**Protection Against Malware**

**ISO 27001:2022**

**Non-disclosure**

The information contained in this communication is confidential and intended solely for the recipient. Unauthorized disclosure, copying, or distribution of this information is strictly prohibited. Any views or opinions expressed are solely those of the author and do not necessarily represent those of the organization. By receiving this information, you agree to keep it confidential and to use it only for the intended purpose. If you are not the intended recipient, please notify the sender immediately and delete this message. Thank you for your understanding and cooperation in maintaining the confidentiality of this information.

**Table of contents**

[1 Introduction 4](#_Toc199342946)

[2 Disclaimer 4](#_Toc199342947)

[3 Purpose 4](#_Toc199342948)

[4 Scope 4](#_Toc199342949)

[4.1 Comprehensive Protection Across Systems 5](#_Toc199342950)

[4.2 Detection and Prevention of Various Malware Types 5](#_Toc199342951)

[4.3 Incident Response and Recovery 5](#_Toc199342952)

[4.4 Adaptation of Emerging Threats 6](#_Toc199342953)

[5 Policy requirements 6](#_Toc199342954)

[5.1 Comprehensive protection across all systems 6](#_Toc199342955)

[5.2 Detection and Prevention of Various Malware Types 7](#_Toc199342956)

[5.3 Incident response and recovery 9](#_Toc199342957)

[5.4 Adaptation of Emerging Threats 10](#_Toc199342958)

[6 Non-Compliance 12](#_Toc199342959)

# Introduction

Malware poses a significant threat to the confidentiality, integrity, and availability of information assets, making effective malware control a crucial component of an organization's cybersecurity strategy. In alignment with the requirements of ISO 27001:2022 Annex A 8.7 “Protection Against Malware”, in next text “Malware Control Policy”, this policy establishes the framework for preventing, detecting, and mitigating the impact of malicious software. It aims to safeguard sensitive data, protect critical systems, and ensure compliance with applicable legal and regulatory requirements. The organization is committed to implementing robust controls, including the use of anti-malware software, regular updates, and employee awareness training. By adhering to this policy, the organization seeks to minimize risks associated with malware and maintain a secure operating environment.

# Disclaimer

This Malware Control Policy is provided as a guideline to support the organization in establishing effective measures to prevent, detect, and respond to malicious software threats in accordance with ISO 27001:2022. While the policy outlines best practices and recommended controls, it should be tailored to the unique requirements, risks, and operational context of the organization.

The policy does not serve as a substitute for professional cybersecurity advice or a comprehensive risk assessment. The organization must ensure that the implementation of controls and measures is aligned with its specific business needs, regulatory obligations, and technological infrastructure.

This document is intended to promote awareness and responsibility but does not guarantee absolute protection from malware or other cybersecurity threats. The organization reserves the right to amend this policy as needed to address evolving security challenges and compliance requirements.

# Purpose

The purpose of the Malware Control Policy is to establish a comprehensive approach to safeguarding the organization’s information assets from malware threats. This policy aims to implement effective preventive measures, including the deployment of anti-malware software and user awareness training, to mitigate risks associated with malicious software. By defining clear roles and responsibilities, the policy ensures that all personnel are equipped to recognize and respond to potential malware incidents. Ultimately, the policy seeks to maintain the integrity, confidentiality, and availability of critical data and systems, thereby supporting the organization's overall information security objectives.

# Scope

The scope of the Malware Control Policy is designed to ensure comprehensive protection against malware threats across all aspects of an organization's information systems. It applies to all employees, contractors, and third-party users who interact with the organization's information assets, ensuring that everyone adheres to the defined security measures.

This policy covers all devices and systems used to access, process, transmit, or store organizational data, including physical devices, virtual environments, and cloud-based systems. It also extends to external files, software, and removable media, ensuring that these are scanned and secured before integration into the organization's network.

Additionally, the policy includes technical controls, such as antivirus software, intrusion detection systems, and secure configurations, as well as user awareness training to mitigate risks associated with human error. The scope ensures that malware protection measures are implemented at all levels, from individual devices to network-wide systems, to maintain the confidentiality, integrity, and availability of information assets

Scope topics of Access Policy are:

* Comprehensive Protection Across Systems: Malware control encompasses safeguarding a wide range of systems, including personal devices, enterprise networks, and cloud environments. Malware can target multiple systems within a network, making it essential to assess and secure all potential points of vulnerability.
* Detection and Prevention of Various Malware Types: Malware control addresses different types of malicious software, such as viruses, worms, ransomware, spyware, and trojans. Each type operates differently, requiring tailored detection and prevention strategies.
* Incident Response and Recovery: Beyond prevention, malware control includes responding to incidents, mitigating damage, and recovering affected systems. This involves identifying the malware's entry point, removing it, and restoring normal operations.
* Adaptation to Emerging Threats: The scope also involves staying ahead of evolving malware threats. New and unknown malware variants require advanced technologies and continuous updates to security measures.

## Comprehensive Protection Across Systems

The malware control policy ensures comprehensive protection across all systems by addressing the risks posed by malicious software to an organization’s information assets. It applies to all devices, including physical, virtual, and cloud-based systems, that process, store, or transmit organizational data, ensuring no system is left vulnerable. The policy mandates the use of approved anti-malware tools, regular updates, and system-wide scanning to detect and mitigate threats effectively. By implementing these measures, the organization creates a robust defense against malware, safeguarding the confidentiality, integrity, and availability of its critical information assets.

## Detection and Prevention of Various Malware Types

The malware control policy emphasizes the importance of detecting and preventing a wide range of malware types, including viruses, ransomware, spyware, and trojans. It requires the implementation of up-to-date anti-malware tools and regular system scans to identify and neutralize known vulnerabilities, reducing the likelihood and impact of attacks. The policy also mandates proactive measures, such as monitoring for unusual activity and applying security patches, to prevent the exploitation of emerging threats. Additionally, organizations are encouraged to educate personnel on recognizing malware risks and adhering to safe practices, such as avoiding suspicious links or downloads. By addressing both technical and human factors, the policy ensures a comprehensive approach to mitigating malware risks and protecting critical information assets.

## Incident Response and Recovery

Incident response and recovery are critical components of the malware control policy, ensuring that organizations can effectively manage and recover from malware-related incidents. The policy emphasizes the need for predefined incident management procedures, including roles, responsibilities, and escalation paths, to ensure a quick and consistent response to minimize operational and financial damage. It also requires organizations to implement processes for detecting, analysing, and containing malware incidents, followed by controlled recovery measures to restore normal operations while safeguarding data integrity. Additionally, the policy highlights the importance of post-incident activities, such as root cause analysis and lessons learned, to improve future incident management and prevent recurrence. By integrating these practices, the policy ensures that organizations are prepared to handle malware incidents efficiently, reducing their impact on business continuity and information security.

## Adaptation of Emerging Threats

The malware control policy emphasizes the need for organizations to adapt to emerging threats by continuously monitoring and analysing the evolving malware landscape. This involves leveraging threat intelligence to identify new attack vectors, tactics, and vulnerabilities, enabling the organization to proactively update its defences. Regular system assessments, software updates, and the implementation of advanced detection tools are critical to staying ahead of sophisticated malware threats. Additionally, the policy encourages organizations to educate personnel on the latest malware trends and ensure that all security measures are aligned with current risks. By adopting a proactive and dynamic approach, the policy ensures that organizations remain resilient against both known and emerging malware threats.

# Policy requirements

## Comprehensive protection across all systems

The malware protection policy outlines several requirements to ensure comprehensive protection across all systems. These include:

Applicability Across All Systems:

* Apply malware protection measures to all devices, including desktops, laptops, servers, mobile devices, IoT devices, and cloud-based systems.
* Extend protections to virtual environments and on-premise infrastructure.

Endpoint and Network Protection:

* Install and maintain anti-malware solutions on all endpoints (e.g., user devices, servers, and network gateways).
* Use a defense-in-depth approach, including endpoint devices and gateway controls, to address multiple attack vectors (e.g., ransomware).
* Implement network segmentation to isolate sensitive systems and limit the spread of malware.

External Media and File Scanning:

* Scan external storage devices (e.g., USB drives) and files obtained from external sources before use.
* Enforce policies for securely handling email attachments and downloaded files to prevent malware infiltration.

Software and Application Control:

* Use allow listing to restrict the execution of unauthorized or unverified applications.
* Regularly update operating systems, software, and applications to address vulnerabilities that could be exploited by malware.

Cloud Service Protection:

* Ensure that cloud services used by the organization are configured securely and include malware detection and prevention capabilities.
* Monitor and manage access to cloud resources to prevent unauthorized activities or malware infections.

Backup and Disaster Recovery:

* Implement a robust backup and disaster recovery plan to ensure quick recovery from malware incidents.
* Protect backup systems from malware by isolating them from the primary network and implementing robust access controls.

Monitoring and Threat Intelligence:

* Continuously monitor for malware threats and gather intelligence on emerging risks from trusted sources.
* Ensure that all notifications regarding potential malware threats come from reliable and accurate sources.

User Awareness and Training:

* Provide anti-malware training to all personnel, covering topics such as email security, social engineering, and safe computing practices.
* Educate users on recognizing malware risks and adhering to safe practices.

Special Cases for Non-Standard Systems:

* For systems that cannot support standard malware protection (e.g., industrial control systems), establish alternative measures such as full reinstallation of compromised systems.

High-Risk Activities:

* Implement controls to prevent malware intrusions during high-risk activities, such as emergency protocols or maintenance.

By implementing these requirements, organizations can ensure comprehensive protection across all systems, safeguarding their information assets from malware threats.

## Detection and Prevention of Various Malware Types

The malware protection policy includes specific requirements to ensure the effective detection and prevention of different types of malware, such as viruses, ransomware, spyware, trojans, and more. Below are all the relevant policy requirements:

Deployment of Malware Detection Tools:

* Install and maintain anti-malware solutions on all systems, including endpoints, servers, and network gateways.
* Ensure malware detection tools are updated regularly to recognize the latest malware signatures and threats.

Regular and Automated Scans:

* Conduct regular, automated scans of all files, systems, and devices to detect and mitigate malware infections.
* Schedule scans for critical systems and files, and ensure they are performed after any significant system changes.

Real-Time Malware Detection:

* Enable real-time scanning for incoming files, emails, instant messages, and web traffic to block malware before execution.
* Configure alerts to notify administrators of any detected malware incidents.

Blocking Malicious Websites:

* Use web filtering tools, such as block listing, to restrict access to known or suspected malicious websites.
* Employ domain reputation services to prevent connections to high-risk websites.

Control of Unauthorized Software:

* Enforce allow listing to ensure only approved and verified applications can be installed or executed on systems.
* Prohibit the use of unauthorized or unlicensed software to reduce the risk of malware introduction.

Email and File Scanning:

* Scan all email attachments, links, and downloads for malware before they are accessed or opened.
* Implement email security tools to detect phishing attempts and malicious payloads.

External Media and File Handling:

* Mandate scanning of external media, such as USB drives and external hard drives, before connecting them to organizational systems.
* Enforce policies for securely handling files from external sources.

System and Application Updates:

* Regularly update operating systems, software, and applications to patch vulnerabilities that could be exploited by malware.
* Automate updates where possible to ensure timely implementation of security patches.

Behavior-Based Malware Detection:

* Deploy advanced detection tools (e.g., endpoint detection and response, or EDR) to identify and block malware based on suspicious behavior, even if signatures are unknown.
* Monitor for unusual activities, such as unauthorized file encryption or unexpected network traffic.

Proactive Threat Intelligence:

* Integrate threat intelligence feeds to stay informed about new malware variants and attack methods.
* Adapt detection mechanisms to address emerging malware threats.

Encrypted File Inspection:

* Use tools capable of inspecting encrypted files or traffic to detect malware hidden within encrypted communications.

User Awareness and Training:

* Train employees to recognize common malware threats, such as phishing emails, malicious links, and rogue software.
* Promote awareness of safe browsing habits, secure email practices, and the dangers of unverified downloads.

Incident Reporting Mechanisms:

* Establish a streamlined process for employees to report suspected malware infections or unusual system behavior.
* Encourage prompt reporting to enable swift detection and containment of malware.

Audit Logs and Monitoring:

* Maintain logs of malware detection and prevention activities for review and analysis.
* Regularly monitor these logs to identify trends, anomalies, or recurring threats.

Specialized Tools for Advanced Threats:

* Deploy specialized tools, such as sandboxing, to analyze and isolate suspicious files or applications in a controlled environment.
* Leverage machine learning or artificial intelligence (AI)-based tools to detect sophisticated, zero-day malware threats.

By following these requirements, organizations can create a robust detection and prevention framework that addresses various malware types, ensuring the security of their information systems and assets.

## Incident response and recovery

The malware protection policy outlines specific requirements for responding to and recovering from malware incidents. Below are all the policy requirements for incident response and recovery:

Incident Response Requirements

Establish Incident Response Procedures:

* Define and document clear procedures for responding to malware incidents, including detection, containment, eradication, and recovery.
* Assign roles and responsibilities for incident management to ensure accountability and swift action.

Incident Detection and Reporting:

* Implement mechanisms for detecting malware incidents, such as automated alerts from anti-malware tools or unusual activity monitoring.
* Encourage employees, contractors, and third parties to promptly report suspected malware incidents or anomalies.

Incident Classification and Prioritization:

* Assess and classify incidents based on their severity (e.g., critical, high, medium, low) and potential impact on organizational operations or data security.
* Prioritize responses to minimize damage to information assets and services.

Containment of Malware Incidents:

* Take immediate steps to isolate affected systems or devices to prevent the spread of malware across the network.
* Disable infected accounts, networks, or endpoints as needed to contain the threat.

Eradication of Malware:

* Use appropriate tools and techniques to remove malware from affected systems.
* Validate that all traces of malware have been eliminated before restoring systems to normal operation.

Communication and Escalation:

* Establish communication protocols to notify relevant stakeholders (e.g., management, IT teams, customers, or regulatory bodies) of malware incidents.
* Escalate high-severity incidents to external cybersecurity experts or law enforcement if necessary.

Evidence Collection and Forensics:

* Collect and preserve evidence related to the malware incident for further investigation, including legal or disciplinary actions.
* Perform forensic analysis to determine the malware's origin, attack vector, and vulnerabilities exploited.

Recovery Requirements

System Restoration:

* Restore systems, data, and services to operational status using clean backups or validated recovery processes.
* Ensure that restored systems are free from malware and vulnerabilities before reconnecting them to the network.

Backup Verification:

* Regularly test and verify the integrity of backups to ensure they can be used for recovery purposes.
* Maintain isolated, offline backups to minimize the risk of them being compromised by malware (e.g., ransomware).

Post-Incident Review:

* Conduct a post-incident review to analyze the effectiveness of the response and identify areas for improvement.
* Document lessons learned to refine incident response plans and strengthen defenses against future incidents.

Update Policies and Procedures:

* Update malware protection policies, incident response plans, and system configurations based on findings from the malware incident.
* Apply patches, updates, or configuration changes to prevent recurrence of the identified vulnerabilities.

Continuous Improvement:

* Use insights from incident response and recovery activities to improve malware detection, prevention, and response capabilities.
* Regularly test and review incident response and recovery plans to ensure ongoing readiness.

Training and Awareness

Incident Response Training:

* Train employees and IT teams on incident response procedures, including how to recognize and escalate malware incidents.
* Conduct simulated malware incident exercises (e.g., tabletop tests or penetration tests) to evaluate readiness.

Awareness of Recovery Procedures:

* Educate staff on the importance of following recovery protocols, such as using clean backups and avoiding premature reconnection of infected systems.

## Adaptation of Emerging Threats

The malware protection policy emphasizes the need for organizations to adapt to emerging threats in the constantly evolving threat landscape. Below are all the policy requirements to address and adapt to emerging threats:

Proactive Threat Intelligence

Monitor Emerging Threats:

* Continuously monitor the cybersecurity landscape for new malware types, attack vectors, and vulnerabilities through trusted threat intelligence sources.
* Subscribe to threat intelligence feeds, reports, and updates from industry bodies, vendors, and government agencies.

Threat Analysis and Interpretation:

* Analyze threat intelligence to understand how new malware or attack techniques could impact organizational systems.
* Integrate the findings into risk assessments to evaluate the likelihood and impact of emerging threats.

Security Updates and Patching

Regular Software Updates:

* Ensure operating systems, applications, and anti-malware tools are regularly updated to address vulnerabilities that could be exploited by new threats.
* Automate patch management processes where possible to ensure timely deployment of security patches.

Zero-Day Threat Preparation:

* Implement advanced security solutions (e.g., endpoint detection and response (EDR), intrusion detection systems (IDS)) capable of addressing zero-day malware threats.
* Use behavioral analysis tools to detect anomalies and prevent zero-day exploits.

Advanced Security Mechanisms

Behavioral-Based Detection:

* Deploy tools that use behavioral analysis and machine learning to detect new and unknown malware based on suspicious activities rather than relying solely on signatures.

Sandboxing and Isolation:

* Use sandboxing solutions to analyze and isolate suspicious files or programs in a safe environment to prevent potential harm to the system.

Encrypted Malware Inspection:

* Implement solutions capable of inspecting encrypted traffic to detect malware hidden within encrypted communications.

Incident Response for Emerging Threats

Update Incident Response Plans:

* Regularly update incident response procedures to include handling of new malware types or techniques.
* Train incident response teams to recognize and respond to emerging malware trends.

Testing and Simulations:

* Conduct regular security drills and simulations to test the organization's readiness to handle new threats, such as ransomware or advanced persistent threats (APTs).

Escalation to Experts:

* Establish escalation protocols to involve external cybersecurity experts or specialized teams to handle complex or previously unknown threats.

Awareness and Training

Employee Training on New Threats:

* Provide ongoing training to employees on the latest malware trends, such as phishing, ransomware, or social engineering tactics.
* Update awareness programs to include information on how to identify and avoid new attack methods.

IT and Security Staff Training:

* Train IT and security teams to use advanced tools and techniques for detecting and preventing emerging threats.
* Encourage participation in cybersecurity certifications and threat intelligence workshops.

Continuous Improvement

Review and Enhance Malware Protections:

* Regularly review and enhance malware detection tools to ensure they remain effective against emerging threats.
* Adjust malware protection policies and controls based on new risks identified from threat intelligence and incident reviews.

Collaboration and Information Sharing:

* Collaborate with industry peers, vendors, and cybersecurity organizations to share information on emerging threats and best practices.
* Participate in information-sharing platforms such as Information Sharing and Analysis Centers (ISACs) or sector-specific threat forums.

By implementing these requirements, organizations can stay ahead of emerging malware threats and ensure their malware protection measures remain effective in protecting critical information assets.

# Non-Compliance

Non-compliance with this policy can lead to serious security vulnerabilities, increasing the risk of unauthorized access to sensitive information.

Individuals who fail to adhere to the established guidelines may face disciplinary actions, which could include retraining, account suspension, or even termination, depending on the severity of the violation.

Furthermore, persistent non-compliance can undermine the organization's overall security posture, potentially exposing it to data breaches and legal liabilities, thereby affecting its reputation and trustworthiness in the industry.