SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR TEAMS MOVING TO OR CLEANING UP MICROSOFT 365

The Microsoft 365 Done Right Playbook.

A zero downtime migration plan, the default settings that leave you exposed, the backup Microsoft does not provide and a SharePoint and Teams structure that stays tidy.

INSIDE THE PLAYBOOK

01 Zero downtime migration
02 Defaults to change
03 Backup for M365
04 SharePoint and Teams

Published by Solution Builders
Bloomington, Minnesota · www.solutionbuilders.com

30+ YEARS
Top 1% OF MSPS
98% CSAT

WHAT'S INSIDE

Built for companies that live in Outlook and Teams.

Microsoft 365 is the most important system most companies run, and the least deliberately configured. Tenants get set up in an afternoon, then carry that afternoon's defaults for a decade. This playbook shows you how to move in cleanly, lock it down and keep it that way.

01 **A zero downtime migration checklist.**
Six phases from discovery to hypercare, what moves and what trips people up, and the cutover weekend plan that means nobody notices on Monday.
PAGE 03

02 **The default settings you must change.**
A new tenant works out of the box. That is the problem. Eight defaults ranked by risk, the fix for each, and why conditional access beats security defaults.
PAGE 06

03 **Why M365 needs its own backup.**
Microsoft runs the service. Your data is your problem, in writing. The recycle bin math, the ransomware gap and what a real Microsoft 365 backup has to include.
PAGE 09

04 **Setting up SharePoint and Teams properly.**
Structure before files. Hub sites, naming, sensitivity labels, guest rules and a lifecycle that retires dead teams, so the tenant looks as good in year five as on day one.
PAGE 12

WHO IT IS FOR
Owners, operations leaders and IT managers at companies with 25 to 500 people who are moving to Microsoft 365 or suspect their tenant was never finished.

HOW TO USE IT
Migrating? Start with chapter 01. Already live? Chapter 02 is a one hour audit. Chapters 03 and 04 are for everyone who owns the tenant.

READING TIME
About 25 minutes cover to cover. The settings table in chapter 02 is built to hand to whoever holds your global admin password.

SOLUTION BUILDERS®

01

A zero downtime migration checklist.

Nobody remembers a migration that went well. They remember the Monday the calendars were empty. Zero downtime is not luck and it is not a feature you buy. It is six phases run in order, with a pilot that fails in private before anything can fail in public.

6
phases, from discovery to hypercare, each with its own exit criteria

0
minutes of user downtime when mail syncs in the background and cutover runs over a weekend

10%
of users in the pilot group is enough to surface most surprises before cutover

90 days
to take an 85 user manufacturer through a full IT transformation, downtime eliminated

Migrations fail in week one, not on cutover weekend.

Every painful migration we have rescued skipped the same step: nobody counted what was actually there. Shared mailboxes, forwarding rules, a PST on the CFO's desktop, a scanner that emails invoices. Discovery is boring. It is also where zero downtime is won.

WEEK 1

Discovery

Inventory mailboxes, files, shared resources, devices and every app that sends email.

WEEK 2

Identity

Clean up Active Directory, sync to Entra ID, assign licenses, turn on MFA before anyone logs in.

WEEK 3

Pilot

Ten percent of users, including one skeptic and one executive assistant. Fix what they find.

WEEKS 4 TO 5

Mail and files

Background sync of every mailbox and file share while people keep working in the old system.

WEEK 6

Cutover and hypercare

Flip MX records on Friday night. Engineers on the floor Monday. Two weeks of fast fixes.

What moves, and what trips people up

WORKLOAD	MOVES HOW	WATCH FOR
Mailboxes	Staged sync, then MX cutover	Oversized items, mailbox rules, delegates
Calendars and contacts	With the mailbox	Room resources, meetings owned by ex staff
Shared mailboxes and lists	Recreated, then synced	Nobody knows who owns them. Decide now.
File shares	SharePoint Migration Tool	Long paths, odd characters, broken permissions
Archives and PSTs	Import service or network upload	PST files on laptops nobody mentioned
Apps that send email	New connector or SMTP relay	Scanners, ERP alerts, website forms

6 wk

typical end to end timeline for a 25 to 500 person company

1

named owner per workload, or it does not move

The exit criteria rule

A phase is done when its checklist is signed, not when the calendar says so. Pilot is done when the skeptic stops filing tickets.

> **Effortless on Monday means exhausting five weeks earlier. That is the trade.**
>
> SOLUTION BUILDERS PROFESSIONAL SERVICES

Nobody should notice on Monday. Here is how.

The cutover itself takes about an hour. Everything that makes it uneventful happens in the ten days before and the ten days after. Print this page, put a name next to every line and do not skip the rollback plan because you feel confident.

Ten days before

- [ ] Confirm every mailbox has synced at least once and the remaining delta is under an hour.
- [ ] Lower the DNS time to live on your MX and autodiscover records to five minutes.
- [ ] Send the "what changes Monday" email with screenshots, twice. People read the second one.
- [ ] Test the scanner, the ERP alerts and the website contact form against the new tenant.
- [ ] Enroll every pilot device in Intune and confirm Outlook opens without a password prompt.
- [ ] Write the rollback plan: who decides, what triggers it and how long it takes.

Cutover weekend

- [ ] Friday 6 p.m.: final delta sync, then switch MX, SPF, DKIM and autodiscover.
- [ ] Saturday: verify inbound and outbound mail from three outside domains, phones included.
- [ ] Saturday: reconnect shared mailboxes, distribution lists and room calendars.
- [ ] Sunday: sign in as five real users on five real devices and send a calendar invite.
- [ ] Sunday night: go or no go call. The rollback window closes at midnight.

Rollback triggers

IF YOU SEE	THEN
Inbound mail failing for 30+ minutes	Revert MX, investigate, retry next weekend
Calendar data missing for a department	Pause, rerun the sync for that batch
A handful of users cannot sign in	Proceed, fix the accounts one by one
Old signatures, missing shortcuts	Proceed, fix in hypercare

Hypercare, the first ten days

1. **Engineers on the floor**
   Monday and Tuesday, in person or on a standing call, so two minute fixes stay two minute fixes.
2. **Daily ticket review**
   Every ticket tagged migration gets read at 4 p.m. Patterns become fixes, not folklore.
3. **Decommission on purpose**
   Old server read only for 30 days, then powered off, then backed up and retired.

Sources: Microsoft Learn, Exchange Online migration and SharePoint Migration Tool documentation; Solution Builders migration runbooks, 2020 to 2026; Solution Builders client engagement, 85 users, manufacturing.

02

The default settings you must change.

Microsoft ships a tenant that is easy to adopt, not hard to attack. Legacy protocols stay open, anyone can forward mail outside, anyone can share a file with the world. None of this is Microsoft being careless. It is Microsoft leaving the decisions to you. This chapter makes them.

99%
of password spray attacks use legacy authentication protocols that cannot do MFA

67%
fewer account compromises in tenants that blocked legacy authentication

99.9%
of account compromise attacks are stopped by multifactor authentication

7,000
password attacks per second blocked by Microsoft, up from 4,000 a year earlier

Eight defaults, ranked by how badly they can hurt you.

Work down this table with whoever holds your global admin password. Most items take under an hour. The first four are the ones attackers test on day one, and the ones your cyber insurer asks about on the renewal form.

SETTING	WHAT IT SHIPS AS	RISK	CHANGE IT TO
Multifactor authentication	Prompted, not enforced, in older tenants	**Critical**	Required for everyone through conditional access, phishing resistant for admins
Legacy authentication	Allowed in tenants created before 2020	**Critical**	Blocked. POP, IMAP and basic SMTP cannot do MFA and attackers know it.
External mail forwarding	Users can auto forward anywhere	**Critical**	Blocked in the outbound spam policy, exceptions approved and logged
Admin accounts	One global admin that also reads email	**Critical**	Two to four cloud only admins with no mailbox, plus two sealed break glass accounts
External sharing	"Anyone with the link" allowed everywhere	**High**	New and existing guests only, links expire in 30 days
User app consent	Anyone can grant an app access to their data	**High**	Admin consent workflow. A rogue OAuth app survives a password reset.
Safe Links and Safe Attachments	Off without Defender for Office 365	**High**	On for everyone, including links in Teams and SharePoint
Audit log retention	On, kept for 180 days	**Medium**	Extended to one year, with alerts routed to a person who acts

< 1 hr
to change most of the settings in this table

2 to 4
global admins is the right number, each with a separate daily account

258
days on average to identify and contain a breach, longer than a 180 day audit log

Sources: Microsoft Learn, Microsoft 365 security baseline and Entra ID documentation; IBM Cost of a Data Breach Report 2024 (time to identify and contain).

Security defaults are the floor. Conditional access is the plan.

Security defaults turn on MFA for everyone and block legacy authentication, and for a ten person company that may be enough. Past that, you need rules that look at who is signing in, from what device, from where, and decide accordingly. That is conditional access.

SECURITY DEFAULTS

One switch, no nuance

- MFA for everyone, but Microsoft decides when to prompt.
- No way to require a managed device or block a country.
- Cannot exclude a break glass account or a conference room PC.

CONDITIONAL ACCESS

Rules you can defend

- Require MFA for all users, phishing resistant for admins.
- Allow Microsoft 365 only from compliant or company owned devices.
- Block sign ins from countries you do not operate in, step up on risk.

Five policies to deploy first

- **Require MFA for everyone.** Every user, every cloud app. Exclude only the break glass accounts, and alert the moment one is used.
- **Block legacy authentication.** One policy closes the door that 99 percent of password spray attacks walk through.
- **Protect admins harder.** Phishing resistant MFA, no persistent sessions, admin portals only from managed devices.
- **Require a healthy device.** Microsoft 365 apps only from Intune compliant or hybrid joined devices. Phones included.
- **Respond to risk.** A risky sign in gets an MFA prompt. A risky user gets a password change. Nobody has to be awake.

Roll it out without locking anyone out

1. **Report only first**
   Run every new policy in report only mode for a week and read what it would have blocked.
2. **Pilot group**
   Enforce for IT and ten volunteers. Fix the copier that uses basic authentication now.
3. **Enforce in waves**
   Department by department, with a one line message the day before.
4. **Review quarterly**
   New apps, new countries, new devices. Policies rot if nobody reads them.

Sources: Microsoft, "New tools to block legacy authentication in your organization," 2020 (legacy authentication figures); Microsoft Digital Defense Report 2024 (password attacks per second); Microsoft, 2019 (MFA effectiveness); Microsoft Entra conditional access documentation.

SOLUTION BUILDERS®

03

Why M365 needs its own backup.

Ask ten business leaders whether Microsoft backs up their email and files, and eight will say yes. Microsoft's own terms say otherwise. The service is extraordinarily reliable. Your data inside it is exactly as safe as your weakest password, your angriest former employee and your most tired admin.

93
days a deleted SharePoint or OneDrive file survives in recycle bins before it is gone

30
days before a deleted user, with their mailbox and OneDrive, is purged by default

59%
of organizations were hit by ransomware in the past year

75%
of enterprises will treat SaaS backup as critical by 2028, up from 15% in 2024

Microsoft runs the service. The data is on you.

Every cloud contract splits responsibility the same way. The provider owns the infrastructure, the uptime and the security of the platform. You own your data, who can reach it and getting it back when something goes wrong. Microsoft is unusually explicit about this.

Who owns what

MICROSOFT IS RESPONSIBLE FOR	YOU ARE RESPONSIBLE FOR
Uptime and a 99.9% financially backed SLA	Your data, and getting it back
Security and patching of the platform	Who has access, MFA, sharing settings
Replication against hardware failure	Accidental deletion, ransomware, insiders
Short recycle bins and version history	Long term retention and legal hold
Keeping the lights on	A copy before someone empties a site

> **We recommend that you regularly backup your content and data that you store on the services.**
>
> MICROSOFT SERVICES AGREEMENT, SECTION 6B

What the built in safety nets actually give you

ITEM	DEFAULT WINDOW	THEN
Deleted email	14 days, 30 at most	Gone
Deleted user and mailbox	30 days	Gone, OneDrive included
Deleted file in OneDrive or SharePoint	93 days, two recycle bins	Gone
Deleted team or group	30 days	Gone, site and chats too
Version history	500 versions	Overwritten, encrypted ones too
Retention policy	As long as you set	Holds items, cannot restore a site

Windows per Microsoft Learn. Admins can extend some of them. An attacker with admin rights can shorten them.

Retention is not backup

Retention keeps copies inside the same tenant, under the admin accounts an attacker just took over. Backup lives somewhere else, under different credentials, and can put a whole site back the way it was on Tuesday.

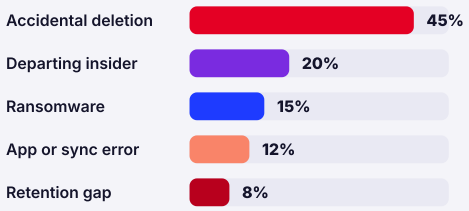
What a real Microsoft 365 backup includes.

A backup that only covers mailboxes is a 2012 backup. Modern tenants keep the business in Teams channels, SharePoint libraries, OneDrive folders and the identity configuration that ties them together. Here is the coverage list to hold any vendor, including us, against.

Coverage checklist

- Exchange: every mailbox, shared mailboxes, calendars, contacts and in place archives.
- OneDrive: every user, including the ones who left last year.
- SharePoint: all sites, libraries, lists, permissions and version history.
- Teams: channels, chats, files and the group settings behind each team.
- Entra ID: users, groups, conditional access policies and app registrations.
- Stored outside your tenant, in a separate cloud, under separate admin credentials, immutable.

How Microsoft 365 data actually gets lost



Illustrative distribution based on Solution Builders restore requests. Ransomware is the smallest slice and by far the most expensive one.

3x
daily backup runs is the norm for mailboxes and OneDrive

22 min
to contain a ransomware attack at a 42 user accounting firm, 100% of data recovered

7 yrs
of retention is the common floor for finance, legal and regulated data

Three questions for any backup vendor

- **How long for a full site restore?** Hours, not days, and they should have done one for a client this quarter.
- **Where does the copy live?** A different cloud or region, immutable, with credentials your admins do not share.
- **Can you restore permissions?** Files without their sharing settings are a second disaster.

Sources: Microsoft Learn, Exchange Online, SharePoint and Microsoft Entra retention documentation; Microsoft Services Agreement; Sophos, The State of Ransomware 2024; Gartner, Magic Quadrant for Enterprise Backup and Recovery Software Solutions 2024. Case data from a Solution Builders client engagement, 42 users, accounting.

04

Setting up SharePoint and Teams properly.

Teams and SharePoint do not get messy. They start messy and never get the structure that would have fixed them. A tenant with 400 orphaned teams and a search box nobody trusts is not a user problem. It is a design that was never done. This chapter is that design.

57%
of a knowledge worker's day is spent communicating in meetings, email and chat

19%
of the work week goes to searching for and gathering information

2
owners minimum on every team, so a departure never strands a workspace

365
day expiration policy, renewable in one click, is how dead teams retire themselves

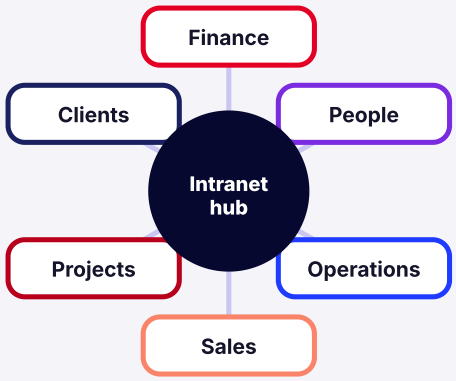
Decide where things live before the first file lands.

Most tenants grow by accident: a team per project, a site per mood, files in chat. The fix is a small set of decisions made once. Flat structure, hub sites for navigation, a naming convention people can guess and a clear answer to "where does this go?"

Six decisions to make first

- **Flat, not nested.** One site per team or function, joined to a hub for navigation. Subsites are where files go to disappear.
- **Who can create teams.** A small group or a request form. Open creation is how you end up with four Marketing teams.
- **A naming convention.** Department, then purpose: FIN Budgeting, HR Onboarding, ACME Rebrand. Short and obvious in search.
- **Private by default.** Private for work, public for reference. Decide once so nobody has to think about it.
- **Where chat ends.** Decisions and files go in a channel, not a private chat. Chat is for coordination, not records.
- **Lifecycle from day one.** Two owners, an expiration date and a review for every team. Dead teams get archived, not haunted.

One hub, flat sites underneath



The new hire test

Pick any new document and ask a new hire where it should go. If the answer takes more than five seconds, the structure is wrong, not the hire.

Where things live

CONTENT	PUT IT IN	NOT IN
Personal drafts and working notes	OneDrive	Email attachments to yourself
Team working files	The team's channel folder	A private chat
Company wide reference	A communication site on the hub	Someone's OneDrive
Client deliverables	A client site with a sensitivity label	A shared mailbox
Records you must keep	A labeled library with retention	A file share nobody backs up

Labels, guests and lifecycle keep it tidy in year five.

Structure gets you a good day one. Three controls keep it that way: sensitivity labels that travel with the file, guest rules that let partners in without leaving the door open, and a lifecycle that retires what nobody uses.

A four label starter set

LABEL	USE IT FOR	WHAT IT DOES
Public	Marketing, published pricing	No restrictions
General	Day to day internal work	Default for new files, blocks anonymous links
Confidential	Client data, finance, HR	Encrypted, internal and named guests only, no download to unmanaged devices
Highly confidential	M&A, payroll, source code	Encrypted, named people only, no forwarding, no copy

Guest access rules

- Guests join by invitation from an owner, never by an "anyone" link.
- Guest accounts expire after 90 days unless an owner renews them.
- Guests see one channel or one site, not the whole team by default.
- Quarterly access review: owners confirm each guest or the guest is removed.
- Block guests from Confidential and above with the label, not with memory.

Team lifecycle in four steps

1. **Request**
   A short form: purpose, two owners, public or private, expected lifespan. Ten minutes, not ten days.
2. **Provision**
   Created from a template with the right channels, label and naming already applied.
3. **Review**
   Owners attest every 365 days with one click. Inactive teams get a nudge, then a deadline.
4. **Archive**
   Read only, searchable, backed up. Deleted only when the retention label says so.

90
day guest expiry, renewable by the owner

2
owners on every team, enforced by the request form

Sources: Microsoft Work Trend Index 2023 (time spent communicating); McKinsey Global Institute, The social economy, 2012 (time spent searching); Microsoft Learn, SharePoint information architecture, sensitivity labels and Microsoft 365 group expiration documentation.

Microsoft 365, migrated and managed.

Solution Builders has run Microsoft environments for Minnesota businesses since 1995. Our 50+ engineers migrate, harden, back up and support Microsoft 365 as one practice, built on the RISE framework and watched by a 24/7 security operations center.

R

Resilient

Microsoft 365 backed up three times a day to a separate cloud, with tested restores.

I

Integrated

Identity, devices, SharePoint and Teams designed as one system, not a pile of settings.

S

Secure

Conditional access, Defender policies and 24/7 monitoring of every sign in.

E

Evolving

A tenant that is Copilot ready, with permissions and labels that AI can respect.

01

Tenant Health Check

A 30 minute review of your Microsoft 365 tenant against the settings table in chapter 02. You leave with your top three fixes.

FREE · 30 MINUTES

02

Microsoft 365 Migration

Discovery to hypercare, run by senior engineers, with a weekend cutover and nobody noticing on Monday.

FIXED FEE · 4 TO 6 WEEKS

03

Managed Microsoft 365

Hardening, backup, licensing, SharePoint governance and support for your people, every month.

MONTHLY · ONGOING

Find out what your tenant is really set to.

Book a free Tenant Health Check with a Solution Builders solution architect. Thirty minutes, no pitch, and a written list of what to change first.

Book my tenant health check

THE SHORT VERSION

Three things to remember.

If this playbook disappears into a drawer, keep these three ideas. They are the difference between a tenant that works for you and a tenant that works against you.

01 **Downtime is a planning failure.**

Count everything in discovery, pilot with a skeptic and cut over on a Friday night with a rollback plan you never need.

02 **Defaults are not a security policy.**

Enforce MFA, block legacy authentication, stop external forwarding and give admins their own accounts. This week.

03 **Microsoft does not back up your data.**

Recycle bins are measured in days. Back up Exchange, OneDrive, SharePoint and Teams somewhere else, and test the restore.

SOLUTION BUILDERS®

START THE CONVERSATION

www.solutionbuilders.com

(952) 854-8188 · 1550 American Blvd East, Suite 900, Bloomington, MN 55425
Your technology partner since 1995

Book a free assessment

© 2026 Solution Builders, Inc. All rights reserved. Product names and marks are the property of their respective owners. Figures marked illustrative are planning estimates, not guarantees.