TECH THAT MATTERS

Elevaite365

Antivirus Policy

Version 1.0

PURPOSE

This policy covers all Elevaite365 (hereby referred to as “organization”) business-critical information systems and/or process, store, or transmit the organization’s data. It applies to all employees, contractors, third-party entities, or other persons with authorized access to organization networks and system resources. This includes, but is not limited to, servers, desktops, laptops, mobile devices, network infrastructure, virtualization platforms, and removable media. The policy requirements are enforced globally across all geographic regions and business units where the organization operates.

SCOPE

This policy establishes the mandatory requirements to prevent, detect, respond to, and recover from malicious software (malware) threats across the organization’s technology landscape. By implementing a unified anti-malware framework, the organization ensures the confidentiality, integrity, and availability of its information assets, thus supporting both operational resilience and compliance with recognized security standards

DEFINITION

- **ISG**: Information security group
- **Malware**: Any malicious software intended to harm or exploit computer systems (e.g., viruses, worms, ransomware, trojans, spyware).
- **Real-Time Protection**: Continuous scanning of files, processes, and network traffic for suspicious or unauthorized activity.
- **Endpoint Detection and Response (EDR)**: An advanced security platform that identifies malicious activities on endpoints, allowing rapid investigation and containment.
- **Security Operations Center (SOC)**: The team or function responsible for continuous monitoring, threat detection, and incident response.

RESPONSIBILITIES

1. **Executive Management / Security Steering Committee**
    a. Provides strategic direction and adequate resources.
    b. Reviews major malware incidents and policy effectiveness.
2. **Chief Information Security Officer (CISO)**
    a. Owns the Anti-Malware Policy; oversees its alignment with the organization’s security strategy.
    b. Authorizes policy exceptions and escalates critical violations as necessary.
3. **IT Security / SOC**
    a. Deploys, configures, and maintains anti-malware solutions (e.g., antivirus, EDR).
    b. Investigates malware alerts; leads containment, eradication, and recovery efforts.
    c. Tracks key metrics (e.g., detection time, response time) and reports outcomes.
4. **IT Infrastructure / Operations**
    a. Ensures all systems receive timely security patches and updates.
    b. Coordinates scheduled scans; manages network and email gateway protections.
5. **All Employees and Contractors**

a. Must not disable or modify anti-malware settings.

b. Promptly report any suspected malware incident or abnormal system behavior

c. Complete mandatory security awareness training.

POLICY

Malware Prevention

1. **Mandatory Anti-Malware Software:**

   a. All computing devices (servers, workstations, mobile devices) must run approved anti-malware or EDR software with real-time scanning enabled.

   b. Devices not meeting minimum security standards shall be denied network access until they are brought into compliance.

2. **Automatic Updates:**

   a. Malware signatures and scanning engines shall update daily or as new critical releases become available.

   b. All endpoints must be configured to install updates automatically where feasible, with manual intervention required only for exceptional cases (e.g., critical business systems that demand controlled change windows).

3. **Network Protections:**

   a. The organization shall maintain email and web-filtering gateways to block malicious attachments, URLs, and domains.

   b. DNS filtering solutions should be deployed to prevent resolving known malicious or high-risk domains.

   c. Firewall rules and Intrusion Prevention Systems (IPS) must be regularly reviewed and tuned to minimize the attack surface.

4. **Least Privilege & Application Control:**

   a. Users should be granted only the privileges necessary to perform their duties, reducing the risk of malware escalating privileges.

   b. Allowlisting of approved applications may be enforced on critical servers to prevent unauthorized executable files from running.

Detection & Monitoring

1. **Scheduled Scanning:**

   a. A comprehensive security scan of all endpoints and servers should be conducted with minimal impact on business continuity and operational performance.

   b. Based on the results of risk assessments, high-risk or mission-critical servers may require daily or more frequent scanning schedules.

2. **Alerting & Triage:**

   a. Malware alerts generated by security tools shall be logged, correlated, and investigated immediately by the SOC/IT Security.

   b. Critical alerts (e.g., ransomware detection) must trigger an automated or on-call escalation process to expedite containment.

3. **Threat Hunting:**

   a. Periodic threat-hunting exercises leverage EDR, SIEM (Security Information and Event Management), and threat intelligence data to identify and contain hidden threats.

b. Adversary emulation or red teaming may be performed periodically to validate detection and response capabilities.

4. **Log Retention & Analysis:**

   a. All security-related logs (e.g., antivirus logs, EDR alerts, system event logs) must be retained for a minimum of 90 Days (or longer if regulatory requirements apply).

   b. Automated tools should parse logs for anomalous behaviors, enabling timely remediation.

Incident Response & Recovery

1. **Immediate Reporting:**

   a. Users must report any unusual pop-ups, encrypted files, suspicious network activity, or system slowdowns via the designated incident reporting channel (e.g., IT helpdesk, SOC hotline, ticketing system).

   b. Early detection is critical; employees are encouraged to err on the side of reporting rather than ignoring suspicious signs.

2. **Containment & Eradication:**

   a. The SOC isolates infected systems, removes malicious code, and verifies remediation before reconnecting systems to the network.

   b. Following chain-of-custody procedures, forensic images of compromised endpoints may be taken for legal or investigative purposes.

3. **Root Cause Analysis (RCA):**

   a. Significant malware incidents require documented RCA to refine policies, update signatures, and address any identified gaps.

   b. Post-incident reviews must include lessons learned, which should be integrated into awareness training and technical controls.

4. **Recovery & Continuity:**

   a. Critical data and systems backup must be performed regularly and stored securely (preferably offline or in read-only environments).

   b. Disaster Recovery (DR) testing should validate that restoration processes can be initiated quickly if widespread malware compromises occur.

Removable Media & External Sources

1. **Pre-Use Scanning:**

   a. All removable media (USB drives, external HDDs) must be scanned for malware before being used in the organization's systems.

   b. Auto-run/autoplay features on removable media should be disabled to mitigate automatic malware execution.

2. **Restricted Usage:**

   a. Using unauthorized removable media is prohibited; any exceptions require written approval from the CISO and compensating security controls (e.g., full-disk encryption dedicated scanning stations).

   b. Implement solutions that track and audit removable media usage in high-security areas to reduce the risk of data exfiltration or malware introduction.

3. **External File Sources:**

a. Files downloaded from external sources (e.g., internet, vendor portals) must be scanned upon receipt.

b. Cloud storage platforms should enable anti-malware scanning before allowing files to sync locally.

User Awareness & Training

1. **Mandatory Training:**

   a. All personnel must undergo initial and annual refresher training on malware risks, reporting procedures, and secure computing best practices (e.g., phishing avoidance).

   b. New hires must complete security training within their first 30 days of employment.

2. **Security Bulletins:**

   a. The IT Security Team may issue advisories about new malware trends or urgent patch requirements.

   b. Phishing simulations or interactive quizzes may be conducted periodically to reinforce user vigilance.

3. **Role-Based Training:**

   a. Employees in high-risk roles (e.g., finance, HR, executive leadership) may require enhanced training to recognize targeted (spear-phishing) attacks.

   b. Technical teams (e.g., developers and system admins) should receive specialized sessions on secure coding and system hardening.

Policy Compliance & Enforcement

1. **Audits & Reviews:**

   a. Periodic internal/external audits (e.g., SOC 2, ISO certifications) will assess adherence to this policy. Findings must be addressed promptly.

   b. Remediation plans must be documented and tracked to closure for any identified gaps or non-compliances.

2. **Disciplinary Measures:**

   a. Violations, including intentional disabling of anti-malware controls, may result in disciplinary action, including termination or contract cancellation.

   b. If applicable, repeat offenses or deliberate misuse may prompt legal action or referral to law enforcement.

3. **Exceptions:**

   a. Any policy exception must undergo a formal risk assessment and receive written approval from the CISO or delegate.

   b. Compensating controls must be in place to ensure risks introduced by the exception are mitigated effectively.

4. **Reporting to Stakeholders:**

   a. Regular compliance reports may be shared with executive management or the board, summarizing major incidents, policy violations, and remediation efforts.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan