



COMPUTER TIES IT RESOURCE CENTER • CHECKLIST

Microsoft 365 Administration Checklist

The things somebody in your organization should know about your Microsoft 365 setup, whether or not you administer it yourself.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

Microsoft 365 is usually the most important system a small organization has. It holds the email, the files, the calendars, and the identity every other service signs in with. It is also the system most organizations know least about, because it was set up once and has run ever since.

This checklist is not about how to configure anything. It is about knowing who controls it, who can get back into it, what you are paying for, and whether the protections are actually switched on.

The words you will hear, and what they actually mean

Tenant

Microsoft's name for your organization's own Microsoft 365 space: your users, your email, your files, under your domain name. Your unit in the building, as opposed to the building.

Global administrator

The most powerful account there is. It can change anything, including who else holds power. The master key, and there should be very few copies.

Break-glass account

An emergency administrator account, not used day to day, with its credentials stored offline. The key in the case on the wall. You hope never to need it and you would be very glad it existed.

Legacy authentication

Older sign-in methods that predate multifactor authentication and can bypass it entirely. A side door fitted before the alarm was installed, still connected to nothing.

Conditional access

Rules about who can sign in, from where, and on what. A door policy rather than a lock. Availability depends on your subscription level.

Retention is not backup

Microsoft keeps deleted items for a period, then removes them permanently. That is a grace period, not an archive, and the difference matters the day somebody needs a file from two years ago.

1

Who Actually Owns It

Start here. Everything else depends on the answer.

- ☐ The subscription is in your organization's name, with your billing details, not a supplier's.
If your IT provider bought it under their own account, you may not own what you think you own.
- ☐ At least one person inside your organization holds a global administrator login.
Not your provider. You. This is the account that lets you change providers, recover from a dispute, or get back in if a relationship ends.
- ☐ You know the credentials for that account, and they are stored somewhere safe and reachable.
Somewhere that does not depend on Microsoft 365 being available, since that is exactly when you would need them.
- ☐ You know which domain names are attached, and who controls the registration for each.



- ☐ You know what happens to your data if you stopped paying tomorrow, and how long you would have to retrieve it.
- ☐ Billing goes somewhere the organization monitors, not to one person's inbox.

Our tenant is

Global administrators inside our organization

Who else has administrator access, and why

Where the emergency administrator credentials are kept

2 Administrator Accounts

- ☐ The number of global administrators is small. Two or three is usually right.
Every one of them is a complete set of keys to the organization.
- ☐ You can list them by name, today, and every one of them is somebody who should have it.
- ☐ Administrators use a separate login for administrative work rather than their everyday one.
The everyday account is the one that reads email all day, which is where the risk lives.
- ☐ Two-step sign-in is turned on for every administrator, without exception.
This is the single most important line on this page.
- ☐ There is a break-glass account kept aside for emergencies.
One account, not used day to day, with credentials stored offline, so a lockout or a lost phone does not shut you out of your own organization.
- ☐ Nobody who has left the organization still holds administrative access.
- ☐ Somebody reviews this list at least once a year.

3 Sign-In Protection

- ☐ Two-step sign-in is required for everybody, not offered as an option.
- ☐ You know which accounts are exempt, and why.
Shared mailboxes, meeting-room accounts, and old automated logins are the usual exceptions, and the usual way in.
- ☐ Legacy authentication is blocked, so no older sign-in method can bypass the second step.
- ☐ You would find out about repeated failed sign-ins or a sign-in from somewhere unexpected.
- ☐ Password reset can be done in a way that does not require an administrator every time, without weakening anything.
- ☐ Anyone signing in from outside the country, if that should never happen, would be noticed.



4 Licenses and What You Are Paying For

- ☐ You know how many licenses you are paying for and how many people you employ.
These two numbers drifting apart is the most common wasted spend in Microsoft 365.
- ☐ Licenses belonging to people who have left have been released or reassigned.
- ☐ People are on the level they actually need.
Putting everyone on the most capable plan is easy and expensive. So is putting everyone on the cheapest and then working around the gaps.
- ☐ You know when your subscription renews and whether it renews automatically.
- ☐ You know whether you are on a commitment that cannot be reduced mid-term.
- ☐ Somebody checks the license count against the staff list at least twice a year.

Licenses we pay for

People who need one

Renewal date

Bought through

5 Email Protection

- ☐ Filtering for spam, scams, dangerous links, and dangerous attachments is switched on.
- ☐ Your domain has the records that stop outsiders sending mail that appears to come from you.
Your IT provider will call these SPF, DKIM, and DMARC.
- ☐ Messages from outside the organization are visibly marked as external.
A small change that makes impersonating a colleague much harder.
- ☐ Automatic forwarding out of the organization is blocked or monitored.
Setting up a secret forward is one of the first things an intruder does.
- ☐ Somebody would notice hidden mailbox rules, especially ones that delete or hide replies.
- ☐ Shared mailboxes are set up as shared mailboxes rather than as ordinary accounts with a shared password.

6 Files, Sharing, and Retention

- ☐ You have decided what people can share outside the organization, and with whom.
The default settings are usually more open than most organizations expect.
- ☐ Links that let anybody with the address open a file are limited, or expire.
- ☐ You know which shared areas hold sensitive information and who can reach them.



- ☐ Files are saved into shared storage rather than only onto individual computers.
This is what makes them recoverable, searchable, and available to whoever takes over the work.
- ☐ You know how long deleted items are kept, and it matches what you actually need.
The built-in periods are shorter than most people assume, and they are not a backup.
- ☐ Anything you are legally required to keep is covered by something more deliberate than habit.

Microsoft keeps the service running. Your content is your responsibility

Microsoft's job is to keep Microsoft 365 available. Recovering your email and files after somebody deletes them, or after an account is taken over and files are encrypted, is a separate matter with a limited window. If you would be in trouble without your mailboxes and files, back them up separately.

7 When People Join and Leave

- ☐ New accounts are set up the same way each time, with access based on the job.
- ☐ Two-step sign-in is set up before the person's first day rather than left to them.
- ☐ Leaving accounts are disabled and signed out everywhere the same day.
- ☐ The license is released or reassigned rather than left on a disabled account.
- ☐ Mailboxes and files belonging to people who leave are handled deliberately rather than left indefinitely.
- ☐ Somebody reviews accounts periodically for logins that no longer belong to anybody.

8 Keeping It Running

- ☐ Somebody in the organization would see a Microsoft service notice or an outage announcement.
- ☐ Somebody reviews the security recommendations Microsoft surfaces, rather than nobody ever looking.
- ☐ You know who to contact for support, and whether that is Microsoft directly or your provider.
- ☐ Your setup is written down somewhere other than in one person's head.
- ☐ You have thought about what happens if the person who manages this leaves.
This is the question this whole checklist really exists to answer.



■ Review record

Organization

Completed by

Date

Blank items

Next review

About this checklist

Microsoft changes plan names, features, and default settings regularly. This is general guidance rather than configuration instructions, and it does not describe any particular plan. Confirm current details against Microsoft's own documentation, which is linked from the Computer Ties IT Resource Center. Using Microsoft 365 does not by itself make an organization compliant with HIPAA, CJIS, CMMC, or any other framework.

Not sure who controls your Microsoft 365?

Computer Ties reviews and manages Microsoft 365 for organizations across southern Michigan: ownership and administrator access, sign-in protection, license right-sizing, email security, and the joining and leaving process. If nobody in your organization currently holds an administrator login, that is the first thing worth fixing.

NEW PROJECTS AND PLANNING

(517) 788-6393

EXISTING CUSTOMER SUPPORT

(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990

