Acceptable Use Policy (Rules of Behavior)

Version 1.0 · Last updated 2026-10-20 · Owner: Security Lead

Acceptable Use Policy (Rules of Behavior)

> **Unified-set note.** This is Silkline's single Acceptable Use Policy. It serves both the SOC 2 program and the FedRAMP 20x certification. It also functions as the **Rules of Behavior (NIST PL-4)** referenced by the Executive Security Charter. Where a provision applies only to personnel with access to the FedRAMP certification boundary, that is stated explicitly; all other provisions apply company-wide.

1. Purpose

This policy specifies acceptable use of end-user computing devices, company technology, and company data. It defines the rules of behavior every workforce member must follow, and the sanctions for non-compliance. Training reinforces understanding of current best practices, the sensitivity tiers of data, and acceptable use.

2. Scope

- All Silkline personnel (employees, contractors, temporary staff, third-party users) who use company IT assets.
- Company assets are those owned or managed by Silkline — workstations and mobile devices — and any device that connects to company systems or stores company data (including BYOD), per the Data Classification Policy.
- Personnel with access to the FedRAMP certification boundary are additionally subject to the Access Management Policy and the boundary-specific controls noted below.

3. Personnel Security

- Background verification checks on all candidates for employment and contract are carried out in accordance with relevant laws, regulations, and ethics, proportional to the business need, the data classification to be accessed, and the perceived risk.
- Employees, contractors, and third-party users must agree and sign the terms and conditions of their engagement and comply with this policy before access is granted.
- Onboarding familiarizes personnel with the environments, systems, security requirements, and procedures in place; ongoing, audited security awareness training follows (see Security Awareness and Training Policy).
- Offboarding reiterates duties that survive termination, verifies removal of access to Silkline systems, and confirms return of company-owned assets.
- A fair, documented disciplinary process applies to suspected security breaches (see Code of Conduct); Silkline reserves the right to terminate for serious misconduct.

4. Acceptable Use Requirements

All workforce members must comply with the following:

- All workforce members are treated as **remote users** and must follow all system access controls and remote-access procedures.
- Use of Silkline computing systems is subject to monitoring by Silkline IT and/or Security.
- Computing devices (laptops, smart devices — company-provided or BYOD) used for business must not be left unattended in public.
- **Full-disk encryption** must be enabled on all devices accessing company data (whole-disk encryption for all laptops).
- Email messages containing sensitive or confidential data must be encrypted.
- Sensitive or confidential data must not be posted in public forums or chat rooms; sanitize data before posting for technical support.
- All storage devices and media are managed per the Data Classification Policy and data-handling procedures.
- Reproduction technology (photocopiers, printers) is for authorized use only; media containing classified information is removed from printers immediately, and PIN-print is used where available.

5. Prohibited Activities

Use of Silkline computers, networks, and internet access is a privilege that may be revoked for inappropriate conduct, including: unsolicited spam; private/personal business use; accessing systems or data without authorization; unauthorized copying, deletion, or concealment of company data; misrepresenting oneself or the company; violating any law; propagating malware; abusive, profane, threatening, or discriminatory language; accessing pornographic material; degrading company systems; and defeating or attempting to defeat security controls.

6. Protection Against Malware

- **Software installation restrictions** — only legal, approved, licensed software installed through a pre-approved source; least privilege applied to who may install; permitted/prohibited installation types are defined.
- Anti-malware (or equivalent) protection and monitoring is installed and enabled on all endpoints that may be affected by malware.
- Controls to prevent/detect unauthorized software (application allowlisting) and known/suspected malicious sites (blocklisting) are implemented.
- Malware-exploitable vulnerabilities are reduced through technical vulnerability management (see Vulnerability Detection and Response Procedure).

7. Mobile and Remote Use

- Secure remote access uses encryption (VPN) and strong authentication. For boundary administrative access, the FIPS-validated bastion path in the Network Security and

Segmentation Policy applies; commercial VPN tooling must not broker access to federal customer data.
- Up-to-date endpoint protection is required on all devices; security tooling must not be disabled or circumvented.
- Lost or stolen devices and suspected incidents are reported immediately to the Security Lead or security@silkline.ai.

8. Return of Assets

Upon separation, all Silkline-owned assets and devices are returned within 5 business days. Company data is removed from personal (BYOD) devices prior to the effective date of separation.

9. Clean Desk / Clear Screen

Sensitive/confidential materials (hardcopy or electronic) are secured when not in use or when the workspace is unattended; screens are locked when stepping away; printouts are removed immediately; whiteboards are erased; portable media is treated as sensitive, encrypted, and secured.

10. Enforcement

Violations are addressed through the disciplinary process in the Code of Conduct and the organization's HR standards. Repeated or willful non-compliance may result in access revocation and, for serious cases, termination and/or legal remedies.

11. Acknowledgement

All personnel acknowledge this policy upon hire and annually thereafter. For boundary personnel, acknowledgement is a precondition of access (Rules of Behavior, PL-4).

12. Policy Maintenance

- **Review frequency**: Annually, or upon material change to acceptable-use risk.
- **Approval**: Security Lead.
- **Distribution**: All personnel; acknowledgement tracked.
- **Version control**: Maintained in the policy repository with pull-request-based review.