

[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

1	Document Version Control.....	2
2	Document Contents Page.....	3
3	Malware and Antivirus Policy	5
3.1	Purpose	5
3.2	Scope.....	5
3.3	Principle	5
3.4	Approved Software	6
3.5	Malware and Antivirus Software	6
3.6	Education	7
3.7	System Configurations.....	7
3.8	Email.....	7
3.9	Internet Proxy/Secure Web Gateway Configuration	7
3.10	File Integrity Checks	8
3.11	Host Intrusion Detection / Network Intrusion Detection	8
4	Policy Compliance	9

4.1	Compliance Measurement	9
4.2	Exceptions	9
4.3	Non-Compliance	9
4.4	Continual Improvement.....	9
5	Areas of the ISO27001 Standard Addressed.....	10

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.



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.

[Redacted]

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.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

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 [REDACTED]

[REDACTED]

3.8 Email

Email servers must [REDACTED]

[REDACTED]

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
- [REDACTED]
- [REDACTED]
- Log all detections

- [REDACTED]

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.

[REDACTED]

[REDACTED]

[REDACTED]

[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.