

# Empowering Vendors to Reduce Risk

*LinkSECURE provides hands-on guidance to help small- to mid-sized vendors implement essential security safeguards in order to strengthen their cybersecurity operations.*

## Target Audience

LinkSECURE is designed for third-party vendors and service providers in retail and hospitality, including:

**Supply Chain:** Logistics, shipping, warehouse, fulfillment

**Operations:** Cleaning, maintenance, laundry and linen

**Business Services:** Consulting, staffing, print and advertising

**Industry Specific:** Food and beverage, franchisees, manufacturing

## The Process

1. Guided Baseline Self-Assessment
2. Step-by-step, guided implementation of critical security controls
3. Access to an online hub to download tools, resources, and collaborate with other cybersecurity professionals
4. Select, review, and implement benchmarks and build kits to harden systems
5. Utilize automation tool to check if systems are configured according to benchmark and build kit recommendations

## Cost

\$6,000 per year

## Progress Tracking & Reporting

Progress reports and tracking tools ensure transparency and accountability, allowing for the monitoring of improvements, demonstration of compliance, and optimization of security strategy.

## LINKSECURE BENEFITS



### Cybersecurity Maturity Program

Evolve from basic defenses to a robust framework that reduces attacks, protects data, and builds trust.



### Third-Party Risk Reduction

Secure your vendors' security controls to minimize third-party risks, protect the supply chain, ensure business continuity, and maintain brand integrity.



### Guided Security Implementation

Simplify deploying security safeguards through hands-on guidance, enabling efficient resource allocation, reduced errors, and faster security implementation.



### Expert Support & Resources

Security experts, training, and an online hub empower teams to effectively manage cybersecurity, maximize investment, and foster a security-aware culture.

## Tools & Resources

LinkSECURE participants will have access to:

**Online Hub:** Download tools and resources, plus access interactive community forums to discuss security topics, ask questions, and collaborate with other cybersecurity professionals.

**Benchmarks:** They are comprehensive, consensus-driven configuration guidelines and best practices for securing computer systems, software, and networks. Widely recognized as industry standards, they are referenced by various compliance frameworks to establish baseline security.

**Buildkits:** Pre-configured templates/scripts to automate the process of hardening systems according to selected benchmarks.

**Tracking & Collaboration Tool:** Facilitates collaboration among team members to track and document progress on security control implementation. Enables organizations to tailor assessments to their specific needs and generates detailed reports on security gaps and compliance status.

**Assessment Tool:** Automatically assess the security posture of systems and networks against industry-recognized security best practices.

## Security Controls & Safeguards Overview

CONTROL 01 <b>Inventory &amp; Control of Enterprise Assets</b> A complete picture of your assets	CONTROL 02 <b>Inventory &amp; Control of Software Assets</b> A complete picture of your software landscape	CONTROL 03 <b>Data Protection</b> Protect your most valuable asset: data
CONTROL 04 <b>Secure Configuration of Enterprise Assets &amp; Software</b> Lock down your assets	CONTROL 05 <b>Account Management</b> Take control of your accounts	CONTROL 06 <b>Access Control Management</b> Right user, right access, right time
CONTROL 07 <b>Continuous Vulnerability Management</b> Stay ahead of threats	CONTROL 08 <b>Audit Log Management</b> Track every action	CONTROL 09 <b>Email &amp; Web Browser Protections</b> Protecting your digital front line
CONTROL 10 <b>Malware Defenses</b> Detect and prevent malware infections	CONTROL 11 <b>Data Recovery</b> Ensure business continuity through data recovery	CONTROL 12 <b>Network Infrastructure Management</b> Secure network devices and services
CONTROL 13 <b>Network Monitoring &amp; Defense</b> Threat hunting and response	CONTROL 14 <b>Security Awareness &amp; Skills Training</b> Building a security-savvy workforce	CONTROL 15 <b>Service Provider Management</b> Building trust with your service providers
CONTROL 16 <b>Application Security Software</b> Application security: built-in, not bolted on	CONTROL 17 <b>Incident Response Management</b> Prepared for the unexpected	CONTROL 18 <b>Penetration Testing</b> Test Your defenses