Microsoft 365 Security Assessment Checklist

A practical review of the Microsoft 365 settings that matter most, for MSPs assessing a client tenant.

How to use it: work through each check in the client's admin centres, mark Pass, Gap or N/A, and note the evidence. Every Gap is a remediation task, and usually a project to quote.

Identity and access

CHECK	STATUS	NOTES
Every user has MFA registered Entra admin centre: authentication methods activity.	☐ Pass ☐ Gap ☐ N/A	
MFA is enforced by policy, not just registered Conditional Access policies, or Security Defaults if the tenant has no Entra ID P1.	☐ Pass ☐ Gap ☐ N/A	
Legacy authentication is blocked Older protocols such as basic-auth POP, IMAP and SMTP skip MFA entirely.	☐ Pass ☐ Gap ☐ N/A	
Admin roles are held by separate admin accounts Day-to-day accounts should not hold Global Administrator.	☐ Pass ☐ Gap ☐ N/A	
Global Administrators are kept to a small number Microsoft recommends fewer than five.	☐ Pass ☐ Gap ☐ N/A	
Admins use stronger MFA than SMS Authenticator app, passkeys or security keys.	☐ Pass ☐ Gap ☐ N/A	
Emergency access accounts exist and are documented Monitored, excluded carefully from policies, credentials stored securely.	☐ Pass ☐ Gap ☐ N/A	
Inactive accounts are disabled No sign-in for 90 days or more, including leavers.	☐ Pass ☐ Gap ☐ N/A	
Guest accounts are reviewed Remove guests who no longer need access.	☐ Pass ☐ Gap ☐ N/A	

Email security

CHECK	STATUS	NOTES
SPF is published for every sending domain	☐ Pass ☐ Gap ☐ N/A	
DKIM signing is enabled for every domain	☐ Pass ☐ Gap ☐ N/A	
DMARC is published, ideally at quarantine or reject A p=none policy only monitors.	☐ Pass ☐ Gap ☐ N/A	

Automatic forwarding to external addresses is blocked A common route for data loss after a compromise.	☐ Pass ☐ Gap ☐ N/A	
Mailbox and unified audit logging are on Needed for any incident investigation.	☐ Pass ☐ Gap ☐ N/A	

Data and sharing

CHECK	STATUS	NOTES
SharePoint and OneDrive external sharing is no wider than needed	☐ Pass ☐ Gap ☐ N/A	
"Anyone" links expire, or are turned off	☐ Pass ☐ Gap ☐ N/A	
Teams external access and guest access match the client's policy	☐ Pass ☐ Gap ☐ N/A	

Devices

CHECK	STATUS	NOTES
All Windows devices run a supported version Unsupported versions no longer receive security updates.	☐ Pass ☐ Gap ☐ N/A	
Devices are managed and compliant Intune or your RMM.	☐ Pass ☐ Gap ☐ N/A	

Licensing and cost

CHECK	STATUS	NOTES
No paid licences sit unassigned	☐ Pass ☐ Gap ☐ N/A	
Licences are not assigned to disabled or former users	☐ Pass ☐ Gap ☐ N/A	
Licence tiers match what users actually need	☐ Pass ☐ Gap ☐ N/A	

Monitoring

CHECK	STATUS	NOTES
Microsoft Secure Score is reviewed and trending up	☐ Pass ☐ Gap ☐ N/A	
Alert policies notify someone who will act on them	☐ Pass ☐ Gap ☐ N/A	

Run these checks in minutes. MSPSnaps reads Microsoft 365, Autotask and NinjaOne read-only and turns the gaps into branded client reports with projects to quote. Start free at mspsnaps.com.

This checklist is a general guide, not a complete security audit. Settings and recommendations change; confirm against current Microsoft documentation.