Sample Security Policy

Purpose: This sample, all-in-one security policy is intentionally concise but complete enough to test ingestion, parsing, and control-mapping in security automation tools. It is aligned to NIST SP 800-53 Rev. 5 control families and uses consistent headings, IDs, and metadata to make machine parsing easier.

Document Metadata

- **Policy ID:** SEC-POL-0001
- **Title:** Enterprise Information Security Policy
- **Version:** 1.0.0
- **Status:** Approved
- **Classification:** Internal
- **Owner:** CISO
- **Approver:** CEO
- **Effective Date:** 2025-09-01
- **Next Review:** 2026-03-01
- **Applies To:** All employees, contractors, systems, and data assets
- **Standards/Refs:** NIST SP 800-53 Rev.5; NIST SP 800-171; CIS Controls v8; ISO/IEC 27001:2022

---

1. Purpose

Establish a unified set of security requirements and governance mechanisms to protect the confidentiality, integrity, and availability of organizational information systems and data.

2. Scope

This policy applies to all organizational units, personnel, contractors, and third parties who create, access, process, transmit, or store organizational data or connect to organizational networks or cloud environments.

3. Definitions (Selected)

- **CUI:** Controlled Unclassified Information.
- **System of Record (SoR):** Authoritative source for a data element.
- **MFA:** Multi-Factor Authentication.
- **Least Privilege:** Minimizing access rights to the bare minimum needed to perform job functions.

---

4. Governance & Roles

- **CISO:** Owns this policy, monitors compliance, reports to executive leadership.
- **Security Engineering:** Implements technical controls, monitoring, and tooling.
- **IT Operations:** Maintains systems, patching, backups, and asset inventory.
- **Data Owners:** Classify data and approve access requests.
- **All Personnel:** Complete security awareness training and comply with this policy.

Control Mapping: PM-1, PM-9, CA-1, AT-1, AT-2, PL-1, PL-2

---

5. Policy Statements by Domain

5.1 Access Control

Policy: Access to systems and data must be authorized, authenticated, and logged. Access is granted on a least-privilege, need-to-know, role-based basis and must be reviewed at least quarterly.
Standards: - Enforce MFA for all privileged accounts and all remote access.
- Implement SSO with centralized identity provider (IdP).
- Disable dormant accounts after 30 days of inactivity.
- Require unique user IDs; prohibit shared accounts except for approved break-glass, with per-use justification and logging.
Procedures (Summary): Access requests via ITSM; Data Owner approval required; quarterly access recertification; immediate revocation upon termination.
Control Mapping: AC-1, AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, IA-2, IA-5, IA-8, PS-4

5.2 Identification & Authentication

Policy: All interactive users and services must be uniquely identified and authenticated using strong credentials. Passwords must meet complexity/length requirements; secrets managed in a vault.
Standards: Minimum 14-character passwords; passphrases recommended; rotate credentials for non-human accounts every 90 days or via short-lived tokens.
Control Mapping: IA-1, IA-2, IA-5, IA-6, IA-8, AC-7

5.3 Configuration Management

Policy: Systems must be configured to secure baselines and changes tracked through a controlled process.
Standards: CIS-hardened baselines; infrastructure as code (IaC) with code review; prohibit direct changes to production outside change windows; scan images and IaC for misconfigurations.
Control Mapping: CM-1, CM-2, CM-3, CM-6, CM-7, RA-5

5.4 Asset Management & Inventory

Policy: Maintain an authoritative inventory of hardware, software, cloud resources, and data stores; tag assets with owner, environment, and data classification.
Control Mapping: CM-8, PM-5, SA-5

5.5 Data Classification & Protection

Policy: Classify data as Public, Internal, Confidential, or Restricted (CUI). Apply controls commensurate with classification, including encryption at rest and in transit.
Standards: TLS 1.2+; disk encryption for all endpoints and servers; object storage with SSE-KMS; DLP for email and file sharing; privacy by design for personal data.
Control Mapping: MP-4, SC-8, SC-12, SC-13, SC-28, PL-8, PT-2

5.6 Logging, Monitoring & Detection

Policy: Centralize logs for security-relevant events; retain minimum 365 days; implement alerting for critical detections; protect log integrity.
Standards: Collect auth, access, network, endpoint, cloud control plane, and application logs; time-sync via NTP; use immutability controls (e.g., WORM) for critical audit logs.
Control Mapping: AU-2, AU-3, AU-6, AU-8, AU-9, SI-4

5.7 Vulnerability & Patch Management

Policy: Continuously identify, assess, and remediate vulnerabilities and apply patches based on risk.
Standards: Critical vulns patched within 7 days; High within 14; Medium within 30; emergency out-of-band patching allowed with CAB notification.
Control Mapping: RA-3, RA-5, SI-2, CM-3

5.8 Incident Response

Policy: Establish and exercise an Incident Response Plan (IRP) covering preparation, detection, analysis, containment, eradication, recovery, and lessons learned.
Standards: 24×7 reporting channel; severity classification (SEV-0–SEV-3); notify stakeholders per communications plan; preserve evidence.
Control Mapping: IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-8

5.9 Business Continuity & Disaster Recovery

Policy: Maintain BCP/DR plans aligned to RTO/RPO targets; test at least annually.
Standards: Daily incremental and weekly full backups for critical systems; off-site or cross-region backups; quarterly restore tests.
Control Mapping: CP-1, CP-2, CP-4, CP-6, CP-9, CP-10

5.10 Secure Development & Change Control

Policy: Apply SSDLC practices including threat modeling, code review, automated testing, SCA/DAST, and pre-prod security gates.
Standards: All code changes via PR; mandatory reviews; secret scanning in repos; SBOM maintained for releases.
Control Mapping: SA-3, SA-8, SA-11, SA-15, SI-3

5.11 Third-Party & Supplier Risk

Policy: Assess security posture of vendors processing organizational data; require security terms, breach notification, and right to audit.
Standards: Due diligence questionnaire; minimum controls for SaaS; DPAs for personal data; annual reassessment.
Control Mapping: SA-9, SR-3, SR-5, SR-6, SR-11

5.12 Physical & Environmental Security

Policy: Control physical access to facilities, networking closets, and server rooms; maintain environmental safeguards.
Standards: Badge access; CCTV retention 30 days; visitor logs; locked racks; temperature and humidity monitoring.
Control Mapping: PE-1, PE-2, PE-3, PE-6, PE-8, PE-12, PE-13

5.13 Privacy & Data Subject Rights

Policy: Process personal data lawfully, minimize collection, and honor data subject rights (access, deletion, correction) where applicable.
Control Mapping: AP-1, AR-2, AR-4, IP-1

---

6. Data Lifecycle Requirements

- **Create/Collect:** Data owners classify data upon creation.
- **Store:** Apply encryption, backup, and retention controls.
- **Use/Share:** Enforce least privilege and DLP; use approved channels only.
- **Archive/Dispose:** Follow retention schedule; sanitize media before disposal.

Control Mapping: MP-6, MP-7, PL-8, AU-11

---

7. Training & Awareness

All personnel must complete onboarding and annual security awareness training; specialized training for admins and developers is required.
Control Mapping: AT-1, AT-2, AT-3

---

8. Risk Management

Perform periodic risk assessments, track risks in a register with owner, likelihood, impact, and treatment plan.
Control Mapping: RA-1, RA-2, PM-9

---

9. Exceptions

Exception requests must document business justification, compensating controls, sunset date, and be approved by the CISO.
Control Mapping: PM-1, CA-1, PL-2

---

10. Enforcement

Violations of this policy may result in disciplinary action up to and including termination and/or legal action.

---

11. Review & Maintenance

This policy is reviewed at least annually or upon material change in risk, technology, or regulation.

---

12. References

- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-171 Rev. 3 (Draft)
- CIS Critical Security Controls v8
- ISO/IEC 27001:2022

---

13. Appendices

Appendix A — Minimum Technical Baselines (Examples)

- **Endpoints:** Full-disk encryption; EDR installed; screen lock ≤ 10 minutes; OS auto-update enabled.
- **Servers/Containers:** CIS baseline; no SSH password auth; key-based only; patched per §5.7.
- **Cloud:** All storage private by default; public access requires ticket and time-bound exception; log buckets immutable (WORM) for 90 days.

Appendix B — Sample Control Coverage Matrix (Excerpt)

Control	Policy Section	Evidence Examples
AC-2	§5.1 Access Control	IdP user list, quarterly access review records
IA-2	§5.1/5.2	MFA settings, auth logs
CM-6	§5.3	Baseline configs, IaC repo links
AU-6	§5.6	SIEM alert rules, incident tickets

Control	Policy Section	Evidence Examples
RA-5	§5.7	Scanner reports, remediation SLAs
IR-4	§5.8	IR playbook, incident timeline
CP-9	§5.9	Backup configs, restore test results
SA-11	§5.10	Code review records, SAST/DAST reports
SR-6	§5.11	Vendor assessment, contract clauses
PE-3	§5.12	Badge access logs, visitor logs

Appendix C — Revision History

Version	Date	Author	Change Summary
1.0.0	2025-09-01	CISO	Initial release