

Introduction to Security Policies and Procedures

Introduction to Security Policies and Procedures
Key concepts, purpose, components, and best-practice guidelines

1. What Is a Security Policy?

Aspect	Description
Definition	A formal, high-level document that states an organization's security objectives, principles, and rules for protecting information assets.
Scope	Applies to people, processes, technology, and physical environments across the entire enterprise (or specific business units).
Audience	Executives, managers, employees, contractors, and third-party partners.
Characteristics	Concise, authoritative, approved by senior management, and reviewed regularly (usually annually).

Why It Matters

- Provides a **baseline** for consistent decision-making.
- Demonstrates **compliance** with regulations (e.g., GDPR, HIPAA, PCI-DSS).
- Reduces risk by defining **acceptable behavior** and **responsibilities**.
- Serves as a reference for **incident response**, audits, and training.

2. Types of Security Policies

Policy Type	Focus	Typical Content
Enterprise-wide (master) policy	Overall security philosophy	Vision, governance structure, risk management approach
Issue-specific policies	Particular domains	Acceptable Use, Password, Mobile Device, Remote Access
System-specific policies	Individual platforms	Server hardening, Database encryption, Cloud service usage
Regulatory-specific policies	Legal requirements	HIPAA Privacy, PCI-DSS Cardholder Data Protection

Introduction to Security Policies and Procedures

3. Core Components of a Security Policy

1. **Purpose & Objectives** – Why the policy exists and what it aims to protect.
 2. **Scope & Applicability** – Who/what is covered (employees, contractors, locations, systems).
 3. **Definitions** – Clarify terminology (e.g., “confidential data”, “incident”).
 4. **Policy Statements** – Mandatory rules and controls (e.g., “All passwords must be at least 12 characters”).
 5. **Roles & Responsibilities** – Ownership for enforcement, monitoring, and compliance.
 6. **Compliance & Enforcement** – Consequences for violations and audit mechanisms.
 7. **Review & Revision Cycle** – Frequency of updates and change management process.
 8. **References** – Linked standards, legal requirements, and supporting procedures.
-

4. What Are Security Procedures?

Aspect	Description
Definition	Detailed, step-by-step instructions that implement the high-level policy statements.
Level of Detail	Operational; includes specific commands, forms, contacts, and escalation paths.
Audience	Personnel performing the tasks (e.g., IT staff, helpdesk agents, end users).
Lifecycle	Created, tested, approved, disseminated, and periodically refreshed.

Relationship to Policies

- **Policies** = “What must be done.”
- **Procedures** = “How it is done.”

A policy may reference multiple procedures; a single procedure may support several policies.

5. Typical Security Procedures

Procedure	Trigger	Key Steps
-----------	---------	-----------

Introduction to Security Policies and Procedures

User Account Provisioning

New hire or role change

1. HR notifies IT.
2. Create account per least privilege principle.
3. Assign to appropriate groups.
4. Document and notify user.

Password Reset

Forgotten password or compromise

1. Verify identity.
2. Reset via secure admin console.
3. En