ENDPOINT SECURITY POLICY

INLINE WITH ISO 27001:2022 & SOC 2

PREPARED BY :

MINISTRY OF MOS SECURITY

Document Management Information

Document Title:	Endpoint Security Policy
Document Number:	ORGANISATION-END-SEC-POL
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

CONTENTS

1. PURPOSE 4
2. SCOPE 4
3. TERMS AND DEFINITIONS 5
4. ROLES AND RESPONSIBILITIES 5
5. ENDPOINT SECURITY PRINCIPLES 6
6. APPROVED DEVICES AND OPERATING SYSTEMS 7
7. DEVICE AUTHENTICATION AND CONTROL 8
8. ENDPOINT CONFIGURATION AND HARDENING REQUIREMENTS 8
9. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES 9
10. PATCH AND VULNERABILITY MANAGEMENT 10
11. MALWARE PROTECTION AND ANTIVIRUS 10
12. CONTROL OF SOFTWARE INSTALLATION AND UPDATES 11
13. CONTROL OF INPUT/OUTPUT DEVICES AND REMOVABLE MEDIA 12
14. ENDPOINT DATA STORAGE SECURITY 13
15. ENCRYPTION REQUIREMENTS FOR ENDPOINTS 13
16. SECURING WEB BROWSERS 14
17. RESTRICTION ON EXTERNAL CONNECTIONS 15
18. ENDPOINT MONITORING AND DETECTIVE CONTROLS 15
19. DEVICE CAPACITY MONITORING AND MANAGEMENT 16
20. REMOTE AND BYOD ENDPOINT CONTROLS 17
21. PHYSICAL SECURITY OF ENDPOINTS 17
22. INCIDENT DETECTION AND RESPONSE FOR ENDPOINTS 18
23. ENFORCEMENT 19
24. POLICY EXCEPTIONS 19
25. ESCALATION MATRIX 20
26. REVIEW AND MAINTENANCE 20

1. PURPOSE

The purpose of this policy is to establish a standardized framework for securing all endpoint devices within the organization's IT environment. This includes laptops, desktops, mobile devices, servers, and any computing device that connects to the organization’s network or processes organizational data.

This policy defines technical and procedural controls to:

- Ensure that endpoint devices are protected from malware, unauthorized access, and data leakage.
- Minimize the risk of compromise due to configuration weaknesses or unauthorized applications.
- Align the organization's endpoint security posture with ISO/IEC 27001 controls and SOC 2 Type 2 requirements.

This document serves as a foundational component of the organization’s overall Information Security Management System (ISMS), supporting continuous risk reduction and cyber resilience.

2. SCOPE

This policy applies to all endpoint devices that access, process, or store organizational data or connect to the organization's network, cloud services, or information systems. This includes but is not limited to:

- Laptops, desktops, and workstations
- Mobile devices including smartphones and tablets
- Virtual machines, thin clients, and remote desktop systems
- Servers and application-specific endpoint devices
- Personally Owned Devices (BYOD), where permitted

It is applicable to:

- All employees, contractors, consultants, temporary staff, and third-party service providers
- All geographic locations and network zones where endpoints operate, including remote and hybrid environments
- All environments (e.g., production, development, testing, and staging)

This policy must be read and enforced in conjunction with related policies such as the BYOD Policy, Remote Access Policy, Information Security Policy, and Asset Management Policy.

3. TERMS AND DEFINITIONS

- **Endpoint**: Any device that connects to the organization's network or accesses organizational data, including laptops, desktops, mobile devices, servers, virtual desktops, and IoT devices.
- **Endpoint Protection Platform (EPP)**: Security solutions deployed on endpoint devices to prevent file-based malware, detect malicious activity, and provide investigation and remediation capabilities.
- **Endpoint Detection and Response (EDR)**: A security solution providing continuous monitoring and response to advanced threats on endpoints.
- **Device Hardening**: The process of securing a device by reducing its attack surface through configuration settings, patching, and disabling unnecessary services.
- **BYOD (Bring Your Own Device)**: Personally owned devices used to access corporate data or systems.
- **Malware**: Any software intentionally designed to cause damage to a computer, server, or network (e.g., viruses, worms, ransomware).
- **Removable Media**: Any portable storage device that can be attached to a system to read or write data (e.g., USB drives, CDs, external hard disks).
- **Administrative Privileges**: Elevated system access rights allowing users to make configuration changes, install software, or access restricted areas of a system.
- **Zero-Day Vulnerability**: A previously unknown software flaw exploited by attackers before the vendor becomes aware and issues a fix.

4. ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Information Security Officer (CISO)	Accountable for overall endpoint protection strategy, policy approval, and exception management.
Information Security Team	Responsible for designing endpoint security standards, reviewing logs, conducting risk assessments, and ensuring ongoing compliance.
IT Operations Team	Implements and maintains technical controls including EDR/EPP, patching, configuration management, and encryption enforcement on endpoints.

Line Managers	Ensure that team members are using only authorized endpoints and complying with all policy requirements. Report any deviations to Security or IT.
Asset Owners	Validate device compliance within their domains and provide approval for access to sensitive systems via managed endpoints.
Employees and Contractors	Required to comply with this policy, report incidents or violations, and use endpoints responsibly as per approved guidelines.
HR Department	Supports onboarding/offboarding workflows and triggers provisioning or revocation of endpoint access.

5. ENDPOINT SECURITY PRINCIPLES

1. Defence in Depth

Endpoint security must be implemented as part of a layered defence strategy, with coordinated controls at the device, network, application, and data layers to protect against malware, unauthorized access, and configuration drift.

2. Zero Trust Posture

All endpoints, regardless of location, must be treated as untrusted by default and must authenticate and be authorized before accessing organizational resources. Continuous verification and least privilege access principles must apply.

3. Secure by Default and Design

Endpoints must be configured securely from the time of provisioning, based on hardened baselines that disable unnecessary services and enforce strong security settings.

4. Standardization and Automation

Standard OS images, software configurations, and automation tools must be used for consistent endpoint setup, policy enforcement, and remediation.

5. Visibility and Monitoring

All endpoint activity must be continuously monitored using approved EDR or logging tools. Monitoring must support threat detection, investigation, and compliance.

6. Timely Updates and Responsiveness

Endpoints must be kept up-to-date with operating system patches, antivirus signatures, and security agent updates. Critical vulnerabilities must be addressed based on severity.

7. User Awareness and Responsibility

End-users must be made aware of their responsibility in keeping endpoints secure, including avoiding untrusted sources, reporting incidents, and complying with usage policies.

6. APPROVED DEVICES AND OPERATING SYSTEMS

1. Standardized Devices

Only devices that are owned, leased, or approved by [ORG NAME] shall be used to access, store, or process organizational data. All endpoints must be part of the asset inventory and managed through centralized systems.

2. Approved Operating Systems

- Only operating systems supported by the vendor and receiving regular security updates are permitted. These may include:
  - Microsoft Windows (supported editions)
  - macOS (latest two major versions)
  - Linux distributions (approved enterprise variants)
  - iOS and Android (latest two major versions for mobile endpoints)
- Deprecated or unsupported OS versions must not be used unless isolated with compensating controls and formally approved by the CISO.

3. Device Enrolment and Registration

- All devices must be enrolled in the organization's endpoint management platform (e.g., MDM/EMM/Intune/SCCM) before gaining access to the network.
- Asset tags, serial numbers, user assignment, and purpose must be captured in the central asset register.

4. Non-Standard or Specialized Equipment

- Use of specialized devices (e.g., kiosks, testing rigs, field equipment) must be risk assessed, approved by IT Security, and protected using equivalent controls.
- Exceptions must be formally documented and subject to periodic review.

7. DEVICE AUTHENTICATION AND CONTROL

1. Authentication Requirements

- All endpoints must support and enforce authentication mechanisms before allowing access to the device or the organization's network.
- Acceptable authentication methods include strong passwords, biometric authentication, and smart card-based logins, as applicable.

2. Centralized Identity Management

- Endpoint access must be integrated with centralized identity and access management systems (e.g., Active Directory, Azure AD) to ensure consistent access control and user identity verification.
- Single Sign-On (SSO) must be implemented wherever feasible to reduce password fatigue and enhance traceability.

3. Trusted Network Access

- Endpoints must not be allowed to connect to organizational systems unless they are authenticated and verified as trusted devices via endpoint compliance checks (e.g., device certificates, posture validation).

4. Lock Screen and Session Timeout

- Endpoints must auto-lock after a maximum of 10 minutes of inactivity.
- Users must re-authenticate to regain access after screen lock or session timeout.

5. Device Naming and Identification

- All endpoints must follow a standardized naming convention to enable easy identification and management in monitoring systems.

6. Device Revocation

- Devices that are lost, stolen, decommissioned, or non-compliant must have their access revoked immediately from all enterprise systems using centralized device management tools.

---

8. ENDPOINT CONFIGURATION AND HARDENING REQUIREMENTS

1. Baseline Configuration Standards

- All endpoints must adhere to hardened baseline configurations established by the Information Security Team. These baselines must reflect industry benchmarks (e.g., CIS, NIST) and be tailored to organizational needs.

   - Any deviation from baseline standards must be formally approved and documented.

2. **Unnecessary Services and Features**
   - Default and unnecessary services, ports, accounts, and protocols must be disabled.
   - Endpoint configurations must minimize the attack surface and eliminate unused components.

3. **Secure Boot and BIOS/UEFI Configuration**
   - Secure Boot must be enabled on all modern hardware to prevent unauthorized firmware or OS loading.
   - BIOS/UEFI must be password-protected and configured according to secure standards.

4. **Application Whitelisting**
   - Where technically feasible, only approved software applications should be permitted to execute on endpoints using application allowlisting tools.

5. **Configuration Drift Monitoring**
   - All endpoint configurations must be monitored for unauthorized or unexpected changes.
   - Alerts must be triggered for deviations from approved baselines.

---

9. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

1. **Privilege Assignment**
   - Administrative privileges must be assigned only to authorized personnel based on role-based access control (RBAC) principles.
   - Users must not operate endpoints under administrative accounts for routine tasks.

2. **Separate Administrative Accounts**
   - Privileged users must maintain separate admin and non-admin accounts. Admin accounts must be used strictly for administrative tasks.

3. **Just-in-Time (JIT) Privilege Access**
   - Where feasible, JIT access must be implemented to grant time-bound elevated privileges for critical operations.

4. **Monitoring and Logging**
    - All use of administrative privileges must be logged and regularly reviewed for unauthorized or suspicious activity.
5. **Privilege Review**
    - Privileged access rights must be reviewed at least quarterly.
    - Any excessive, redundant, or unnecessary privileges must be revoked and documented accordingly.

10. PATCH AND VULNERABILITY MANAGEMENT

1. **Mandatory Patching**
    - All endpoints must have operating systems, third-party software, security agents, and drivers regularly updated with the latest security patches.
    - Critical and high-severity vulnerabilities must be patched within 7 days or mitigated using compensating controls.
2. **Automated Patch Deployment**
    - Endpoint patching must be automated using centralized patch management tools. Manual patching may only be done in approved edge cases.
3. **Vulnerability Scanning**
    - Endpoints must be subject to periodic vulnerability scans using approved vulnerability management tools.
    - Findings must be tracked to closure with remediation timelines aligned to risk.
4. **Patch Compliance Reporting**
    - Monthly compliance reports must be generated and reviewed by the Information Security Team. Non-compliance must be escalated to respective system owners.
5. **Change Control**
    - All major patches or updates that may impact stability must follow formal change management procedures.

11. MALWARE PROTECTION AND ANTIVIRUS

1. **Mandatory Anti-Malware Controls**
    - All endpoint devices must have organization-approved antivirus or endpoint detection and response (EDR) software installed and running at all times.

  - The anti-malware solution must support real-time scanning, behavioural analysis, automatic remediation, and centralized logging.

2. **Automated Signature and Engine Updates**
    - Malware detection engines and threat signature databases must be configured to update automatically and at least once daily.
    - Devices found with outdated definitions must trigger alerts and be brought into compliance immediately.
3. **Active Threat Detection and Isolation**
    - Any device exhibiting malware-like behaviour or confirmed infection must be automatically isolated from the corporate network.
    - The Information Security Team must validate and coordinate remediation before rejoining the endpoint to the network.
4. **Remediation and Incident Management**
    - Confirmed malware incidents must follow the Incident Response Plan.
    - Logs must be preserved, root cause identified, and corrective actions implemented.
    - Re-imaging or data recovery procedures must follow secure handling protocols.
5. **End-User Awareness and Prevention**
    - Users must be trained to recognize malware symptoms, avoid risky behaviours (e.g., clicking unknown links or installing untrusted software), and report suspicious activity.
    - Phishing simulations and malware awareness modules must be included in periodic training.
6. **Audit and Efficacy Validation**
    - The Information Security Team shall conduct quarterly reviews of antivirus/EDR effectiveness, scan coverage, signature freshness, and incident metrics.
    - Results must be documented and used to improve detection and response strategies.

---

12. CONTROL OF SOFTWARE INSTALLATION AND UPDATES

1. **Authorized Software Only**
    - Installation of software on endpoints must be restricted to approved applications listed in the organization's software whitelist.

- Unauthorized software installations are strictly prohibited and must be removed immediately upon detection.

2. **Centralized Software Deployment**
   - Wherever feasible, software must be deployed using centralized configuration and deployment tools (e.g., SCCM, Intune) to ensure consistency and security.
3. **User Restrictions**
   - End users must not have permissions to install or update software without prior approval.
   - Installation rights, where granted temporarily for operational reasons, must be time-bound and monitored.
4. **Update Management**
   - All installed software must be updated regularly to the latest stable and secure versions.
   - Updates must be tested in staging environments before rollout to production endpoints, where applicable.
5. **Auditing and Remediation**
   - Endpoint software inventory must be reviewed monthly. Deviations from the approved list must be investigated and remediated.

---

13. CONTROL OF INPUT/OUTPUT DEVICES AND REMOVABLE MEDIA

1. **Removable Media Restrictions**
   - Use of USB drives, CDs, external hard drives, and other removable media is prohibited unless explicitly authorized for business purposes.
   - Where allowed, encryption of all removable media is mandatory.
2. **Device Control Software**
   - Endpoints must be equipped with device control agents to monitor and restrict the use of input/output ports (e.g., USB, Bluetooth).
   - Exceptions must be documented and approved by IT Security.
3. **Data Loss Prevention (DLP)**
   - DLP tools must be implemented to prevent unauthorized transfer of sensitive or regulated data via removable devices.
4. **Logging and Monitoring**

- All usage of removable media must be logged and subject to review by the Information Security Team.
- Any unauthorized use must be treated as a security incident.

5. **Disposal of Media**
   - Removable media containing sensitive data must be securely wiped or physically destroyed before disposal, following the Media Disposal Policy.

14. ENDPOINT DATA STORAGE SECURITY

1. **Local Data Storage Minimization**
   - Wherever feasible, data must not be stored locally on endpoints unless explicitly required for business needs.
   - Cloud storage, secure enterprise file shares, or virtual desktop infrastructure (VDI) must be preferred.
2. **Sensitive Data Classification**
   - Endpoints that process or store sensitive data must be configured based on data classification and corresponding security controls.
3. **Local Data Protection**
   - Endpoints authorized to store data locally must implement full-disk encryption and data protection tools.
   - Sensitive files must be protected with additional access controls, including document-level encryption where applicable.
4. **Backup and Recovery**
   - Critical endpoint data must be backed up regularly to secure, managed backup systems. Backups must be encrypted and tested periodically for recovery integrity.

---

15. ENCRYPTION REQUIREMENTS FOR ENDPOINTS

1. **Full-Disk Encryption (FDE)**
   - All corporate-managed endpoints, including laptops and desktops, must have full-disk encryption enabled using enterprise-approved encryption software.
2. **Mobile Device Encryption**
   - Mobile devices (smartphones, tablets) used for accessing corporate data must have device-level encryption enabled and enforced via MDM.

3. Removable Media Encryption

- All data written to removable media (e.g., USB drives, SD cards) must be encrypted using organizational tools or approved solutions.
- Unencrypted media must not be used to store or transport corporate data.

4. Encryption Key Management

- Encryption keys must be stored securely, managed centrally, and protected against unauthorized access. Key rotation and revocation procedures must be defined.

5. Verification and Compliance

- Periodic audits must be conducted to verify encryption compliance across all endpoint categories. Non-compliant devices must be remediated or access restricted.

---

16. SECURING WEB BROWSERS

1. Approved Browsers and Configuration

- Only organization-approved browsers are allowed on endpoints. Browsers must be configured according to secure baselines that disable risky features (e.g., Java, Flash).

2. Extension and Plugin Control

- Installation of browser extensions must be restricted. Only vetted and whitelisted extensions required for business use shall be permitted.

3. Safe Browsing Settings

- Security settings such as pop-up blocking, phishing protection, safe browsing modes, and script control must be enabled.

4. Regular Updates

- Browsers must be updated automatically or through centralized tools to patch vulnerabilities.

5. Monitoring and Logging

- Access to high-risk websites and anomalies in browsing behaviour must be logged and monitored by IT Security.

---

17. RESTRICTION ON EXTERNAL CONNECTIONS

1. Internet Access Control

- Endpoints must access the internet only through the organization's secure web gateways or proxies. Direct connections to the internet are not permitted.

2. Blocking Unauthorized Tunnels

- Use of external tunnelling protocols (e.g., SSH tunnels, VPNs) not authorized by the organization is strictly prohibited.

3. Wireless Network Restrictions

- Connecting to public or unsecured wireless networks using corporate devices is prohibited unless tunnelled through a secure organization-approved VPN.

4. Peer-to-Peer (P2P) and External Sharing

- Peer-to-peer file sharing software and unauthorized file transfer tools are not permitted. File sharing must occur through approved cloud services with access control and logging.

5. Network Isolation

- High-risk endpoints must be logically isolated or segmented to restrict lateral movement in case of compromise.

---

18. ENDPOINT MONITORING AND DETECTIVE CONTROLS

1. Centralized Monitoring Tools

- All endpoints must be monitored using centralized Endpoint Detection and Response (EDR) or Security Information and Event Management (SIEM) systems approved by the Information Security Team.

2. Real-Time Alerting

- The EDR/SIEM system must be configured to generate real-time alerts for suspicious or unauthorized activities such as:
  - Installation of unauthorized software
  - Use of administrative privileges
  - Disabling of security tools
  - Indicators of compromise (IOCs)

3. Anomaly Detection

- Behavioural baselines should be established where feasible to detect anomalies in endpoint behaviour that could indicate malware, insider threats, or lateral movement.

4. Log Retention and Integrity

- Logs must be retained for at least 12 months and protected from unauthorized modification. Access to logs must be limited to authorized personnel.

5. Periodic Review

- Security analysts must review endpoint logs and alerts at least weekly. High severity alerts must be escalated immediately in accordance with the Incident Response Plan.

---

19. DEVICE CAPACITY MONITORING AND MANAGEMENT

1. Hardware Health Monitoring

- Endpoint capacity metrics such as CPU usage, memory, disk utilization, and battery health (for mobile devices) must be monitored using IT management tools.

2. Thresholds and Alerts

- Thresholds for resource usage must be defined (e.g., disk space below 10%) and alerts configured to notify the IT Operations Team for remediation.

3. Capacity Planning

- Capacity trends must be reviewed quarterly to support procurement and hardware upgrade planning.

4. Proactive Maintenance

- Devices that consistently operate beyond capacity thresholds must be investigated for optimization or scheduled for upgrade.

5. Inventory Accuracy

- Monitoring data must be reconciled with the asset inventory to ensure device records remain current and complete.

---

20. REMOTE AND BYOD ENDPOINT CONTROLS

1. **Remote Device Requirements**
    - All remote devices used to access organizational systems must comply with the same endpoint protection standards as on-premise devices.
    - Mandatory controls include full-disk encryption, anti-malware software, VPN access, and endpoint configuration hardening.
2. **Secure Access Channels**
    - Remote endpoints must connect through secure, organization-approved VPNs or virtual desktop infrastructure (VDI) solutions with MFA enforcement.
3. **Mobile Device Management (MDM)**
    - All BYOD and mobile devices must be enrolled in the organization's MDM solution. MDM must enforce encryption, remote wipe, password policies, and app control.
4. **Segregation of Corporate and Personal Data**
    - BYOD devices must implement secure containers or profiles to logically separate organizational data from personal content.
5. **Revocation of Access**
    - Remote/BYOD device access must be immediately revoked in the event of termination, loss, or policy non-compliance.
6. **User Consent and Awareness**
    - All BYOD users must sign an acknowledgment form agreeing to monitoring, control, and security requirements before being granted access.

---

21. PHYSICAL SECURITY OF ENDPOINTS

1. **Workplace Security**
    - Endpoints must be physically secured when unattended in open or public areas. Use of cable locks, locked drawers, and privacy screens is strongly recommended.
2. **Travel and Remote Work Protocols**
    - When traveling or working remotely, users must ensure that endpoints are never left unattended in vehicles, hotels, or public places without physical safeguards.

3. **Theft or Loss Reporting**
    - Lost or stolen endpoint devices must be reported immediately to the IT Helpdesk and Information Security Team. A formal incident report must be filed.
4. **Physical Access Restrictions**
    - Access to server rooms, storage areas, and other locations where endpoints are maintained must be restricted to authorized personnel.
5. **Asset Disposal**
    - Endpoints must be securely wiped or physically destroyed prior to decommissioning or disposal in accordance with the Media Disposal Policy.

22. INCIDENT DETECTION AND RESPONSE FOR ENDPOINTS

1. **Detection Integration**
    - Endpoint alerts from antivirus, EDR, DLP, or system logs must be integrated with the organization’s central SIEM system for correlation and automated threat detection.
2. **Incident Classification**
    - Security events on endpoints must be classified based on severity and mapped to predefined incident categories under the Incident Response Plan.
3. **Containment and Eradication**
    - Compromised endpoints must be isolated from the network, and forensic analysis initiated to identify the root cause and affected systems.
    - Infected files must be quarantined and malware removed before restoring systems.
4. **Notification and Escalation**
    - All confirmed endpoint incidents must be reported to the CISO and escalated based on the defined escalation matrix and SLA.
5. **Post-Incident Review**
    - A root cause analysis must be conducted for major endpoint-related incidents. Lessons learned must be documented and used to improve controls.

23. ENFORCEMENT

1. Policy Compliance

- All users and administrators are required to comply with this policy. Violations may result in disciplinary action including revocation of access, HR sanctions, or legal proceedings.

2. Monitoring and Auditing

- Endpoints are subject to periodic audits and continuous monitoring. Unauthorized configurations, software, or usage may be flagged and remediated.

3. Non-Compliance Handling

- Repeated or intentional violations shall be formally investigated. Evidence will be collected, and enforcement actions will be documented by the Information Security Team.

---

24. POLICY EXCEPTIONS

1. Request Procedure

- Exception requests must be submitted via the formal Exception Request Form and must include:
  - Justification
  - Compensating controls
  - Duration of exception
  - Approval from IT, Information Security, and CISO

2. Validity and Review

- Exceptions must be time-bound and reviewed at least quarterly. All active exceptions must be recorded in the Exception Register.

---

25. ESCALATION MATRIX

Escalation Level	Role/Designation	Responsibility	Contact Mode
Level 1	Reporting Manager / Team Lead	First-level support for endpoint issues	Email / Ticketing Tool
Level 2	IT Operations Team	Technical resolution of endpoint controls	Internal support channel
Level 3	Information Security Officer	Security review, escalation & risk validation	Email / Escalation Tool
Level 4	Chief Information Security Officer	Final authority for endpoint policy enforcement	Direct escalation

26. REVIEW AND MAINTENANCE

1. **Policy Ownership**
   - The CISO is the owner of this policy and responsible for its annual review, alignment to standards, and updates based on risk changes.
2. **Revision Frequency**
   - This policy must be reviewed at least annually or upon significant technology, threat, or organizational changes.
3. **Distribution**
   - Updated versions must be communicated to all stakeholders and published in the official document repository.