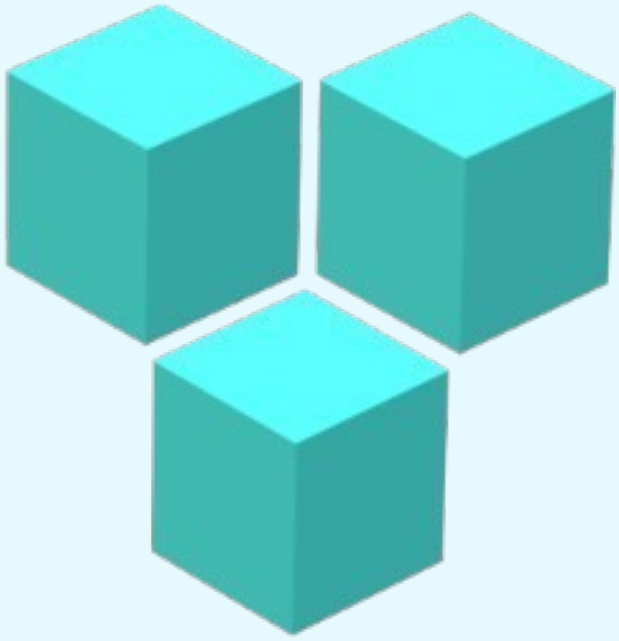

# SofTouch Systems

## STS Patch & Update Compliance Checklist

“Close the gaps. Stop the threats. Stay secure.”

**No-Surprise IT:** Predictable. Proactive. Proven.

## Why Patch Compliance Matters

Most small business owners assume their systems update themselves. You installed antivirus, you run Windows or macOS, and you see occasional “Update Required” pop-ups.

That assumption is your single biggest security risk.

Thinking updates “just happen” is the exact behavior modern cybercriminals count on. Every major ransomware attack you see in the news began with the same pattern:

A known vulnerability + an unpatched system = full compromise.

It only takes one missed update on one machine to put every device, every account, and every employee at risk.

This checklist shows you the exact areas where compliance fails and how to verify your protection.

# SECTION 1 — Operating System (OS) Vulnerabilities

Your OS is the foundation of your security. When Microsoft or Apple releases a patch, it’s because a vulnerability has already been discovered and is now public knowledge. Hackers race to exploit it before small businesses update.

## OS Patch Compliance Checklist

✔ Confirm automatic updates are enforced (not optional)

✔ Verify machines install updates without waiting for user approval

✔ Ensure devices left powered off are still receiving updates

✔ Check that servers follow a scheduled, verified patch cycle

✔ Review OS version numbers monthly to ensure end-of-life systems are replaced

✔ Confirm updates are logged, monitored, and centrally reported

**Risk Insight:**

Relying on default update schedules means updates may wait days or never apply at all. Without centralized verification, you cannot assume your OS is protected.

# SECTION 2 — Third-Party Applications: The Hidden Threat

Even if your OS is fully patched, your biggest risk often comes from everyday programs:

Adobe Acrobat

Zoom

Chrome / Firefox / Edge

Java

QuickBooks

Dropbox

Teams / Slack

…and dozens more.

These apps run constantly and are attacked constantly. Most do not update in coordination with your OS.

## Third-Party Patch Compliance Checklist

✔ Maintain an inventory of all applications running on all endpoints

✔ Verify browser updates weekly

✔ Confirm updates for PDF tools, office software, cloud sync tools

✔ Remove unused apps (attackers exploit old versions long after you stop using them)

✔ Ensure auto-update is enabled wherever available

✔ Use centralized tools to validate third-party patch success

## Risk Insight:

Tracking 10–20 applications across 10–20 employees is impossible manually.

Unpatched third-party software is the #1 entry point for credential theft, ransomware, and spyware.

# SECTION 3 — Firmware, Certificates & Renewals: The Silent Killers

These items don’t generate complaints when they’re outdated—until something breaks.

## Firmware Compliance Checklist

✔ Verify firewall firmware is current

✔ Confirm Wi-Fi access points and switches receive updates

✔ Review router firmware quarterly

✔ Check for security advisories from hardware vendors

### Risk Insight:

An outdated firewall is like a locked door with a broken hinge—easy to bypass.

### Certificate & Renewal Compliance Checklist

✔ Check SSL certificate expiration dates for websites and email servers

✔ Confirm domain renewals are monitored

✔ Verify security and licensing renewals are tracked in a central system

✔ Ensure no product expires without alerting IT

### Risk Insight:

An expired certificate can take down your website or email instantly. No attack required just an overlooked renewal.

## SECTION 4 — Compliance Verification: The Automated Audit

Compliance is not:

Hoping updates ran

Trusting staff to click “Install”

Believing “Windows handles it”

Compliance is:

Verifying every update applied

Monitoring every machine

Alerting instantly when anything falls out of policy

Documenting patch success across the entire network

### Automated Audit Checklist

✔ Centralized dashboard showing real-time update status

✔ Alerts for failed or missing updates

✔ Weekly patch compliance report

✔ Logged evidence of patch completion

✔ Constraints that prevent users from bypassing updates

✔ Monthly review of non-compliant devices

✔ Automatic quarantining of high-risk endpoints

### Risk Insight:

If you cannot see your compliance, you do not have compliance.

# SECTION 5 — The STS Patch Compliance Scorecard

Use this quick scorecard to assess your current posture:

### 1 — Operating System (OS) Compliance

Goal: All systems must be fully updated with the latest Windows/macOS security patches.

☐ OS auto-updates enabled

☐ Latest cumulative/security updates installed

☐ Last update check within 7 days

☐ All devices online during update windows

☐ Reboots completed after patching

Score (0–5): _____

### 2 — Third-Party Applications

Goal: Adobe, Java, Chrome/Firefox/Edge, QuickBooks, Zoom, etc. must be patched within 48 hours of release.

☐ Adobe Acrobat updated

☐ Browsers updated (Chrome/Edge/Firefox)

☐ Zoom/Teams updated

☐ QuickBooks updated

☐ All apps validated with a software inventory

Score (0–5): _____

## 3 — Firmware & Certificates

Goal: Infrastructure and perimeter must stay compliant to avoid silent vulnerabilities.

☐ Firewall firmware current

☐ Switch/router firmware current

☐ SSL certificate expiration checked

☐ Domain expiration checked

☐ Security licenses validated (AV, backup, etc.)

Score (0–5): _____

## 4 — Verification & Auditing

Goal: Updates must be verified, not assumed.

☐ Patch compliance report reviewed

☐ Failed/partial updates resolved

☐ Offline devices checked manually

☐ Auto-remediation tools in place

☐ Weekly audit completed

Score (0–5): _____

**TOTAL SCORE (0–20): _____**

# How to Interpret Your Score

18–20: Excellent (Low Risk)

Your systems are being properly maintained with minimal exposure.

14–17: Fair (Moderate Risk)

You're partially compliant, but several gaps remain that attackers routinely exploit.

10–13: Poor (High Risk)

Your patching posture leaves major vulnerabilities open.

You are one missed update away from ransomware.

0–9: Critical (Severe Risk)

# SECTION 6 — : Patch Management Is a Security Strategy

Patch management is not a “set it and forget it” task.

It is a constant, evolving, business-critical security requirement.

Without automation and verification, your system:

Mislabels machines as “updated”

Leaves third-party apps unpatched

Ignores firmware

Misses certificates

Lets expired licenses create silent failures

Cannot guarantee protection

Manual patching is no longer realistic for any business of any size.

# STS Can Close Every One of These Gaps

Our Managed Services (Tier 1) include:

24/7 Real-Time Monitoring

Antivirus & Anti-Malware

Automated Patch Deployment

Firmware & Device Compliance Tracking

License/Credential Renewal Audits

Full Compliance Reporting

No-Surprise IT — predictable cost, predictable protection

We handle the vigilance so you don’t have to.

# FREE 15-Minute Security Compliance Audit

Want to see exactly where your systems are exposed?
We'll show you:
Your missing patches
Your outdated software
Your high-risk endpoints
Your compliance gaps
Your top 3 vulnerabilities
Zero obligation. No pressure. Pure insight.

→ Book your audit now **HERE**

SofTouch Systems

*Simplifying technology, maximizing results.*