[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

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 authenticated
- systems connection to the network should be restricted
- Perimeter firewalls are installed between all wireless networks and the cardholder data environment and configured to deny traffic. (Unless traffic is necessary for business purposes and documented and approved then permit only authorized traffic between the wireless environment and the cardholder data environment)
- Permit only “established” connections into the network.

- 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.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The company should ensure that network service providers implement these measures.

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 based on an assessment of the security requirements of each domain. The assessment is in accordance with the access control policy, access requirements, value and classification of information processed and takes account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration is made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway before granting access to internal systems.

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

- Been included where possible in the network management system
- Ports, services, applications, and guest accounts removed or disabled that are not required.

3.8 Network locations

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

- Within the UK boarders
- Within the European Economic Area (EEA) boarders
- Within countries with adequacy of the protection of personal data in non-EU countries as outlined by GDPR. For one source on the most recent list the following link is considered but any list is verified by legal counsel before deployment. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Where standard contractual clauses are in place as outlined by GDPR. For one source on the most recent list the following link is considered but any list is verified by legal counsel before deployment. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

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 line with **the Information Classification and Handling Policy** specifically the section on the Destruction of Electronic Media / Devices.

Physical networks devices are in line with the **Asset Management Policy** and subject to the asset management process.

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
- Command and control servers
- Malicious websites identified in threat intelligence
- Websites sharing illegal content

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 deployed based on risk, business need and where practical to do so.

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.