## **ISO 27001 Endpoint Policy Template**

### **1. Introduction**

This document outlines the Endpoint Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes measures to secure endpoints, including laptops, desktops, mobile devices, and other hardware, to protect organizational assets and information.

### **2. Purpose**

The purpose of this policy is to:

1. Define security requirements for endpoints used within the organization.
2. Prevent unauthorized access, malware infections, and data breaches through endpoint security measures.
3. Ensure compliance with ISO 27001 and applicable regulations.

### **3. Scope**

This policy applies to all endpoints used to access [Organization Name]’s networks, systems, or data. It includes:

* Desktops, laptops, and tablets.
* Mobile devices (e.g., smartphones).
* Removable storage devices (e.g., USB drives).
* Internet of Things (IoT) devices.

### **4. Policy Statement**

[Organization Name] requires all endpoints to adhere to stringent security controls, ensuring the protection of organizational information and systems. This includes:

1. Implementing encryption for data stored on endpoints.
2. Enforcing secure authentication mechanisms, including multi-factor authentication.
3. Regularly updating and patching endpoint operating systems and software.
4. Ensuring regular endpoint backups to enable data recovery in case of device failure or loss.

### **5. Roles and Responsibilities**

1. **Employees and Contractors:** Comply with endpoint security practices and report lost, stolen, or compromised devices immediately.
2. **IT Department:** Manage endpoint security, including device configuration, patching, and monitoring.
3. **Information Security Officer (ISO):** Oversee endpoint security policies and ensure compliance with ISO 27001 requirements.

### **6. Compliance and Monitoring**

1. Conduct regular endpoint audits to verify compliance with this policy.
2. Monitor endpoints for unauthorized activities or configuration changes.
3. Implement tools for endpoint detection and response (EDR) to identify and mitigate threats.

### **7. Related Documentation**

1. Acceptable Use Policy
2. Mobile Device Management Policy
3. Incident Management Policy

### **8. Review and Revision**

This policy will be reviewed annually or whenever significant changes occur in the endpoint environment or regulatory requirements. Updates will be coordinated by the Information Security Officer.

### **Appendix A: Endpoint Security Checklist**

| **Endpoint Type** | **Security Measure** | **Compliance Status** |
| --- | --- | --- |
| Laptops | Full-disk encryption enabled |  |
| Mobile Devices | Multi-factor authentication configured |  |

### **Appendix B: Endpoint Incident Report Template**

| Incident ID | Date/Time | Affected Endpoint | Description of Incident | Actions Taken | Resolution Status |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

### 

### 

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the Endpoint Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_