

Information Security Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy sets out how [Company name] (the "Company") runs its information security program: who owns it, which policies sit under it, how management oversees it and how it is kept current. It supports the SOC 2 common criteria CC1.1, CC1.3 and CC2.2.

This policy applies to all [In-scope personnel] and [In-scope systems]. Where a topic policy listed in section 6 is more specific, the topic policy applies.

2. Security objectives

The security program exists to meet these objectives, and every policy under it serves at least one of them.

- Protect customer data from unauthorized access, change and loss.
- Keep the service available enough to meet the commitments made to customers.
- Meet the security obligations in customer contracts and applicable law.
- Find and fix weaknesses before they are exploited, and learn from incidents when they happen.

3. Management commitment and oversight

The security program, including its policies, controls and risk assessment results, is reviewed, updated and formally approved by the [Policy approver role] at least once a year.

The [Management review body] meets at least once a year to oversee the security program, business strategy and risks. Meeting minutes are kept as evidence. The [Security owner role] reports to it at least twice a year on open risks, control deficiencies and their remediation, incidents, and the results of recurring reviews.

4. Security roles

Role	Held by	Core responsibilities
Executive sponsor	[Policy approver role]	Sets the tone for security, approves policies and risk acceptance, provides resources, and receives security reporting at least twice a year.
Security and compliance owner	[Security owner role]	Runs the security program day to day: maintains policies, runs risk assessments and access reviews, leads incident response, manages the audit, and tracks remediation.
Engineering lead	[Engineering owner role]	Owns the security of the Company's product and the production cloud environment: secure development, change management, vulnerability remediation, logging, backups and recovery.
IT lead	[IT owner role]	Owns corporate systems and devices: account provisioning and removal, device encryption and updates, endpoint protection, and administration of the software services the Company subscribes to.
People lead	[People owner role]	Owns the people side of security: background checks, onboarding and offboarding notices, policy acknowledgments, training records and disciplinary process.
All personnel	Everyone	Follow Company policies, complete training, protect credentials and data, and report suspected incidents within 1 hour.

At a company of this size one person often holds more than one role. That is acceptable, provided each role has a named holder and no one approves their own access or reviews their own work.

5. Responsibility matrix

R = Responsible (does the work). A = Accountable (owns the outcome and signs off; exactly one per activity). C = Consulted (gives input before the work is done). I = Informed (told of the result).

Activity	Frequency	Executive	Security owner	Engineering	IT	People
User access reviews	As set in the Access Control Policy	I	A	R	R	I

Activity	Frequency	Executive	Security owner	Engineering	IT	People
Onboarding and offboarding of accounts	Each joiner and leaver	I	A	R	R	R
Vendor security reviews	As set in the Vendor Management Policy	I	A, R	C	C	I
Incident response	Each incident	C	A, R	R	R	C
Policy approval	Yearly	A	R	C	C	C
Risk assessment	As set in the Risk Assessment Policy	A	R	C	C	C
Vulnerability remediation	As set in the Vulnerability Management Policy	I	A	R	R	I
Backup restore testing	As set in the Business Continuity and Disaster Recovery Plan	I	A	R	I	I
Security awareness training	As set in the Security Awareness Training Policy	I	A, R	C	I	R

Where the frequency names a topic policy, that policy sets it, so the two documents cannot disagree.

Where one person holds two roles in the same row, a different person performs the review or approval.
For access reviews, no one reviews their own access; the [Policy approver role] reviews the access of the security owner.

6. Policy framework

The policies below sit under this one. Each names its owner, is approved by the [Policy approver role] and is reviewed at least once a year.

Policy	What it covers	Criteria
Access Control Policy	Accounts, authentication, least privilege and access reviews	CC6.1, CC6.2, CC6.3
Acceptable Use Policy	Use of company systems, accounts, devices and data	CC1.1, CC1.5
Change Management Policy	How code and infrastructure changes are reviewed, tested and released	CC8.1
Vendor Management Policy	Assessing, contracting with and monitoring third parties	CC9.2
Data Classification and Retention Policy	Classification levels, handling, retention periods and disposal	CC6.1, CC6.5
Encryption Policy	Encryption at rest and in transit, keys and certificates	CC6.1, CC6.7
Business Continuity and Disaster Recovery Plan	Recovery targets, backups, restore tests and failover	CC7.5, CC9.1
Risk Assessment Policy	The annual risk assessment, the risk register and treatment	CC3.1, CC3.2, CC3.3, CC3.4
Vulnerability Management Policy	Scanning, fix deadlines, patching and network protections	CC6.6, CC7.1
Logging and Monitoring Policy	What is logged, how long it is kept, alerting and review	CC7.1, CC7.2
Security Awareness Training Policy	Screening, training, acknowledgments and discipline	CC1.4, CC1.5
Incident Response Plan	Severity, roles, notification and post-incident review	CC7.3, CC7.4, CC7.5

7. Communication and acknowledgment

- Policies are published where all personnel can read them, in [Documentation system].
- Security roles and responsibilities are documented in job descriptions and explained during onboarding and annual training.

- New personnel acknowledge this policy and the policies that apply to them before or on their first day. Everyone acknowledges the current versions once a year.
- Control deficiencies are recorded with an owner and a due date and tracked until closed.

8. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Signed role acknowledgments	Each role holder accepts the role in section 4.	[Evidence storage location]
Policy acknowledgment log	Who acknowledged which policy version, and when.	[Evidence storage location]
Management review minutes	The oversight meetings in section 3, with the report presented.	[Evidence storage location]

9. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

10. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

11. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Management review body]	The group that oversees security, for example the leadership team meeting or an advisory board.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.

Field	What to enter
[In-scope personnel]	Who the policy covers, for example employees and contractors with access to company systems.
[In-scope systems]	The product, cloud accounts and tools inside the audit boundary.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[IT owner role]	The role that runs company devices and accounts, for example IT lead.
[People owner role]	The role that runs hiring and departures, for example head of people.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/information-security-policy (CC BY 4.0).