Newman University
BIRMINGHAM

Information Technology
Access Control Policy

Document History

Date of issue	Version	Role responsible for change	Nature of change
May 2018	1.0	Director of IT Services	Originated
May 2018	1.1	Director of IT Services	Modification of clause
02 February 2019	1.2	Director of IT Services	Addition of content page and document history for auditors
12 March 2019	1.4	Director of IT Services	Modification to clause 2.14
16 March 2020	1.5	DPO	Tracking Changes for Director IT Services Review
24 August 2020	1.6	Director of IT Services	Approved by ULT
5 March 2021	1.7	Head of IT Services	Minor amendments

Contents

1. Introduction and Purpose

Newman University implements physical and logical access controls across its networks, IT systems and services in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy.
Access control systems are in place to protect the interests of all authorised users of Newman University IT systems, as well as data provided by third parties, by creating a safe, secure and accessible environment in which to work.

1.1 Scope

This policy covers all Newman University networks, comms rooms, IT systems, data and authorised users.

1.2 Relationship with existing policies

This policy is for internal use and sits beneath Newman University's overarching Information Security Policy. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are approved and published and are available for viewing on Newman University's website. All staff, students and any third parties authorised to access the network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.
A full list of existing information technology policies can be found on the web site under IT User Policies

2. Policy

2.1 Principles

Newman University will provide all employees, students and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

2.2 Generic identities

Generic or group IDs shall not normally be permitted as means of access to Newman University data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

Under all circumstances, users of accounts **must** be identifiable in order for Newman University to meet the conditions of its Internet Service Provider, JISC (as laid out in the JISC 'Acceptable Use Policy').
Generic identities will never be used to access restricted data or personal data, including data supplied to Newman University by external sources.

2.3 Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a senior manager (such as a head of department a Dean or a ULT member), and will be documented by the system owner.

IT Services shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.
Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, not for program use, unless it is otherwise impossible to operate the program.

2.4 Least privilege and need to know

Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know.

2.5 Maintaining data security levels

Every user must understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user must still maintain the security of data commensurate to their sensitivity.

The Newman University Information Classification Table enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.

Users electing to place information on non-IT Services managed systems and databases, digital media, cloud storage, or removable storage devices are advised only do so where:

- such an action is in accord with the information's security classification, Information Security Policy and Bring Your Own Device (BYOD) Policy
- the provision meets any research data supplier or other contracts,
- other protective measures (such as the use of encryption) have been implemented.

Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations from data providers they may have to meet.
Users are obligated to report instances of non-compliance to the DPO via the IT Service Desk.

3 Access control authorisation

3.1 User accounts

Access to Newman University IT resources and services will be given through the provision of a unique user account and complex password.
Accounts are provided on the basis of valid records in the HR (iTrent) and student records (SITS). For any user not in either of those systems, access is granted via the appropriate staff form received from the Director of Quality and Deputy Registrar.

3.2 Passwords

Password issuing, strength requirements, changing and control will be managed through formal processes.
Password issuing will be managed by IT Services for staff and students. Password length, complexity and expiration criteria for both staff and student passwords are governed by the Newman University Password Policy.

Password changes, resets and account unlocking can be performed by users via the self-serve password reset system. It is mandatory for users to register to use this facility.

3.3 Access to restricted and highly restricted information

Access to 'Restricted' and 'Highly Restricted' information will be limited to authorised persons whose job or role responsibilities require it, as determined by law, contractual agreement with interested parties or the Information Security Policy.
Access to any of these resources will be constrained and controlled by use of firewalls, network segregation, secure log-on procedures, access control restrictions and other controls as appropriate.
The responsibility to implement access restrictions lies with the managers of the role based resource (e.g. Finance office APTOS software access is granted by the Head of Finance), but must be implemented in line with this policy.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within Newman University's Active Directory domain and administered by IT Services.
There are no restrictions on the access to 'Public' information.

3.4 Policies and guidelines for use of accounts

Users are expected to become familiar with and follow Newman University policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the Conditions of Use of IT Systems at Newman and the JISC Acceptable Use Policy.

3.5 Access for remote users

Access for remote users shall be subject to authorisation by IT Services and be provided in accordance with the BYOD Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

4 Physical access control

Physical access across the Newman University campus, where restricted, is controlled primarily via ID Cards. Visitors must sign in / out at Reception and will be given a numbered visitor ID card where necessary. This will provide basic level access to controlled doors. The sharing of ID cards is not permitted. If staff or students forget their badge they must sign one out / in a numbered visitor's badge at Reception. Access to the Communication Room is additionally restricted via a key lock.

4.1 Lost cards

Lost ID Cards must immediately be reported to the IT Service Desk, who will cancel the card through the access control system.

4.2 Reissuing ID cards

Replacement cards cannot be issued until confirmation that a prior card has been cancelled. New cards with the same level of access control will be issued by the IT Service Desk.

5 Access control methods

Access to data is variously and appropriately controlled according to the Information classification table and the Information Security Policy.

Access control methods used by default include:

- explicit logon to devices,
- Windows share and file permissions to files and folders,
- user account privilege limitations,
- server and workstation access rights,
- firewall permissions,
- network, IP telephone systems
- IIS/Apache intranet/extranet authentication rights,
- Newman domain user login rights,
- Database access rights and ACLs,
- Encryption at rest
- Any other methods as contractually required by interested parties.

Access control applies to all Newman University owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Newman University.

5.1 Penetration tests

Newman University's access control provision will be regularly penetration tested, in order to ascertain the effectiveness of existing controls and expose any weaknesses. Tests will include, where appropriate and agreed to, the systems of cloud service providers. For example: The web site hosting provider via AWS.

6 Review and development

This policy shall be reviewed and updated regularly by IT Services, the DPO and an external auditor to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
Additional regulations may be created to cover specific areas.