

Introduction to Cyber Security Policies and Procedures

Introduction to Cyber Security Policies and Procedures

Purpose: Provide a concise, easy-to-read guide for newcomers to cyber security governance.

1. Why Policies & Procedures Matter

Reason	What It Achieves
Risk Management	Identifies, assesses, and mitigates threats before they cause damage.
Regulatory Compliance	Meets legal requirements (e.g., GDPR, HIPAA, PCI-DSS).
Consistent Behavior	Ensures every employee follows the same security baseline.
Incident Response	Provides a clear, rehearsed path for handling breaches.
Auditability	Creates documented evidence for internal/external auditors.

2. Core Components of a Cyber Security Policy Suite

Component	Typical Content	Owner
1. Information Security Policy (ISP)	High-level vision, scope, objectives, governance structure.	Executive Management / CISO
2. Acceptable Use Policy (AUP)	Rules for using corporate IT assets, internet, mobile devices.	IT / HR
3. Access Control Policy	Role-based access, least-privilege, authentication standards.	Security Operations
4. Data Classification & Handling	Classification levels (public, internal, confidential, restricted) and handling procedures.	Data Governance
5. Incident Response Policy	Roles, communication flow, escalation matrix, post-mortem process.	Incident Response Team
6. Business Continuity / Disaster Recovery (BC/DR) Policy	Recovery time objectives (RTO), recovery point objectives (RPO), backup strategy.	Continuity Planning

Introduction to Cyber Security Policies and Procedures

Component	Typical Content	Owner
7. Vendor / Third-Party Security Policy	Due-diligence, contractual clauses, monitoring of suppliers.	Procurement / Legal
8. Password & Authentication Policy	Complexity, rotation, multi-factor authentication (MFA) requirements.	Security Operations
9. Remote Access / VPN Policy	Secure tunneling, device health checks, split-tunnel rules.	Network Engineering
10. Security Awareness & Training Policy	Frequency of training, content topics, testing methods.	HR / Security Awareness Team

3. Relationship Between Policies & Procedures

Level	Description	Example
Policy	<i>What</i> must be achieved; high-level, non-technical.	"All privileged accounts must use MFA."
Procedure	<i>How</i> to implement the policy; step-by-step, technical.	"Procedure to enroll a user in the corporate MFA system."
Standard	Specific, measurable requirement supporting a policy.	"Passwords must be at least 12 characters, include upper-case, lower-case, numbers, and symbols."
Guideline	Recommended best practices; flexible.	"Use passphrases where possible for easier memorization."

Policies set the rule; procedures describe the exact actions needed to follow that rule.

4. Developing Effective Policies

1. Stakeholder Involvement

- Identify owners (business unit leads, IT, legal).
- Conduct workshops to capture requirements and concerns.

2. Risk-Based Scope

Introduction to Cyber Security Policies and Procedures

- Perform a quick risk assessment to prioritize coverage.
- Align policy depth with the organization's risk appetite.

3. Clear, Concise Language

- Use plain English; avoid jargon.
- Define all acronyms and technical terms in a glossary.

4.