

Mapping Security Policies to ISO 27001 Operational Capabilities

This is a mapping of 50 common security policies with the operational capabilities from ISO/IEC 27001. Use this to ensure alignment and comprehensive coverage of your security policy framework.

~~~~~

### 1. Governance

- Information Security Policy
- Security Governance Policy
- Risk Management Policy
- Segregation of Duties Policy

### 2. Asset Management

- Asset Management Policy
- Intellectual Property Protection Policy

### 3. Information Protection

- Data Protection Policy
- Encryption Policy
- Data Classification Policy
- Data retention policy
- Data leakage prevention policy
- Acceptable use policy (AUP)
- Social media policy
- Internet usage policy
- Email security policy

### 4. Human Resource Security

- Personnel security policy
- Security training and awareness policy
- Visitor access policy

## **5. Physical Security**

- Physical security policy
- Environmental security policy

## **6. System and Network Security**

- Network security policy
- Endpoint security policy
- Wireless security policy
- Cloud security policy

## **7. Application Security**

- Application security policy
- Secure development policy

## **8. Secure Configuration**

- Configuration management policy
- Change management policy
- Software installation policy

## **9. Identity and Access Management**

- Access control policy
- User authentication policy
- User account management policy
- Mobile device policy
- Bring your own device (BYOD) policy

## **10. Threat and Vulnerability Management**

- Vulnerability management policy
- Patch management policy
- Malware and antivirus policy

## **11. Continuity**

- Disaster recovery policy
- Backup policy

## **12. Supplier Relationships Security**

- Supplier security policy
- Third-party security policy

## **13. Legal and Compliance**

- Compliance policy
- Privacy policy

## **14. Information Security Event Management**

- Incident response policy
- Data breach response policy
- Incident reporting policy
- Security monitoring policy

## **15. Information Security Assurance**

- Log management policy
- Security audit policy