditions.

F2.7 Back-up and recovery procedures must be documented and tested. Operation logs must be maintained and be subject to regular independent checks.

F3 Encryption

F3.1 Storage and transfer of sensitive information (organisational sensitive data or personal data defined by the Data Protection Act 1998) should be encrypted or password protected.

Section G: System Acquisition, Planning and Maintenance

G1 Operational Procedures and Areas of Responsibility

G1.1 Purchase and installation of IT equipment or software must be approved by the IT department. The IT Services department must ensure where possible the installation of new equipment and software is done in accordance with the manufacturer's security guidance.

G1.2 Changes to IT systems, equipment or software must be authorised via the Change Advisory Board (CAB) if applicable. The IT department should have emergency procedures in order to minimize the effect of unsuccessful changes to the IT systems. Emergency changes must be authorised via the Emergency Change Advisory board (ECAB) if applicable.

G1.3 Operational procedures should be documented for new systems, services and software or where changes have been made via the Change Advisory Board.

G1.4 Implementation of all new IT systems should be formally risk assessed. Before a new IT system is put into production, plans and risk assessments should be in place to avoid errors or identify unforeseen issues. Information Security should be incorporated in to the Project lifecycle of all new system or software implementation.

G1.5 Duties and responsibilities should be separated where possible to reduce the possibility of unauthorised or unforeseen abuse of Northumbria University's IT equipment and services.

G1.6 The IT Services department must ensure development, testing and maintenance environments are separated from operational IT environments to reduce the risk of unauthorised access or changes, and in order to reduce the risk of impact following error conditions.

G2 System Planning and Acceptance

G2.1 Requirements for information security must be taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes. Routines must be developed for change management and system development/maintenance.

G2.2 IT systems must be designed according to scalability and cost requirements. The load should be monitored by IT services in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.

G3 Applications and Services

G3.1 Operating systems must be approved by the IT Director.

G3.2 Users can install software via Microsoft Software Centre installed on University PC's. Other software must be security checked by the University IT Security Manager before installation and only installed by authorised individuals.

G3.3 Users shall only use legally obtained software on University computing equipment. The unauthorised use of hardware or software, which interrogates the network in any way, is forbidden.

G3.4 Copyright relating to computer programs is protected in the UK through the Copyright, Designs and Patents Act 1988 and subsequent amendments (CDPA). A computer program and the preparatory design material for the creation of a computer program are treated as literary works by the law. Sections 50A-50C of the CDPA set out a number of exceptions relating to computer programs and details which of these cannot be overridden by the terms of a contract.

G3.5 It remains the responsibility of the user to ensure that they do not infringe copyright in their use of software provided to them by the University.

G3.6 The University will produce guidance policy and guidance on copyright and all aspects of Intellectual Property to ensure that staff and students are appropriately informed about the copyright of material and the works they create.

G3.7 The University's Copyright Service (http://library.northumbria.ac.uk/copyright) provided by the University Library shall provide a central point for advice about copyright.

Software in the possession of the University must not be copied unless such copying is

consistent with the CDPA and or relevant licence agreements and either management has previously approved of such copying or copies are being made for contingency planning purposes.

G3.8 Although there is no legal obligation to provide copyright notices it is recommended that all computer programs and program documentation owned by the University include these in order to deter infringement.

G3.9 Users may only use the computing facilities in compliance with provisions of the CDPA and subsequent amendments or any corresponding law in force at any time and with the requirements of all other laws and any licences relating to the use of the facility. Additional information is available from the University's Data Protection Officer.

G3.10 Where there is a need to demonstrate or instruct in network analysis, isolated systems must be provided.

Section H: Information Security Incident Management

H1.1 Actual or potential computer security compromises including lost or stolen devices containing Northumbria University data including personal devices used for business reasons such as email must be reported to the IT Security Manager. For lost and stolen PC equipment a notification to the police may be necessary.

H1.2 All staff, students and third parties must report promptly any suspected information security incident including intrusions and out-of-compliance situations.

H1.3 All staff, students and third parties are required to report to computer virus notifications to the University helpline immediately.

H1.4 All incidents involving Personal/Sensitive Personal data defined by the Data protection Act 1998 should be reported to the IT Security Manager or Records and Information Manger immediately.

H1.5 All network or systems software malfunctions must be reported to the University helpline immediately.

H1.6 All breaches of security, along with the use of information systems contrary to routines, policies or procedures should be treated as incidents and reported in conjunction with the Information Security Incident Reporting Policy.

Section I: Electronic Mail

I1.1 The University will provide policy and procedures on good email practice.

Section J: Hosting Web Services

J1.1 The University will provide policy, procedures and good code of practice for Internet usage.

Section K: Website and content filtering

K1.1 The University exercise its right to use firewall and web filtering technologies to prevent access to undesirable web sites, including in response to the Prevent Duty for Higher Education which requires Relevant Higher Education Bodies, including Northumbria, to consider the use of web filtering in order to deny University users access to extremism-related materials. The current Content Classification System (CCS) through the external web filter provider allows for the application of automatic site blocking by a range of categories i.e. 'Adult', 'Hacking', 'Racism', the list of which is maintained by the web filtering software supplier, not Northumbria University. In the interests of academic freedom, and for bona fide research, teaching and learning purposes, it is recognised that staff and students may require access to sites which are currently blocked based on the criteria of the filtering services. The University has a 'whitelisting' procedure which is detailed in its Acceptable Use Policy. The whitelisting procedure enables staff and students with bona fide requests for access to be granted access through the IT Security Manager to websites and online material which have been blocked through the filtering technologies in force

Section L: Policy Enforcement, Review and Update

L1 Enforcement

L1.1 University staff must be notified that this policy exists and that they are expected to comply with the policy.

L1.2 Compliance with security policies is for the protection of all concerned.

L1.3 Failure to comply with this policy will expose University information and systems to unacceptable risk.

L1.4 Under rare circumstances, certain persons will need to employ systems that are not compliant with this policy. All instances must be approved in advance by the Information Security Manager.

L1.5 Failure to comply with University security policy may lead to disciplinary action being taken.

L1.6 Further guidance may be obtained from Information Security Manage or Records and Information Manager

L2 Update Information

L2.1 This document was last updated on 28 Sept 2016.