Maynooth University
National University of Ireland Maynooth

Maynooth University
IT Services

Network Security Policy v1.1

Policy Details and Revision Record

Policy Name	Network Security Policy
Version Number:	v1.1
Policy Owner:	Head of IT Operations
Approved by	IT Services Management
Approval Date:	24th March 2022
Next Review Date:	Q2 2024

Table of Contents

1. Policy Title

This document outlines the Maynooth University Network Security Policy.

2. Policy Statement

This document outlines the Network Security Policy for Maynooth University (MU) network as operated by IT Services. “The Network” is considered to be any transmission media or service that connects and facilitates data transfer between Maynooth University entities. Network scope includes the Campus Area Network, connected networks and wide area network services (Office365, website, other cloud-hosted platforms).

3. Policy Scope

This Network Security Policy applies to

- the network as operated by IT Services.
- the entities that are used in the physical delivery of the network service – cabling, network equipment and devices attached to the network.
- the logical design of MU systems/services that are accessed from the network (ICT services).
- connected networks - autonomous networks, MaynoothWorks and 3rd parties, as required.

4. The Purpose of the Network Security Policy

The purpose of this policy is to ensure the security of the network. IT Services will:

- Protect the network from against unauthorised access. **(Confidentiality)**
- Protect the network from unauthorized or accidental modification **(Integrity)**
- Ensure the network is accessible as and when required by network users **(Availability)**

5. Policy Principles

Physical & Environmental Security

Network equipment including routers, switches and servers will be:

- Housed in secure areas in communication rooms, protected by a secure perimeter appropriate to the size and purpose of the network equipment.
- Protected with appropriate security barriers and entry controls. Entry controls to data centre locations and communication rooms include logged swipe card access.
- Maintained in an environment that is controlled for temperature, humidity and power supply quality appropriate to the size and purpose of the network equipment.
- Protected from power supply failures, intruder alarms and fire suppression systems when located in data centre locations.

All visitors to data centre locations must be authorised by the ICT Infrastructure Manager, or appropriate deputy.

Devices Connecting to the Network

- IT Services managed devices in AD or AAD will have access to all available ICT services. All other devices will have Internet access and access to Internet accessible MU ICT services.
- Devices connecting to connected networks are granted Internet access and access to Internet accessible MU services.
- Access to key business information systems is governed by additional controls including campus location and/or directory group membership.

Access Control to the Network

- All users of ICT services should have their own individual user identification and password.

- Access to ICT services shall be via a secure log-on procedure.
- Remote access to ICT services on the network should make use of MFA wherever possible.
- Remote access to the network will be granted via a VPN. The VPN services (MU and 3rd parties) will require individual user identification combined with MFA.

Network Operating & Security Procedures

- IT Services should ensure that all network service equipment is maintained to best software level as recommended by the manufacturer in line with the MU Patch Management policy.
- IT Services will ensure that adequate network equipment maintenance contracts as appropriate are in place, maintained and periodically reviewed for all network equipment.
- Documented operating procedures will be prepared and reviewed annually for the operation of network equipment, to ensure correct and secure operation. Any changes to operating procedures should be authorised by the ICT Infrastructure Manager or appropriate deputy.
- IT Services will ensure that access logs for network equipment are maintained and reviewed monthly
- IT Services will ensure that timely information regarding the technical vulnerabilities of network equipment and ICT services is obtained. Any vulnerability will be assessed, and any risks appropriately mitigated and controlled.

Network Service Security & Availability Architecture

- IT Services-operated network infrastructure and authentication services (DNS, DHCP, AD) will be configured to be resilient and highly available as outlined in the IT Disaster Recovery Plan.
- The perimeter, core and distribution layers of the network will be configured to be logically and physically highly available and resilient. The network access layer will rely on cold hardware swap on equipment failure.
- The IT Services Security Incident and Event Management (SIEM) service will record network access logs.
- Connected networks will be segmented from the main campus network.

Internet Security and Web Filtering

- The campus network firewall security policy (inbound) will be configured to ‘deny all’ network traffic.
- The default firewall configuration (outbound) will be configured to ‘permit all’ network traffic.
- Exceptions to these configurations will be recorded and maintained. Inbound configuration rules items will be reviewed quarterly.
- Where a device/destination/or user is marked as an exception by the Advanced Threat Protection (ATP) systems they will be automatically blocked from traversing the firewall to Internet destinations and will only be released when the threat has been investigated and cleared as secure.
- The network is dependent on DDoS protection provided by HEAnet. ICT services hosted in the IT Services supported cloud data centre will be configured for DDoS protection from the data centre service provider.

Email Security Standards

- The Maynooth University email domains including @mu.ie, @mumail.ie will be hosted on the Microsoft 365 platform which is configured that data in transit and at rest is encrypted.
- Email domains will be configured for the Domain-based Message Authentication Reporting and Conformance (DMARC) protocol combining Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).
- This Microsoft 365 platform either natively or via a 3rd party will be configured to deliver email threat protection including phishing identification, malicious URL detection, and attachment scanning for spam and malware filtering.

Advanced Threat Protection

- The campus network perimeter firewall will be updated automatically by subscription to Advanced Threat Protection (ATP) services. This service will provide the latest in security threat intelligence and provide protection from 'zero-day' threats, implement malware blocking and provide Intrusion Prevention System (IPS).
- For IT Services managed devices and servers, software to protect against malware will be installed.
- Software used to protect ICT services against malware will be regularly reviewed and updated.

Clock Synchronization (NTP)

- All network service equipment and ICT systems and services shall be synchronised using IT Services NTP service.

Logging & Monitoring

- Event logs recording network activity, exceptions, faults and security events will be maintained and recorded to the IT Services SIEM service as appropriate.
- Logging facilities and log information shall be protected against tampering and unauthorised access.
- The activity of privileged network service equipment administrators should be logged where practicable, the logs protected and regularly reviewed.

6. Roles and Responsibilities

IT Services

- Approval and regular review of this policy
- Compliance monitoring and reporting (including compliance reporting for connected networks)
- Technical delivery of the policy principles
- Implement network security measures
- Ensuring that owners of connected networks are informed of this policy.
- Design, develop, maintain the network security model on IT systems and services with regard to the network security requirements of confidentiality, integrity and availability

Owners of Connected Networks

- Technical delivery of the policy principles as relevant
- Implement network security measures
- Maintain network services (e.g., DNS, DHCP)

7. Definitions

Active Directory (AD)
Active Directory (AD) is a source database and set of services that is used to connect users with services. Active Directory stores identities in the form of usernames and passwords.

Azure Active Directory (AAD)
AAD is a form of AD stored in Microsoft Azure AD

Connected Network
Any department/section/project that is providing network connectivity services i.e. DNS, DHCP and authentication for devices.

Data Centre Locations
Dedicated rooms on the University campus (North and South) that house network equipment and servers.

Distributed Denial-Of-Service DDoS

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Entity
Item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence.

ICT Services
MU systems/services that are accessed from the network. These include information systems, website and teaching & learning systems.

Intrusion Prevention System (IPS)
An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target system or service.

Network
"The Network" is considered to be any transmission media or service that connects and facilitates data transfer between Maynooth University entities. Network scope includes the Campus Area Network and services such as Microsoft365 and other cloud-hosted services.

Network Time Protocol (NTP)
NTP provides a reference clock that acts as a fixed point for all times recorded in logs and events. All clocks are coordinated according to this clock or time. The coordinated universal time (UTC), which is recognized as a uniform world time clock, is used for this purpose.

Security Incident and Event Management (SIEM)
Security Information and Event Management (SIEM) is a software solution that aggregates and analyses activity from different resources across the ICT infrastructure. SIEM collects security data from network devices, servers and domain controllers. SIEM stores, normalizes, aggregates and applies analytics to that data to discover trends, detect threats, and enables alerts to be investigated.

8. Relevant Information

Related Policies

Maynooth University Password Policy
Maynooth University Patch Management Policy

9. Appendix A – System Audit & Event Logs

Version History

Version	Date	Author/Editor	Comments
0.5	To Jan 2022	P O'Regan, D O'Reilly	Draft reviewed with HEAnet and contributions from IT staff
V0.55	March 2022	D O'Reilly	Including/review of all input and feedback to date
V0.6	March 2022	D O'Reilly	For review/comment
V1	March 2022	D O'Reilly	Updated following review/comment IT Mgrs.
V1.1	April 2024	D O'Reilly	Updated to include Appendix A: Standard for System Audit and Event Logs