

Information Security Policy Set

Build a governed information security policy set using the policy records and implementing forms below. Enter approved requirements, technical values and evidence. Map a policy to an external framework only after its applicability and control reference have been reviewed.

Complete bracketed fields with approved information. Duplicate modules and rows as needed; record the reason for any section marked not applicable.

Document [ID and revision] **Owner** [Role] **Scope** [Organization, site or product]

Effective date [Date] **Approval** [Controlled record] **Next review** [Date or trigger]

Policy framework and governance

Framework element	Organization decision
Scope and applicability	[People, information, systems, locations and exclusions]
Document hierarchy	[Governing policy, topic policies, standards, procedures and guidance]
Adopted references	[Framework or requirement, version, applicable scope and authority]
Policy set index	[Topic, policy ID, owner role and controlled location]

Governing information security policy

Policy element	Approved statement or reference
Purpose and security objectives	[Confidentiality, integrity and availability objectives as adopted]
Principles and commitments	[Exact approved management commitments]
Obligation and compliance	[Who must do what; preserve must, should and may]
Related standards and procedures	[Controlled documents that implement the policy]

Security responsibilities

Role	Accountability and authority	Handoff and segregation
[Management or security function]	[Policy approval and oversight]	[Conflicts and independent review]
[Asset owner or personnel]	[Classification, access or reporting duty]	[Decision route and escalation]

Organizational policies

Repeat this topic-policy record for each approved policy. Keep separate topics independently reviewable.

Policy field	Complete for one topic	
Title purpose and scope	[Policy ID, subject, assets and audience]	
Policy statements	[Numbered approved rules with exact obligation strength]	
Roles and exceptions	[Performer, decision rights and exception route]	
Implementing documents	[Standards, procedures, evidence and control mapping]	
Organizational topic	Policy record and decision	Evidence or open work
[Risk, assets, classification or acceptable use]	[Policy ID and applicability]	[Approval or gap]
[Access, transfer, suppliers or cloud]	[Policy ID and applicability]	[Approval or gap]
[Incidents, continuity or legal duties]	[Policy ID and applicability]	[Approval or gap]

People security policies

Lifecycle point	Approved rule and policy	Check and retained record
Before access	[Screening, terms and confidentiality]	[Authorized verification]
During engagement	[Training, remote work and conduct]	[Acknowledgement and review]
Change or exit	[Access and asset responsibilities]	[Completion evidence]

Physical security policies

Area or asset	Required protection	Policy and verification
[Restricted area or equipment]	[Entry, handling, clear-screen or storage rule]	[Policy ID and evidence]
[Media or disposal route]	[Approved reuse or disposal requirement]	[Record and review]

Technological policies

Enter adopted values and units without replacing them with illustrative defaults.

Control area	Requirement and exact value	Scope and evidence
[Authentication or privileged access]	[Rule, parameter and unit]	[System, standard and verification]
[Encryption or key management]	[Approved specification and lifecycle]	[System and evidence]
[Backup logging or retention]	[Coverage, value, unit and condition]	[Record and restore or review test]
[Vulnerability patching or change]	[Rule, timing basis and authorization]	[Policy, exception and evidence]

Implementing procedures

Access or policy exception request

1. Identify [asset], [requester role], [required access or exception] and the governing [policy ID].
2. Record [business reason], [risk], [compensating control] and [requested duration].
3. Obtain the [specified authority] decision before the controlled action.
4. Record [implementation], [verification], [expiry or revocation] and [closure evidence].

Procedure check	Result and evidence	Reviewer
Request and authorization match the policy	[Result and record]	[Role and date]
Granted access or exception is verified	[Test and outcome]	[Role and date]
Review expiry or revocation is scheduled	[Approved trigger and record]	[Role and date]

Policy administration and reference

Exception and enforcement register

Policy and exception ID	Approval and safeguards	Expiry review and closure
[Rule, affected scope and reason]	[Authority, decision and compensating controls]	[Date or trigger, evidence and status]

Policy lifecycle and acknowledgement

Lifecycle activity	Responsible role and trigger	Record
Approval and publication	[Authority and release decision]	[Version and controlled link]
Staff acknowledgement	[Audience and adopted requirement]	[Completion and gaps]
Review and withdrawal	[Cycle, change trigger and owner]	[Review result and replacement]

Control mapping and staff questions

Policy statement	Adopted framework reference	Evidence and mapping review
[ID and exact requirement]	[Framework, edition and control; if applicable]	[Evidence and reviewer]
Staff question	Approved answer and governing policy	Last verified
[Question]	[Direct answer; policy link]	[Role and date]

Definitions and release check

Term or classification	Approved meaning and handling	Source
[Term]	[Meaning and applicable rule]	[Controlled source]

☐ Policy topics, implementing procedures and standards are linked and independently identifiable.

☐ Technical values, exception authorities and acknowledgements have been reviewed.

Reviewer role	Date and decision	Open actions and approval reference
[Role]	[Approved or returned]	[Record and action owner]