

Information Security Policy

Purpose

This is the top-level information security policy for Your Organization. It articulates the commitment of Your Organization's leadership to protecting the confidentiality, integrity, and availability of information entrusted to it, defines the security objectives that drive the Your Organization Information Security Management System (ISMS), and establishes the authority under which all subordinate security policies, standards, and procedures are issued.

Scope

This policy applies to all Your Organization information assets, in any form and at any location; to every workforce member, contractor, and third party that handles Your Organization information; and to every information system used to store, process, or transmit that information — on-premises, cloud, endpoint, and mobile.

Objectives

Your Organization maintains an information security program to:

- Protect the confidentiality of information commensurate with its classification.
- Preserve the integrity of systems and data against unauthorized or unintended modification.
- Maintain availability of systems and data sufficient to meet business and contractual commitments.
- Comply with applicable laws, regulations, and contractual obligations.
- Identify, assess, and treat information security risk on an ongoing basis.
- Detect, respond to, and recover from security incidents with minimal harm.
- Maintain the trust of customers, partners, and the workforce.

Leadership commitment

Senior leadership at Your Organization is accountable for the information security program. Leadership commits to:

- Approving this policy and the subordinate security policies that implement it.
- Providing the resources (budget, people, tooling) the program requires.
- Setting measurable objectives and reviewing program performance at least annually.
- Holding the organization accountable for policy compliance and continuous improvement.

Governance

- **CISO (or designated security leader).** Owns the ISMS day to day. Issues subordinate policies, standards, and procedures. Reports program status to executive leadership and, where applicable, to the

board.

- **Security Steering Committee.** Cross-functional group that reviews risks, approves exceptions, prioritizes remediation, and ratifies policy changes.
- **Data and System Owners.** Accountable for the classification of their data and for the secure operation of their systems within policy.
- **Workforce members.** Responsible for following security policies, completing assigned training, and reporting suspected incidents.

Policy framework

This policy is implemented by a set of subordinate policies, each of which may carry its own review cadence and ownership:

- Access Control Policy
- Password and Authentication Policy
- Data Classification Policy
- Data Retention Policy
- Acceptable Use Policy
- Incident Response Plan
- Business Continuity Policy
- Change Management Policy
- Vendor Risk Management Policy
- Additional technical and operational policies as the program matures.

Subordinate policies must not conflict with this policy; where a conflict is identified, this policy governs until the subordinate is reconciled.

Risk management

Your Organization operates a recurring risk management cycle: identify assets and threats, assess likelihood and impact, treat risk by mitigation / transfer / acceptance / avoidance, and monitor residual risk. Risk decisions are documented in the risk register and reviewed at least quarterly by the Security Steering Committee.

Compliance

Your Organization maintains compliance with applicable laws, regulations, and contractual security obligations. Compliance gaps are tracked in the remediation register and reported to leadership.

Training and awareness

All workforce members complete security-awareness training on hire and at least annually thereafter. Role-specific training is provided to engineers, administrators, and anyone handling Restricted data.

Enforcement

Violations of this policy or subordinate security policies may result in disciplinary action up to and including termination, and may be referred to law enforcement where applicable.

Scope exceptions

Exceptions to this policy or to subordinate policies must be submitted in writing, describe the business justification and compensating controls, and be approved by the CISO or designee. Exceptions are time-bound and reviewed on expiration.

Review cadence

This policy is reviewed annually by the CISO and the Security Steering Committee, with approval from executive leadership, or sooner if a material change in Your Organization's business, technology, regulatory environment, or risk posture warrants it.

Effective date: [the date this policy takes effect]