Digital Spring Cleaning Checklist

Systems Support
IT Support & Service Since 1989
systemsupport.com
781-661-5619
info@systemsupport.com

1 Know What You Have

VISIBILITY

- ☐ List all software & SaaS tools
- ☐ Inventory company devices
- ☐ Identify all user accounts
- ☐ Assign "owners" to each system

If you don't see it you can't manage it or secure it...

2 Eliminate What You Don't Need

REDUCE COST + COMPLEXITY

- ☐ Cancel unused or duplicate software
- ☐ Archive or purge outdated files
- ☐ Remove old accounts and access
- ☐ Consolidate overlapping tools

IT waste builds up quietly over time when no one is looking...

3 Make Sure It All Works

RISK REDUCTION

- ☐ Test your backups
- ☐ Confirm updates and patches
- ☐ Verify protections
- ☐ Check systems monitoring

The worst time to try your backup is after a disaster...

4 Optimize What you Already Have

IMPROVE PERFORMANCE + ROI

- ☐ Standardize how tools are used
- ☐ Reduce unnecessary notifications
- ☐ Clean up file shares and structures
- ☐ Invest in training for your tools

The solution isn't more tools, it's using what you have well.

5 Set a Simple Maintenance Routine

MAKE IT STICK

- ☐ Schedule regular tech reviews
- ☐ Regularly review licenses and usage
- ☐ Audit user access and permissions
- ☐ Test backups regularly

Cleanup is faster when you make it a habit, not an annual chore...

Unsure about more than 2 of these Items?

IT'S WORTH A CLOSER LOOK

REVIEW
the full guide

TAKE
our IT Risk Assessment

Executive Summary

For SMBs in Massachusetts, “tech spring cleaning” means getting existing IT under control before buying anything new. It’s a systematic program—inventory apps/accounts, validate defenses (patching, backups), retire or secure old assets, and streamline processes. This report offers a playbook to help you take control of your IT (and its costs) and stay on top of things so you don’t go back to the chaos. Of course not every business can do this alone, and that’s why an MSP like Systems Support can be an important partner for your organization.

In this report we will cover four actionable steps (with breakdowns), a priority checklist, and a sprint plan to help your business come out swinging. Insurance companies are creating de facto compliance frameworks, AI companies and consolidation are driving up hardware prices, and economic headwinds are uncertain - so businesses are feeling pressure to do more with less from every direction. So we’re offering up the first steps to help get out from under some of that pressure.

MSP-Led 30/60/90-Day Spring-Cleaning Plan

EXPLORATE

IMPLEMENT

REPEAT

Weeks 1–2: Discover & document everything. Get feedback from employees and stakeholders. Run tools.

Weeks 3–4: “Stop the bleeding”: patch known gaps, test backups, enforce MFA.

Weeks 5–6: Report interim evidence (with screenshots/exports) to client/insurer. Plan endpoint upgrades or ESU.

Weeks 7–9: Execute high-impact fixes: device sanitization, Cloud PC pilot, license cleanup.

Weeks 10–13: Cement processes: finalize policies, train staff, review results. Deliver final evidence binder (inventory exports, reports, logs).

This is an approximate template for delivering fast wins, it should be adjusted based on the size of the business and resources you can assign to the project.

The Goals of Digital Spring Cleaning

Digital spring cleaning is about ***operational discipline***, not just file deletion. Over time, SMBs quietly accumulate outdated OS, forgotten apps, stale accounts, and unchecked misconfigurations. Individually these issues seem minor, but collectively they inflate costs and risk. Think of it as preventive maintenance: align your IT estate with compliance requirements and business needs.

- **Reduce risk:** Ensure every system that holds sensitive data is patched, encrypted, and monitored. (Per MA 201 CMR 17.04, systems with personal info must have encryption on portable devices and up-to-date OS security patches.)
- **Cut waste:** Eliminate unused SaaS licenses and redundant tools (the average org has 100+ apps as of 2024), freeing budget and reducing complexity.
- **Evidence readiness:** Create documentation (inventories, logs, test results) to satisfy insurers and auditors. The FTC Safeguards Rule and Massachusetts law expect encrypted data, MFA, logging, and tested backups.

A spring-clean is not a one-off chore: it establishes processes (patch SLAs, review cycles) that keep your environment healthy and defensible.

Systems Support
IT Support & Service Since 1989

SCHEDULE
a 15-minute discovery call

462 Plain Street Suite 206
Marshfield, MA 02050
www.systemsupport.com
Phone: 781-661-5619
Email: info@systemsupport.com

1) Know What You Have

Create a complete, accurate picture of your IT environment.

Before you can improve anything, you need to clearly understand what you actually have.

Devices & Infrastructure

What hardware and systems exist within your business? You’re looking for a complete, accurate inventory—not just what’s documented, but what’s actually in use.

Checklist:

- Workstations and laptops
- Servers (on-prem or cloud)
- Network equipment (firewalls, switches, WiFi)
- Remote, Home office, and BYOD

What good looks like:

A single list with device name, owner, OS, purchase date, and status.
No “mystery devices” on the network.

Users & Access

Review who has access to your systems and what level of access they have. This includes current employees, former employees, and any shared or administrative accounts.

Checklist:

Active employees or contractors

- Former employees (still have access?)
- Admin or privileged accounts
- Shared accounts

What good looks like:

Every account tied to a real person or function.
No orphaned or unknown accounts.

Subscriptions & Software

What are you actually paying for? Cloud-based tools especially love to multiply and it’s important to know what you have, how it’s used, and if it’s still needed.

Checklist:

- Microsoft 365 / Google Workspace
- Industry tools (CRM, EMR, accounting, etc.)
- File storage (Dropbox, Box, etc.)
- Shadow IT (tools teams signed up for themselves)

What good looks like:

A full list of tools, owners, and renewal dates
Clear understanding of usage vs. cost

Data Locations

Where does your important data live? Important data should be in known, controlled locations, not scattered at random or locked up in a single user account.

Checklist:

- File servers
- Cloud storage
- Local machines
- Backup systems

What good looks like:

You know where critical data is stored
You’re not relying on “someone’s desktop”

Vendors & Dependencies

Who supports your systems? Every system should have a clear point of contact and ownership.

Checklist:

- IT providers
- Software vendors
- Backup providers
- Internet/phone providers

What good looks like:

Clear ownership and contact for each system
No “we don’t know who set that up”

This step almost always uncovers tools that no one remembers buying, old employee credentials that never got turned off, and data that’s being stored in a lot of inconsistent places. Each vestigial account and dangling device isn’t just an expense, it’s a potential vulnerability. At the end of this step you should have a single document (a spreadsheet works fine) that includes your devices, users, tools, vendors, data locations and ownership.

What You’re Trying to Answer:

By the end of this step, you should be able to confidently answer:

- *What systems do we actually have?*
- *Who has access to what?*
- *What are we paying for?*
- *Where does sensitive data live?*

2) Eliminate What You Don't Need

Reduce complexity, cost, and hidden risk

Once you can see your environment clearly, the next step is to simplify it. Most businesses don't struggle because they lack tools—they struggle because they have too many, with overlapping functions, unclear ownership, and lingering access. The goal here is to make deliberate decisions about what stays and what goes.

The Elimination Rubric

1. Is it actively used?
Who uses it, and how often?
Would anyone notice if it disappeared tomorrow?
If no clear usage → candidate for removal

2. Does it have a clear owner?
Is someone responsible for managing it?
Does anyone "own" the relationship or configuration?
If no owner → high risk, likely removable or needs reassignment

3. Does it duplicate something else?
Are there multiple tools solving the same problem?
Are teams using different systems for the same function?
If yes → consolidate

4. Is it still supported and secure?
Is it actively maintained by the vendor?
Does it meet your current security standards?
If no → prioritize replacement or removal

5. Is it worth what you're paying?
Is the cost aligned with actual usage and value?
Are you paying for unused licenses or features?
If no → downgrade, renegotiate, or cancel

Quick Test:

If you can't answer all three questions about a tool, it's a candidate for removal - especially with SaaS tools that can be renewed quickly if they're needed later.

- *Who owns this?*
- *Who uses this?*
- *What would break if this disappeared?*

How to Remove Things Safely

This is where most businesses hesitate—and for good reason.

Before removing anything:

- Check dependencies
- Make sure no critical workflows rely on it
- Export important data
- Assume you won't get easy access later
- Confirm ownership
- Ensure someone signs off on removal
- Document the change
- Keep a record of what was removed and when

Common Pitfalls (This Is Important)

"We might need it later"
This is how clutter accumulates. If something hasn't been used in months, it's usually safe to remove—with a backup.

SaaS Tools That Don't Fully Cancel
Some platforms:

- Continue billing after "cancellation"
- Require multi-step off-boarding
- Retain user accounts or data

Best practice:

- Confirm cancellation in writing
- Remove payment methods if possible
- Set a reminder to verify billing stopped

Forgotten Integrations
Tools are often connected behind the scenes (email sync, APIs, automation tools).
→ Removing one system can break another if not checked first

Licenses vs. Accounts
Removing a user doesn't always remove the license.
→ Make sure you're actually reducing cost, not just access

What Good Looks Like

- Tools have a clear purpose
- No inactive accounts or subscriptions
- Minimal overlap between systems
- Clear ownership across everything in use

Systems Support
IT Support & Service Since 1989

SCHEDULE
a 15-minute discovery call

462 Plain Street Suite 206
Marshfield, MA 02050
www.systemsupport.com
Phone: 781-661-5619
Email: info@systemsupport.com

3) Make Sure It Works

Ensure every active system is secure, up to date, and recoverable.

It's not enough to have controls and failsafes, you need to know that they're working. Plenty of businesses have pieces of security in place, but can they show that they're being updated, tested, and reviewed? That gap is where risk - and failed insurances claims - tends to grow.

Your system doesn't have to be complicated, it has to be something that you can maintain and verify.

Patch Management

Patching is one of the simplest and most effective ways to reduce risk—but only if it's done consistently and tracked. Without visibility, it's easy to assume systems are up to date when they're not.

- Track when systems were last patched and whether any critical updates are missing
- Maintain a simple list of exceptions (systems that couldn't be updated and why)

Backups & Recovery

Backups are often treated as a checkbox, but they only matter if they can be restored when needed. The difference between having backups and being able to recover is what defines resilience.

- Record backup success/failure and the date of the last successful backup
- Document at least one real restore test, including how long it took and what was recovered.

Endpoint Protection

Most businesses have antivirus or endpoint protection in place, but coverage gaps can be common - especially with remote and lightly managed devices. The goal here is greater visibility.

- Track which devices are protected and identify any that are not reported
- Confirm definitions and protection tools are up to date across all endpoints

Access & Authentication:

Access controls are where little oversights can lead to major issues. Over time permissions and shortcuts accumulate and are rarely revisited.

- Maintain a list of privileged and administrative accounts
- Track where MFA is enforced and where there are gaps

Network & Configuration Security

Network configurations tend to persist long after their original purpose is forgotten. Periodic review helps ensure that exposure is intentional, not accidental.

- Track firewall changes and review exposed ports or remote access points
- Confirm that only necessary services are accessible externally

Vulnerabilities & Exceptions

Not every issue can be fixed immediately, but untracked risks tend to become permanent. The key is to acknowledge and manage them intentionally.

- Maintain a list of known vulnerabilities or risks that are still open
- Assign a reason and a target timeline for addressing each one

Check Your Hardware

Hardware issues can create quality of life problems for employees by slowing their productivity and increasing their frustration.

- Ensure devices are in good working order, desktops shouldn't be homes for dust bunnies.
- Go through any extra cables, accessories, and batteries

Most businesses don't need more security tools, they need a better understanding of what is already in place. Once you know what you have and whether or not it's working, then you can start to learn how to bridge any gaps - whether that's implementing more training, encouraging a "security first" culture (and making sure people are actually using the MFA), or investing in new solutions.

The Security Checklist:

By the end of this step, you should have a record of your security steps and know where the logs are:

- *Verify all critical patches have been applied this month*
- *Perform and document at least one restore test*
- *Confirm endpoint protection is active and up to date*

4) Optimize What You Have

Get more value from the systems you already use

Once your environment is stable and simplified, the next opportunity isn't adding more—it's improving how what you already have is used. Most businesses already pay for capable tools, but over time, usage drifts. Workarounds form, processes become inconsistent, and systems are used below their potential.

Optimization is about tightening that gap—so your technology supports how your business actually operates, not the other way around.

Where to Focus

Tool Utilization

Most platforms are only partially used. Features that could save time or reduce manual work often go untouched.

- Review how core tools (Microsoft 365, CRM, line-of-business apps) are actually being used
- Identify features that could replace manual steps or eliminate additional tools

Workflow Simplification

Over time, processes tend to become more complex than they need to be. This usually shows up as duplicate steps, unnecessary approvals, or work happening in multiple systems.

- Map out a few common workflows (onboarding, file sharing, reporting)
- Look for steps that can be removed, combined, or automated

Standardization

When different teams use the same tools in different ways, it creates confusion and inefficiency.

- Define a "default way" of using core systems
- Align teams around consistent structures (file organization, communication tools, naming conventions)

Performance & Friction Points

Slow systems and small inefficiencies add up quickly across a team.

- Identify recurring complaints (slow devices, login issues, file access problems)
- Prioritize fixes that remove daily friction for multiple users

Training and Education

Many software tools are very powerful, especially when you get under the hood. Investing in employee education can have a profound effect on productivity.

- Give access to workshops and trainings for common software and programs.
- Encourage and promote employees sharing information and techniques with colleagues.

Optimization Rubric

Use this to evaluate whether a system is working as well as it could:

1. Are we using this consistently?
If every team uses it differently, it's creating confusion.

2. Are we working around it?
If people rely on spreadsheets, email, or side tools to compensate, something isn't aligned.

3. Is it replacing manual work—or adding to it?
Good systems reduce effort. Poorly used ones create extra steps.

4. Is it solving one problem clearly?
If a tool is trying to do too much (or overlapping with others), it's likely inefficient.

Optimization Rubric

"We'll just add another tool"
This often increases complexity instead of solving the underlying issue.

Over-customization
Highly customized systems can become fragile and difficult to maintain.

Ignoring user experience
If systems are frustrating to use, people will find workarounds—no matter how good the tool is.

What Good Looks Like:

- *Core tools are used consistently across the business*
- *Fewer manual processes and workarounds*
- *Reduced reliance on duplicate or "shadow" systems*
- *Employees spend less time navigating systems and more time working*

Systems Support
IT Support & Service Since 1989

SCHEDULE
a 15-minute discovery call

462 Plain Street Suite 206
Marshfield, MA 02050
www.systemsupport.com
Phone: 781-661-5619
Email: info@systemsupport.com

5) Set a Maintenance Routine

Use your spring cleaning to reset your routines

Where to Focus

Regular Reviews
What gets reviewed gets managed. Without periodic check-ins, issues tend to go unnoticed until they become problems.

- Schedule recurring reviews of users, access, tools, and devices
- Look for anything new, unused, or out of place

Patching & Updates
Consistency matters more than intensity. A simple, reliable schedule is more effective than sporadic effort.

- Maintain a regular patching cadence (e.g., monthly + critical updates as needed)
- Ensure all systems remain supported and up to date

Backup Testing
Backups shouldn't be "set and forget." They need to be validated over time.

- Schedule periodic restore tests (not just backup checks)
- Confirm recovery time and data integrity

Ownership & Accountability
One of the most common gaps in SMB environments is unclear responsibility.

- Assign ownership for key systems and processes
- Ensure someone is accountable for follow-through

Training & Awareness
Technology doesn't operate in isolation—people are part of the system.

- Reinforce basic security practices (MFA, phishing awareness, device use)
- Keep expectations clear and consistent across the organization

Good Habits for Clean IT:

Daily:
Review alerts and notifications
Track Issues (slow systems, access problems, etc)

Weekly:
Check for patches and updates
Document recent changes

Monthly:
Test and verify backups
Review users and permissions

Maintenance Rhythm (Simple Model)

You don't need a complex system to stay in control—just a predictable one. The goal is to create a steady cadence of small, consistent actions that prevent larger problems from building over time.

On a monthly basis, this means keeping systems up to date and paying attention to early warning signs—applying patches, reviewing alerts, and making sure nothing is quietly drifting out of alignment. Quarterly, it's about stepping back and reassessing: reviewing who has access, auditing the tools you're using, and confirming that your backups still work as expected. And at least once a year, it's worth taking a broader view—looking at how your environment has evolved, updating policies, and making sure your systems still reflect how your business operates.

Culture Shift: What This Really Means

This isn't just about maintaining systems—it's about changing how the business approaches technology. Over time, the shift is subtle but important: moving from reacting to issues as they arise to managing them before they surface, from assuming things are working to regularly verifying that they are, and from unclear ownership to defined responsibility.

When this takes hold, IT stops being a source of surprises. It becomes something steady, predictable, and easier to trust.

Need a Closer Look?

Most businesses don't set out to create complexity in their systems. It builds gradually—one tool, one workaround, one decision at a time—until the environment becomes harder to see clearly and harder to manage with confidence.

What this process offers is a way to reset. Not by replacing everything, but by understanding what you have, simplifying where you can, and putting the right structure in place so it stays under control.

If you're not sure where your environment stands—or if you suspect there are gaps you can't quite see—it's worth taking a closer look. We work with businesses across Southeastern Massachusetts to bring clarity, stability, and confidence to their systems.

Start with a conversation. Schedule a discovery call, and we'll help you understand where you are, what matters most, and what to do next.

Systems Support
IT Support & Service Since 1989

462 Plain Street Suite 206
Marshfield, MA 02050
www.systemsupport.com
Phone: 781-661-5619
Email: info@systemsupport.com