[Company]

MALWARE AND ANTI VIRUS POLICY

Protection of assets and information from virus and malware

1 Document Version Control

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

2 Document Contents Page

3 Malware and Antivirus Policy

3.1 Purpose

This policy is to manage and mitigate the risk of malware and viruses.

3.2 Scope

All employees and third-party users.

All company devices.

All devices used to access, process, transmit or store company information.

Virtual devices where applicable and feasible.

3.3 Principle

Company devices have adequate protection of company information from the risk of malware or virus.

3.4 Approved Software

Only company approved and licenced software is to be installed on company equipment.

Unauthorised software, downloaded software, free software or utilities must not be used.

3.5 Malware and Antivirus Software

Malware and Antivirus Software must be installed on every device that can run it.

Malware and Antivirus Software automatically update signature-based definitions as they are released by the vendor.

Malware and Antivirus Software cannot be modified or disabled by the end user.

Malware and Antivirus Software produces an alert when an infection or suspected infection occurs.

Suspected infections are managed via the incident management process.

Malware and Antivirus Software is set to auto repair or quarantine suspect files.

Malware and Antivirus Software is set to automatically scan storage and attached storage.

Malware and Antivirus Software is set to automatically scan any filed that is accessed, modified, or ran.

Malware and Antivirus Software is set to retain audit logs which are monitored.

3.6 Education

Users are educated periodically as part of the user training and awareness process on phishing, safe use of the internet, software usage and what to do in the event of a virus or malware infection.

3.7 System Configurations

Systems are configured to remove unnecessary services, configurations, and ports as part of the infrastructure management process.

3.8 Email

Email servers must have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server.

3.9 Internet Proxy/Secure Web Gateway Configuration

Internet proxies/secure web gateways must be configured to use web reputation scoring to

- Block sites with very poor reputations
- Allow sites with very good reputations
- Scan all content for threats for sites with reputations in between very poor and very good
- Log all detections

- Automatically check for virus definition updates

The use of allow listing and deny listing should be deployed.

3.10 File Integrity Checks

File integrity checks are implemented for all system critical files and any files that contain or access personal customer data.

3.11 Host Intrusion Detection / Network Intrusion Detection

Host intrusion and network intrusion is in place on confidential, personal, customer and card holder information as required based on business need, legal and regulatory compliance, and risk.

Intrusion Detection Systems have up to date detection and prevention engines, patches and signature files and alert authorised personnel based on alerting rules.

Intrusion alerts are managed via the incident management process.

Intrusion Detection Systems have logging enabled and are in line with the **Logging and Monitoring Policy**.

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.