
# SBSS Framework

*Small Business Security Standard*

Prepared by Silex Strategic Group

www.silexstrategicgroup.com

# Table of Contents

## 1. Framework Overview

The Small Business Security Standard (SBSS) offers 50 clearly defined controls across physical and information security. This document presents each control with an explanation to help small businesses assess, strengthen, and certify their readiness. SBSS simplifies enterprise-grade concepts into practical, accessible standards tailored for growing organizations.

## 2. Physical Security Controls

SBSS.Physical.1: Secure all exterior doors with commercial-grade locks. Ensure that all entry points have tamper-resistant, high-quality locks to reduce unauthorized access.

SBSS.Physical.2: Install surveillance cameras at all entry and exit points. Cameras provide continuous visual monitoring, deter intruders, and support investigations.

SBSS.Physical.3: Restrict access to server rooms and sensitive areas. Only authorized individuals should have physical access to locations housing critical systems or data.

SBSS.Physical.4: Implement visitor sign-in and badge system. Logging visitors ensures awareness of who is in your facility and when, enhancing accountability.

SBSS.Physical.5: Use alarm systems monitored by a security provider. Professionally monitored alarms help alert you and law enforcement in real time during break-ins.

SBSS.Physical.6: Conduct regular perimeter security inspections. Routine checks help detect weaknesses like broken locks, gaps in fencing, or blind spots.

SBSS.Physical.7: Post emergency evacuation maps in visible areas. Clearly labeled evacuation maps guide personnel during fire, intruder, or hazard emergencies.

SBSS.Physical.8: Install motion-sensor lighting outside facilities. Lighting deters intruders and improves visibility in vulnerable areas after dark.

SBSS.Physical.9: Train staff on basic physical security practices. Empower employees to recognize and report suspicious activity and understand emergency procedures.

SBSS.Physical.10: Secure windows with locks or shatter-resistant film. Reinforce windows to prevent easy break-ins or reduce risk from external blasts or impacts.

SBSS.Physical.11: Store backups and sensitive materials in locked cabinets. Even internal threats can be mitigated by storing sensitive files and drives in locked containers.

SBSS.Physical.12: Perform routine drills for fire and lockdown procedures. Practice helps ensure rapid, coordinated responses to emergencies, reducing confusion and injury.

SBSS.Physical.13: Ensure access points are monitored and controlled. Entryways should have cameras or be manned/locked when appropriate to reduce unauthorized entry.

SBSS.Physical.14: Conduct background checks for employees with physical access. Screen those with access to sensitive spaces to prevent insider threats and fraud.

SBSS.Physical.15: Maintain a list of authorized personnel. Keeping access rosters updated ensures clarity on who can enter what areas and when.

SBSS.Physical.16: Use electronic access control where feasible. Electronic badges, fobs, or biometrics allow for tracking and restricting movement by user.

SBSS.Physical.17: Verify identity of maintenance and service vendors. Temporary workers must be verified and possibly escorted to prevent unintentional or intentional risks.

SBSS.Physical.18: Protect HVAC and utility systems from tampering. Securing power, water, and air systems prevents outages and potential sabotage.

SBSS.Physical.19: Prevent tailgating with signage and training. Train staff to avoid letting others 'piggyback' into secure areas without verification.

SBSS.Physical.20: Secure company vehicles when not in use. Lock and track vehicles to avoid theft, misuse, or unauthorized travel.

SBSS.Physical.21: Keep doors closed and locked when rooms are unoccupied. Prevents casual theft or snooping in spaces not actively used.

SBSS.Physical.22: Implement lockout/tagout procedures for equipment. Safeguards against accidental startup of machinery during maintenance or repair.

SBSS.Physical.23: Designate security zones for high-value items. Segment critical assets into more secure spaces with limited access.

SBSS.Physical.24: Audit physical keys regularly. Periodic audits help track missing keys, reassign access, or trigger rekeying if necessary.

SBSS.Physical.25: Ensure security systems have battery backup. Maintain surveillance and alarms even during power outages.

## 3. Information Security Controls

SBSS.InfoSec.1: Require strong passwords and regular changes. Enforces basic access hygiene and limits the value of stolen credentials.

SBSS.InfoSec.2: Use multi-factor authentication on all critical systems. Adds a second layer of defense against compromised login details.

SBSS.InfoSec.3: Encrypt sensitive data at rest and in transit. Ensures that even if data is intercepted or stolen, it cannot be read.

SBSS.InfoSec.4: Maintain up-to-date antivirus and anti-malware software. Reduces exposure to common threats like ransomware, spyware, and trojans.

SBSS.InfoSec.5: Perform regular backups and test data restoration. Enables recovery from data loss, corruption, or cyberattacks like ransomware.

SBSS.InfoSec.6: Limit access to data based on user roles. Only give employees access to what they need, minimizing potential damage.

SBSS.InfoSec.7: Train employees on phishing and cybersecurity awareness. Informed users are your first line of defense against social engineering and scams.

SBSS.InfoSec.8: Update software and firmware regularly. Keeps systems patched against known vulnerabilities.

SBSS.InfoSec.9: Use firewalls to protect internal networks. Controls inbound and outbound traffic to guard your digital perimeter.

SBSS.InfoSec.10: Implement endpoint protection and monitoring tools. Monitors computers and mobile devices for unauthorized or malicious behavior.

SBSS.InfoSec.11: Keep an asset inventory of all digital devices. Track what you own so you can secure it, replace it, or investigate it if compromised.

SBSS.InfoSec.12: Secure Wi-Fi with strong encryption and hidden SSID. Prevents unauthorized users from accessing your network or sniffing traffic.

SBSS.InfoSec.13: Disable unused user accounts promptly. Prevents exploitation of dormant accounts by former employees or attackers.

SBSS.InfoSec.14: Use logging and monitoring to detect anomalies. Audit trails help identify unusual access patterns or breaches.

SBSS.InfoSec.15: Conduct periodic vulnerability scans. Scans help find holes in your defenses before attackers do.

SBSS.InfoSec.16: Secure mobile devices with PINs and encryption. Protects data on-the-go, especially for employees working remotely or in the field.

SBSS.InfoSec.17: Develop and test an incident response plan. Prepares you to react quickly and effectively during a cyberattack or data breach.

SBSS.InfoSec.18: Avoid using personal devices for sensitive work tasks. Reduces the chance of data leakage or unmonitored access.

SBSS.InfoSec.19: Review third-party vendor security practices. Evaluate the risk exposure that comes from outside vendors accessing your systems or data.

SBSS.InfoSec.20: Require secure remote access (VPN or equivalent). Keeps remote connections encrypted and protected from snooping or hijacking.

SBSS.InfoSec.21: Protect admin accounts with strict controls. These accounts have elevated privileges and need extra safeguards like MFA and auditing.

SBSS.InfoSec.22: Define and enforce data retention policies. Helps reduce data sprawl and supports compliance with legal and industry requirements.

SBSS.InfoSec.23: Classify data and label it accordingly. Make it clear what data is sensitive, public, or internal-use only.

SBSS.InfoSec.24: Protect email systems from spoofing and spam. Implements SPF/DKIM/DMARC and filters to reduce phishing and impersonation risk.

SBSS.InfoSec.25: Conduct annual security risk assessments. Regular evaluations help identify new threats, vulnerabilities, and areas for improvement.

## 4. Contact Information

To learn more about the SBSS Framework, SBSS Certification, or to schedule a consultation, please reach out to us below:

*Email: silexstrategicgroup@gmail.com*

*Phone: 501-209-3006*

*Website: www.silexstrategicgroup.com*