

[Company]

NETWORK SECURITY MANAGEMENT POLICY

Management and security of the network

1 Document Version Control

Last Modified				Last Modified By				Document Changes			
0.1	[DATE]										Document first created

2 Document Contents Page

1	Document Version Control	2
2	Document Contents Page	3
3	Network Security Management Policy	5
3.1	Purpose	5
3.2	Scope.....	5
3.3	Principle	5
3.4	Network Controls	6
3.5	Security of Network Services	7
3.6	Segregation in Networks.....	7
3.7	Access to networks and network services	8
3.8	Network locations	9
3.9	Physical Network Devices	10
3.10	Web Filtering.....	10
3.11	Host Intrusion, Network Intrusion, Malware and Antivirus	11

4	Policy Compliance	12
4.1	Compliance Measurement	12
4.2	Exceptions	12
4.3	Non-Compliance	12
4.4	Continual Improvement.....	12
5	Areas of the ISO27001 Standard Addressed.....	13

3 Network Security Management Policy

3.1 Purpose

The purpose of this policy is to ensure the protection of information in networks and its supporting information processing facilities.

3.2 Scope

All company employees and external party users.

All company networks, network services, network administration and management solutions and network devices.

3.3 Principle

The network is managed on the principle of least privilege with security by design and default.

3.4 Network Controls

- responsibilities and procedures for the management of networking equipment are established
- operational responsibility for networks is separated from computer operations where appropriate.
- special controls are established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications
- appropriate logging and monitoring are applied to enable recording and detection of actions that may affect, or are relevant to, information security
- management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure

- systems on the network are [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- Do not disclose private IP addresses and routing information to unauthorized parties

3.5 Security of Network Services

Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.

The ability of the network service provider to manage agreed services in a secure way are determined and regularly monitored, and the right to audit should be agreed.



3.6 Segregation in Networks

Large networks are divided into separate network domains. The domains are chosen based on trust levels.

Segregation can be done using either physically different networks or by using different logical networks (e.g., Virtual private networking).

The perimeter of each domain is well defined.

Access between network domains is allowed but is controlled at the perimeter using a gateway (e.g., firewall, filtering router).

The criteria for segregation of networks into domains, and the access allowed through the gateways, is [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.7 Access to networks and network services

Users are only provided with access to the network and network services that they have been specifically authorized to use.

Access to networks and network services is in line with the Access Control Policy.

Before connecting to the network devices have

- Been registered in the asset register
- Been patched to the latest security patch levels
- Appropriate malware protection installed
- Default passwords and accounts deleted or disabled

- █ [REDACTED]
- █ [REDACTED]
- █ [REDACTED]

3.8 Network locations

In the order of preference, physical networks should be within these geographical boundaries

- Within the UK borders
- Within the European Economic Area (EEA) borders
- Within countries with adequacy of the protection of personal data in non-EU countries as outlined by GDPR [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- Where standard contractual clauses are in place as outlined by GDPR. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.9 Physical Network Devices

Physical network devices are managed in line with the Physical and Environmental Security Policy and specifically the section on Network Access Control, Cabling Security, Equipment Siting and Protection.

Physical network devices are destroyed in [REDACTED]

Physical networks devices are in line with [REDACTED]

3.10 Web Filtering

Access to websites containing illegal information or known to contain virus or phishing material is restricted.

Access to the following types of websites where practicable is blocked:

- Websites with an information upload function unless permitted for valid business reasons
- Know or suspected malicious websites

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

3.11 Host Intrusion, Network Intrusion, Malware and Antivirus

Network services and devices are managed in line with the Malware and Antivirus Policy and specifically all sections of the policy.

Host intrusion and network intrusion is [REDACTED]

[REDACTED]

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.