M365 Data Management Checklist

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

1 Identity & Access

WHO CAN REACH WHAT — AND SHOULD THEY?

- ☐ Multi-factor authentication is enforced for every user — including leadership
- ☐ No shared logins or generic accounts exist
- ☐ Access to client and project files is limited to the people working on them
- ☐ Guest and contractor access is time-limited and reviewed when engagements end
- ☐ Former employee accounts are disabled promptly and their data is transferred to company-owned locations

Access should reflect today's reality, not last year's decisions.

2 Email

YOUR MOST-USED TOOL IS YOUR MOST-EXPOSED.

- ☐ All staff use company Outlook accounts exclusively for business communications
- ☐ Automatic forwarding to external addresses is disabled
- ☐ Important client and project emails are saved to a shared location — not just individual inboxes
- ☐ Email is not being used as the organization's primary document storage system

Your email isn't a filing system, it's a quagmire.

3 Files & Structure

REDUCE SCAVENGER HUNTS

- ☐ Every active client or project has one defined home in a company-owned location (SharePoint, not personal OneDrive)
- ☐ There is a consistent folder structure or naming convention across projects and clients
- ☐ A new employee could find an active project's files without a guided tour
- ☐ There is a single source of truth for the current version of any document

When "where is it?" requires a specific person to answer, the structure isn't working.

4 Sharing & Collaboration

EASY TO SHARE. EASIER TO FORGET.

- ☐ Default sharing is set to internal-only (not "anyone with the link")
- ☐ External shared links have expiration dates
- ☐ Guest access is removed when projects or engagements close
- ☐ The organization can identify every external person with current access to its files.

The most common risk isn't a hacker, it's a door left open.

5 Retention & Lifecycle

WHAT TO KEEP AND WHAT TO DISPOSE

- ☐ The firm has a written retention policy for client files, emails, and records
- ☐ Closed matters are archived or restricted — not left open and searchable indefinitely
- ☐ Holds can be applied when needed without disrupting normal operations
- ☐ Closed matters are archived or restricted — not left open and searchable indefinitely

Keeping everything forever isn't caution. It's a larger target.

Unsure about more than 2 of these Items?

IT'S WORTH A CLOSER LOOK

REVIEW the full guide

SCHEDULE a 15-minute discovery call

TAKE our BC/DR Assessment

How Massachusetts Businesses Are Losing Control of Their Most Valuable Asset

Most businesses in Greater Boston and across Southeastern Massachusetts aren't one bad decision away from a data crisis. They're one unconsidered habit away.

The problem isn't that organizations ignore security. It's that the tools they rely on most — Microsoft 365, SharePoint, Teams, Outlook — are flexible enough to work without structure, and most businesses never define one. Files follow people instead of the organization. Access persists long after it should. Data accumulates without a lifecycle. And the risk grows quietly, invisibly, until something breaks.

In Massachusetts, the stakes are unusually high. The state maintains one of the strictest data security laws in the country — 201 CMR 17.00 — requiring any business handling personal information of Massachusetts residents to maintain a documented, actively managed Written Information Security Program. As of early 2026, the state has already recorded 611 reported data breaches affecting nearly 300,000 residents. That number will grow.

The incidents aren't hypothetical. This April alone, Signature Healthcare's Brockton Hospital was hit by the Anubis ransomware group, forcing two weeks of downtime, ambulance diversions, and suspended cancer treatments. A regional emergency communications center in northern Massachusetts serving four towns was taken offline by a cyberattack, disrupting public safety infrastructure across multiple communities. And in March, LexisNexis — a platform used by law firms, financial institutions, and government agencies across the region — confirmed a significant cloud breach traced to an unpatched vulnerability and a hardcoded weak password.
These aren't anomalies. They're a pattern — and it reaches across every industry.

What authoritative sources agree on:

The NIST Cybersecurity Framework defines five functions every organization must address: Identify, Protect, Detect, Respond, and Recover. Most small and mid-sized businesses address only one or two — usually Protect — while leaving the others to chance.

Microsoft's April 2026 security update patched 168 vulnerabilities, including an actively exploited zero-day in SharePoint Server that allows attackers to impersonate users and access sensitive documents without interaction. Organizations that haven't patched are currently exposed.

Massachusetts 201 CMR 17.00 requires a Written Information Security Program (WISP), access controls, encryption of personal data in transit and on portable devices, employee training, and a documented incident response procedure — for every business handling personal information, regardless of industry.

Professional services firms — law, accounting, healthcare, financial management, engineering — face additional obligations through industry-specific regulations, client expectations, and fiduciary duties that raise the bar above the statutory minimum.

The core finding:

The gap between what Massachusetts businesses have (Microsoft 365) and what they use (a fraction of its governance and security capabilities) is where most risk lives. The solution is not new technology. It is data discipline — clear ownership, intentional structure, controlled access, and a defined lifecycle for every piece of information the business holds.

That discipline is achievable. It requires the right guidance, the right configuration, and the willingness to make a few decisions before a crisis makes them for you.

Data Entry Points

KNOW YOUR FRONT DOORS.

Most people think about data management as a storage problem — where files end up. But the real question starts earlier: how does information get into your environment in the first place?
In a typical business, data enters through more doors than anyone realizes. A client sends an email with attachments. Someone fills out a form on your website. A team member scans a document at the front desk or snaps a photo on their phone. A third-party system — billing, CRM, project management — generates records that may or may not sync with Microsoft 365.
Each of these entry points creates a small decision: does this data land somewhere structured and intentional, or does it sit in an inbox, a personal drive, or a device until someone remembers to move it?
Most organizations have never mapped these entry points. That means data is entering the system through doors nobody is watching — and the first gap in the flow happens before anyone has saved a single file.

Check each entry point your organization uses:

☐ We can identify every way client or company data enters our Microsoft 365 environment (email, forms, scans, mobile devices, third-party systems)

☐ Data from each entry point reliably lands in a company-owned, structured location — not just an inbox or personal drive

Identity & Access

WHO CAN REACH WHAT — AND SHOULD THEY?

Access is the foundation of data security — and in most organizations, it's also where the most invisible risk accumulates.

The pattern is remarkably consistent. When someone joins a project, they get access. When a contractor comes on board, they get a guest account. When a colleague needs a file, someone shares a folder. Each decision is reasonable in the moment.

The problem is that almost none of these decisions get revisited.

Over time, access stops reflecting intent and starts reflecting history. People who left the company months ago still have active accounts or lingering permissions. Contractors who finished their work last quarter still have guest access to project folders. Team members have visibility into files they no longer need — not because anyone decided they should, but because nobody decided they shouldn't.

Multi-factor authentication is the single most effective technical control against unauthorized access. Microsoft's own data shows that accounts protected by MFA are 99.9% less likely to be compromised. In Massachusetts, 201 CMR 17.00 requires that access to personal information be restricted to those with a legitimate business need — and "we never got around to removing it" doesn't qualify.

The question isn't whether your people are trustworthy. It's whether your system reflects who actually needs access today.

Check each item that applies to your organization:

☐ Multi-factor authentication is enforced for every user — including leadership

☐ No shared logins or generic accounts exist

☐ Access to client and project files is limited to the people working on them

☐ Guest and contractor access is time-limited and reviewed when engagements end

☐ Former employee accounts are disabled promptly and their data is transferred to company-owned locations

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

Email

YOUR MOST-USED TOOL IS YOUR MOST-EXPOSED.

Email is the center of gravity for most organizations. It's where client communication lives, where documents get exchanged, where decisions are made and confirmed. It's also the single most common path through which data leaves a business — intentionally or otherwise.

The risk isn't just phishing or malware, though those are real. The quieter risk is structural: email becomes, by default, the organization's filing system. Important documents live as attachments in individual inboxes. Client histories exist only in threads that nobody else can access. Institutional knowledge sits in one person's mailbox — and if that person leaves, the knowledge goes with them.

When firms tell us "we know where everything is," what they often mean is "the person who handled that account knows where it is, and it's probably in their email." That works right up until it doesn't.

Beyond storage, email is also where configuration matters most. Automatic forwarding to external addresses — a feature some employees set up for convenience — can silently route every incoming message to a personal account. External sender warnings help staff identify spoofed messages. And encryption, which Microsoft 365 supports natively, is often the difference between a compliant communication and an exposure — particularly under Massachusetts law, which requires encryption of personal information transmitted over public networks.

Check each item that applies to your organization:

- ☐ All staff use company Outlook accounts exclusively for business communications
- ☐ Automatic forwarding to external addresses is disabled
- ☐ Important client and project emails are saved to a shared location — not just individual inboxes
- ☐ Email is not being used as the organization's primary document storage system

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

Files & Structure

NO MORE SCAVENGER HUNTS

This is where most organizations feel the friction of unmanaged data — even if they can't name it.

Microsoft 365 offers multiple places to store files: SharePoint, OneDrive, Teams, Outlook attachments, even OneNote. Each has a purpose. The problem is that without clear guidance, people use whichever one is fastest in the moment. A draft gets saved to OneDrive because it's convenient. A final document gets shared in a Teams chat because the meeting is happening right now. An attachment gets downloaded to a desktop because someone needs to edit it offline.

None of these are bad decisions individually. But collectively, they create an environment where the same document might exist in four different locations — and nobody can say with confidence which one is current.

The deeper issue is ownership. OneDrive is a personal workspace. It's tied to an individual's account. When that person leaves the organization, their OneDrive is typically deactivated within a set period — and anything stored only there becomes difficult to access. SharePoint, by contrast, is a company-owned location. It persists regardless of who comes and goes.

The distinction between OneDrive and SharePoint isn't technical trivia. It's the difference between a filing system that belongs to the business and one that belongs to whoever happens to work there today.

Structure doesn't need to be elaborate. It needs to be predictable. A new employee should be able to navigate to an active project's files without needing someone to translate the system for them. If "where is it?" is a recurring question in your organization, the answer isn't better search — it's better structure.

Check each item that applies to your organization:

- ☐ Every active client or project has one defined home in a company-owned location (SharePoint, not personal OneDrive)
- ☐ There is a consistent folder structure or naming convention across projects and clients
- ☐ A new employee could find an active project's files without a guided tour
- ☐ There is a single source of truth for the current version of any document

Sharing & Collaboration

YOUR MOST-USED TOOL IS YOUR MOST-EXPOSED.

Sharing is where productivity and risk intersect most directly.

Microsoft 365 makes it genuinely easy to share a file with someone outside your organization. A few clicks, a link, and the document is accessible. That speed is valuable — until it isn't.

The issue is what happens after. Most shared links don't expire by default. Most guest accounts aren't time-limited. Most organizations don't have a process for reviewing external access when a project ends or a client relationship pauses. The result is a slow accumulation of open doors that nobody is tracking.

This isn't theoretical. In a typical M365 environment that's been in use for two or three years, there are dozens — sometimes hundreds — of active shared links pointing at files or folders that the organization has forgotten about. No breach. No incident. Just access that was granted for a reason and stayed long after the reason ended.

The fix is usually straightforward. Microsoft 365 allows administrators to set default sharing to internal-only, require authentication for external access, enforce link expiration, and review guest accounts on a schedule. These aren't advanced features. They're settings — and most organizations have never changed them from the defaults.

Under Massachusetts 201 CMR 17.00, organizations are expected to maintain reasonable control over who can access personal information. "We're not sure who has access" is not a defensible position — and it's more common than most businesses realize.

Check each item that applies to your organization:

- ☐ Default sharing is set to internal-only (not "anyone with the link")
- ☐ Automatic forwarding to external addresses is disabled
- ☐ Important client and project emails are saved to a shared location — not just individual inboxes
- ☐ Email is not being used as the organization's primary document storage system

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

Files & Structure

NO MORE SCAVENGER HUNTS

Most organizations default to one of two approaches to data retention: keep everything forever, or delete things randomly when someone panics.

Neither is a strategy.

The instinct to keep everything is understandable. Storage is cheap. Deleting feels risky. And there's always the possibility that someone might need something later. But indefinite retention has real costs that aren't obvious until they matter.

If there's ever a data breach, attackers get access to the full archive — not just recent files, but years of accumulated emails, documents, and records. If there's ever a legal dispute, the organization may be required to produce and review everything it has — and "everything" is a lot more expensive to process when it includes a decade of unmanaged data. If there's an audit, the scope of what needs to be explained grows with every year of unreviewed accumulation.
On the other side, deleting without a policy creates its own risk. Records that the organization is legally required to retain — financial documents, employment records, client files subject to regulatory requirements — can be inadvertently destroyed. And if litigation is anticipated or underway, the duty to preserve evidence means that routine deletion can become spoliation.

The solution is a defined lifecycle. Not every document needs the same treatment. Active projects need full access. Completed work needs to be archived — accessible if needed, but not sitting in the daily workflow. Records with legal or regulatory retention requirements need to be identified and governed accordingly. And data that has outlived its purpose needs to be disposed of intentionally, not left to accumulate indefinitely.

Microsoft 365 provides tools for all of this — retention policies, retention labels, legal holds, and automated archiving through Microsoft Purview. But these tools require decisions before they can function. You can't configure a retention policy until you've decided how long you want to keep things. You can't automate archiving until you've defined what "done" means for a project.

Check each item that applies to your organization:

- ☐ The organization has a written retention policy for client files, emails, and business records.
- ☐ Completed projects are archived or restricted — not left open and searchable indefinitely
- ☐ Legal holds can be applied when needed without disrupting normal operations
- ☐ The organization is not keeping everything forever by default

Need a Closer Look?

This checklist is designed to do one thing: help you see your Microsoft 365 environment more clearly than you did before you started.

If you checked most items confidently, you're ahead of the majority of organizations we work with. That's worth recognizing — and worth maintaining. The environment changes as people join, leave, and create new projects. What's organized today can drift without periodic review.

If you found significant gaps, that's not an indictment. It's the natural outcome of a flexible, powerful tool used without deliberate governance. Microsoft 365 doesn't force structure. It offers options. And when structure is optional, most organizations default to whatever is fastest — which means the system grows around convenience rather than coherence.

The path forward isn't a massive reorganization. It's a small number of durable decisions — about ownership, access, structure, and lifecycle — that hold up under the pressure of daily work. Let's 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