



MICROSOFT 365 · CHECKLIST

Microsoft 365 Security Checklist

Review the Microsoft 365 settings that matter most, from MFA and administrator protection to forwarding rules, sharing and audit logging.

Who this is for

Microsoft 365 administrators, and business owners who manage their own Microsoft 365 tenant. Some user-level checks can be completed by any staff member.

How to use it

- Part A can be completed by any user for their own account.
- Part B requires a Microsoft 365 administrator. Only authorised administrators should change tenant settings.
- Record anything that needs attention in the follow-up actions table.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.

Organisation

Review date

Reviewed by

Microsoft 365 licence plan(s)

Capabilities and licensing vary

Microsoft 365 features, admin centre locations and available settings change over time and depend on your licence. Some checks, such as Conditional Access or longer audit retention, need specific plans. If a feature is not available, record it in the notes and consider alternative controls.

This checklist is not a guarantee

Completing this checklist does not guarantee that your tenant is secure. It covers common, important settings. A thorough review considers your users, devices, data and how your business works.

Part A: User-level checks

Done	Item
☐	MFA is set up on my account An authenticator app or security key is registered, not just SMS where stronger options are available.
☐	My recovery methods are current My recovery phone and email are correct and belong to me.
☐	I have reviewed my recent sign-in activity My Account (myaccount.microsoft.com) shows no sign-ins I do not recognise.
☐	My mailbox has no unexpected forwarding or rules Outlook settings show no forwarding or inbox rules I did not create.
☐	My shared files are still appropriate OneDrive files shared with people outside the business are still needed.

Part B: Administrator-only tasks**Identity and access**

Done	Item	Notes
☐	MFA is enforced for all users Through security defaults or Conditional Access, depending on licence.	
☐	Authentication methods are reviewed Stronger methods are preferred, and weak or unused methods are disabled where possible.	
☐	Administrator accounts are protected Admin roles use separate, MFA-protected accounts that are not used for email or everyday work.	
☐	Least-privilege access is applied Users have the lowest admin role that lets them do their job. Global Administrator is limited to a small number of accounts.	

Done	Item	Notes
☐	User access is reviewed Accounts, licences, group memberships and guest users are reviewed and unused access is removed.	
☐	Sign-in activity is reviewed Sign-in logs are checked for unfamiliar locations, failures and risky sign-ins where available.	
☐	Legacy authentication exposure is checked where applicable Older protocols that cannot use MFA are blocked unless there is a documented need.	

Email

Done	Item	Notes
☐	Mailbox forwarding rules are reviewed Automatic forwarding to external addresses is blocked or monitored, and suspicious inbox rules are investigated.	
☐	Email authentication is configured SPF, DKIM and DMARC records are set up for your domains.	

Data and sharing

Done	Item	Notes
☐	External sharing settings are appropriate SharePoint and OneDrive sharing levels match how your business works, and anyone-with-the-link sharing is restricted.	
☐	OneDrive and SharePoint access is reviewed Site owners and permissions are correct, and former staff do not retain access.	
☐	Recovery readiness is confirmed You understand Microsoft's retention limits and have a separate backup for data you cannot afford to lose.	

Monitoring and lifecycle

Done	Item	Notes
☐	Audit logging is turned on Unified audit logging is enabled, and you know how long logs are kept on your licence.	
☐	Security alerts are monitored Alert notifications go to someone who reviews and acts on them.	
☐	Departing employees are offboarded promptly Accounts are blocked, sessions revoked and data ownership transferred when someone leaves.	

Follow-up actions

Action needed	Responsible person	Target date	Completed

Need a hand?

Omicron I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.