Microsoft 365 Security Check

Your subscription. Your evidence. Your next action.

A practical starting review for any Microsoft 365 subscription, including Business, Enterprise, frontline, and mixed licensing. Allow about 30 minutes for an initial pass; unresolved items may require a service owner or follow-up.

Start with the plan you actually have

Record the licenses and add-ons assigned to each group of users. An available product or admin-center setting is not proof that a capability is licensed for everyone. Conditional Access, endpoint management, threat protection, and data governance vary by plan.

Use this with an authorized administrator and the least-privileged read access appropriate to each service. Review only. Do not change policies, disable protections, or share tenant exports or patient information through a website form.

Organization: _____
Review date / reviewer: _____
Plans and add-ons: _____
Users / roles covered: _____

Record a status, not a universal score

V Verified with evidence **A** Needs attention **L** Licensing need
N Not applicable, with reason **?** Not checked or needs another owner

Use the notes column to record evidence date, affected users, exceptions, owner, and next action. A missing entitlement is a licensing question. A verified setting is not a guarantee of security.

Our licensing recommendation

For organizations with fewer than 300 users, CN generally recommends Business Premium as the core plan, subject to requirements. Eligible nonprofits may receive a substantial discount. For larger organizations, evaluate enterprise/frontline plans and role-specific add-ons. At 300 users, review growth and licensing fit.

Review areas 1-7

Status: V verified / A attention / L licensing / N not applicable / ? not checked

AREA / WHERE TO LOOK	WHAT TO REVIEW	STATUS / EVIDENCE / NEXT ACTION
01 **Assigned licenses** Microsoft 365 admin center	Record assigned plans and add-ons by user group; confirm feature eligibility.	Status: ____ _____ _____
02 **MFA coverage** Entra	Check the current enforcement approach, coverage, registration, and exceptions. Security defaults and licensed Conditional Access are different approaches.	Status: ____ _____ _____
03 **Legacy authentication** Entra	Review policy coverage and recent sign-ins. Record dependencies for administrator follow-up.	Status: ____ _____ _____
04 **Privileged access** Entra roles	Review role assignments, separate admin accounts, emergency-access procedures, and ownership.	Status: ____ _____ _____
05 **Access conditions** Entra / Intune, where licensed	Review device and access requirements, policy state, coverage, and approved exceptions.	Status: ____ _____ _____
06 **Device inventory** Intune or device owner	Compare the managed inventory with devices accessing organizational information.	Status: ____ _____ _____
07 **Device compliance** Intune, where licensed	Review compliance policy coverage and evidence of enforcement through the chosen access controls.	Status: ____ _____ _____

Review areas 8-14

Status: V verified / A attention / L licensing / N not applicable / ? not checked

AREA / WHERE TO LOOK	WHAT TO REVIEW	STATUS / EVIDENCE / NEXT ACTION
08 **Endpoint protection** Defender or security owner	Check onboarding, protection health, alert ownership, and the licensed product in use.	Status: ____ _____ _____
09 **Updates and encryption** Device management / endpoint owner	Record patch and disk-encryption coverage, exceptions, and recovery-key ownership.	Status: ____ _____ _____
10 **Email authentication** DNS / Exchange owner	Review SPF, DKIM, and DMARC evidence with the domain owner. Record alignment gaps.	Status: ____ _____ _____
11 **Email threat protection** Defender / Exchange, where licensed	Review anti-phishing and malware policies, coverage, quarantine, and alert handling.	Status: ____ _____ _____
12 **Mailbox exposure** Exchange	Review external forwarding, delegated access, and business-approved exceptions.	Status: ____ _____ _____
13 **External sharing** SharePoint / OneDrive	Review organization and site sharing limits, link defaults, guests, and sensitive sites.	Status: ____ _____ _____
14 **Collaboration access** Teams / Microsoft 365 groups	Review guest/external access, owners, membership, and lifecycle responsibilities.	Status: ____ _____ _____

Review areas 15-20

Status: V verified / A attention / L licensing / N not applicable / ? not checked

AREA / WHERE TO LOOK	WHAT TO REVIEW	STATUS / EVIDENCE / NEXT ACTION
15 **Sensitive information** Purview / data owners, where licensed	Identify sensitive data and review the labeling and protection approach in scope.	Status: ____ _____ _____
16 **Data loss prevention** Purview, where licensed	Review policy locations, coverage, mode, alerts, and exceptions against actual entitlements.	Status: ____ _____ _____
17 **Retention and recovery** Service / records owners	Document retention obligations and recovery requirements. Retention alone is not a tested backup strategy.	Status: ____ _____ _____
18 **Logging and response** Security / compliance owners	Review available audit records, alert routes, retention, and incident-response ownership.	Status: ____ _____ _____
19 **AI access readiness** App / data owners	Review permissions, oversharing, connectors, approved data, and human oversight before expanding AI access.	Status: ____ _____ _____
20 **Ongoing ownership** IT / business leadership	Name an owner, evidence location, exception process, review cadence, and next action for every area.	Status: ____ _____ _____

Choose the next action

Prioritize access exposure, critical evidence gaps, and time-sensitive requirements with your IT owner. Agree changes through your normal approval and testing process. For help, start at centerednetworks.com/assessments.html. Scope and fees are agreed in writing.

References checked November 14, 2026

Microsoft 365 plan options

Conditional Access planning

Security defaults

Microsoft nonprofit offers