Information Security Policy (Program Umbrella)

Version 1.1 · Last updated 2026-10-20 · Owner: Security Lead and Executive Sponsor

Information Security Policy (Program Umbrella)

> **Unified-set note.** This is the overarching policy for Silkline's Information Security Program (ISP). It serves both the SOC 2 program and the FedRAMP 20x certification — one program, one policy set. Executive commitment, authority, and risk governance are established in the Executive Security Charter; this document defines the program's structure, objectives, and the policy series that implement it.

1. Purpose

Establish a general approach to information security and the minimization of information misuse, compromise, or loss; document security processes and measures; uphold ethical standards; meet regulatory, legal, and contractual obligations; control business risk; and protect Silkline's reputation.

2. Scope

- Information in any form, on any media, and any facility, system, or network used to store, process, or transfer it.
- All Silkline personnel (employees, temporary staff, partners, contractors, vendors, suppliers) and any entity accessing company networks or systems.
- All activity using company information or processing/storage/transmission equipment, on premises or remotely.
- Information resources entrusted to Silkline by external parties (customers, staff, others), including **federal customer data** within the FedRAMP certification boundary.

3. Program Structure

This policy is the overarching policy over the security policy series that constitutes the ISP. The unified series (SOC 2 + FedRAMP 20x) includes:

- Executive Security Charter · Security Budget and Resource Plan
- Acceptable Use Policy (Rules of Behavior) · Code of Conduct
- Access Management Policy · Encryption and Cryptographic Module Policy
- Data Classification Policy · Data Retention and Disposal Policy
- Asset Management Policy · Configuration Management Plan
- Network Security and Segmentation Policy · Log Management and Retention Policy

- Continuous Monitoring Plan · Incident Response Plan · Incident Communications Procedures SOP
- Business Continuity Plan (incorporating backup and disaster recovery)
- Risk Assessment Policy · Physical Security Policy · Maintenance Policy
- Secure Software Development Lifecycle Policy
- Vulnerability Detection and Response Procedure · Vulnerability Disclosure Policy
- Vendor Due Diligence Procedure · Supply Chain Risk Management Policy · SBOM Management Procedure
- Significant Change Notification Procedure · FedRAMP Security Inbox SOP
- Privacy Policy and associated personal-information / data-protection procedures

4. Information Security Objectives

Information in all forms is protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its lifecycle, including appropriate security over the equipment and software used to process, store, and transmit it. The program maintains:

- **Confidentiality** — data protected from unauthorized access
- **Integrity** — data intact, complete, accurate
- **Availability** — systems available when needed

Program objectives: protect information from internal/external, deliberate/accidental threats; enable secure information sharing; encourage consistent, professional use; clarify roles and responsibilities; ensure business continuity; and protect the company from legal liability.

5. Roles and Responsibilities

The Security Lead (Security Officer) is responsible for the design, development, maintenance, dissemination, and enforcement of this policy and the ISP. Governance roles, authority, and reporting lines are defined in the Executive Security Charter.

6. Training

All employees complete general security awareness training at onboarding and annually. Personnel assigned production or Class C boundary access complete general awareness and all relevant role-specific training before access is granted and within five business days of onboarding or role assignment. Five business days is Silkline's internal target. Role training covers privileged/high-risk duties, secure software delivery and incident response or disaster recovery as applicable; refresh it when duties or procedures change and retain applicable annual role-training commitments. Personnel receive role-based guidelines before access and are notified of security changes. Incident-response and contingency training is completed annually and after relevant system, policy or role changes. Record assignment, assessment, completion and access-grant timestamps. Personnel acknowledge security policies on hire and annually. Brent reviews effectiveness and corrective actions at

least quarterly. See the Security Awareness and Training Policy and the quarterly security review records.

7. Policy Review, Accessibility, and Exceptions

- **Review** — at minimum annually, a security/compliance committee of senior management and key personnel evaluates the ISP; all policies are reviewed, updated, signed, and approved.
- **Accessibility** — policies are available to personnel at all times via the compliance automation platform (Drata); role-relevant policies are reviewed and signed on hire and annually.
- **Exceptions** — requests for exceptions to any ISP policy are approved by Executive Management after review and reviewed annually. Exceptions affecting a FedRAMP control are tracked in the VDR register.

8. Enforcement

Management monitors and enforces compliance. Violations are addressed through the disciplinary process in the Code of Conduct, consistent with HR standards; remedies may include warnings, suspension, termination, access revocation, and legal action.

9. Policy Maintenance

Reviewed annually or upon material change; approved by the Security Lead and Executive Sponsor; maintained in the policy repository with pull-request-based review.