



MICROSOFT 365 GOVERNANCE GUIDE FOR NONPROFITS

Make Microsoft 365 easier to manage

A one-hour starting review for nonprofit leaders and their internal or external IT contact. Define who decides, where work belongs and what is checked regularly.

Working method: use the fields as a decision register. Assign a business decision-maker and a technical administrator. Keep completed records internal and record evidence locations instead of secrets.

For a care agency or nonprofit, a new program, staff departure or shared document can cross several tools. Clear responsibilities help staff collaborate without depending on informal access or one person's files.

Tenant / verified domains / administrator contact

Business lead / backup decision-maker / IT management contact

Who approves new accounts, guest access and sensitive sharing?

Who reviews licensing, renewal dates and nonprofit eligibility?

Who approves retention, legal preservation and recovery requirements?

Licenses and nonprofit offers change. Confirm current eligibility, service plans and security features in your tenant before committing to a configuration or cost.



02 / MANAGE IDENTITIES

Make staff changes predictable

Apply one staff-change process across employees, volunteers and vendors. Status: Yes, Partial, No, Unknown or N/A with a reason. [1, 2]

Use individual accounts with appropriate access

Approve access by job and program need. Avoid shared credentials; separate shared workstations from the identities used to reach protected information.

Protect administrators and recovery access

Use separate administrative accounts, multifactor authentication and least privilege. Document emergency access and test recovery with your IT lead.

Choose an MFA baseline that fits the tenant

Have IT assess Security Defaults or an appropriately licensed Conditional Access design. Test sign-in and recovery paths, including shift staff and shared devices.

Review roles, guests and application permissions

Record why access is needed, who approved it and when it ends. Include vendor delegation, app consent and accounts no longer associated with active work.

Departure sequence

At the agreed departure time, block sign-in and revoke sessions. Coordinate device and app access removal. Preserve required email and files, assign a successor and verify their access before deleting accounts or removing licenses. Confirm retention and mailbox-conversion requirements with IT; do not assume deletion windows or licensing rules. [1]

Departure approver / IT executor / data successor / evidence location



03 / PLACE WORK DELIBERATELY

Give shared work a durable home

Use this as a starting model, then record your organization's rules. Microsoft recommends planning SharePoint governance around responsibilities and business needs. [3]

OneDrive: individual work in progress

Set rules for sharing and handing off work. Essential program records should not depend solely on one employee's account.

SharePoint: team and program documents

Name a site lead and deputy. Use groups for access, distinguish internal from external sharing and schedule permission reviews.

Teams and Planner: coordination and follow-through

Define who creates groups, who manages membership and how completed projects are archived. Review the files and connected services behind each workspace.

Forms: approved information collection

Decide who can create forms, which data may be requested and who can read responses. Do not collect participant or clinical data without the organization's approval and suitable controls.

Program / workspace / accountable lead and deputy

--

External sharing rule / access review date / retention and backup decision

--



04 / KEEP IT CURRENT

Use a manageable review rhythm

The schedule below is a suggested starting cadence. Adjust it to staff turnover, service impact, regulatory needs and how often the environment changes.

On every change: Approve staff and vendor access, update license assignments, transfer work and record evidence.

Monthly: Check failed backup jobs, administrative changes, unused accounts, license assignments and unresolved email-delivery issues.

Quarterly: Review guests, group membership, sharing exceptions, vendor access and recovery evidence. Validate one priority collaboration workflow.

Before renewal or a major change: Confirm nonprofit eligibility and current pricing, review required features and budget, and plan migration or offboarding dependencies.

Most important decision / responsible person / due date

--

Next review / evidence location / leadership sign-off

--

Reference guidance

[1] [Microsoft: Remove a former employee - overview](#)

[2] [Microsoft: Multifactor authentication overview](#)

[3] [Microsoft: SharePoint governance overview](#)

Governance starting guide, not certification or a complete retention policy. Validate technical choices and required preservation with the appropriate decision-makers. Reviewed September 8, 2026.

Bitralynx Solutions helps nonprofit teams align identities, collaboration, licensing and ongoing Microsoft 365 management.

Start with a complimentary Technology Readiness Review: one 45-minute conversation and a one-page list of practical priorities. [Book your review](#) or email info@bitralynx.com.