



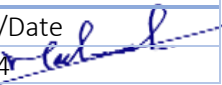
Malware Handling Policy

Doc. Control Number	Version
SNL-72	0.2



Document Reference

Item	Description
Title	Malware Handling Policy
Department	Cybersecurity Department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	31 March 2024
Revision-Date	31 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	31/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	1/4/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	1/4/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	31 March 2023	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Scope	4
3. Policy	4
4. Policy Compliance	5

1. Overview

The Malware Handling Policy outlines the procedures and protocols for detecting, preventing, and responding to malware threats within the company. Malware, including viruses, ransomware, and other malicious software, poses significant risks to the security and integrity of organizational information assets. Therefore, this policy aims to establish a comprehensive framework for safeguarding the company's digital infrastructure against malware attacks.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals accessing the company's network or utilizing organizational devices. It encompasses all devices connected to the organizational network, including but not limited to desktops, laptops, mobile devices, servers, and network appliances.

3. Policy

3.1 Detection and Prevention Controls

- a) The company shall utilize endpoint protection software on all devices accessing the organizational network or storing organizational data.
- b) Endpoint protection software must regularly update its signature database to detect and prevent the latest malware threats.
- c) Measures shall be implemented to prevent unauthorized deactivation or alteration of endpoint protection software by users.

3.2 Technical Controls Implementation

- a) Internet filters and email filters shall be deployed to block malicious traffic sources, including phishing emails and websites hosting dangerous content.
- b) Download restrictions shall be enforced to prevent users from accessing or downloading potentially harmful content from the internet.
- c) Removable media, such as USB drives and external hard drives, must undergo anti-malware scans upon insertion or connection to organizational devices.
- d) Advanced malware detection techniques, such as enabling DNS query logging to detect hostname lookups for known malicious domains, shall be implemented.

3.3 Logging and Monitoring

- a) Advanced logging and monitoring tools shall be employed to analyze and alert on detected malware events in real-time.
- b) Logs related to malware detection and prevention should be regularly reviewed and analyzed to identify trends, patterns, and potential security risks.
- c) Incident response procedures shall be in place to promptly address and mitigate any malware incidents detected through logging and monitoring.

3.4 Employee Training and Awareness

- a) Regular training sessions shall be conducted to educate employees on recognizing and reporting potential malware threats, including phishing attempts and suspicious website links.
- b) Employees shall be informed about the importance of adhering to the company's malware handling policies and procedures to protect organizational information assets.



4. Policy Compliance

The Infosec team will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrust, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.1 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

4.2 Non-Compliance

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