Cybersecurity Basics

ComplyClinic Playbook

Microsoft 365 Security Baseline Checklist

A practical checklist for improving Microsoft 365 security without overcomplicating the environment.

Audience: Organizations using Microsoft 365 for email, files, collaboration, and identity.

General educational resource only. This is not legal advice, certification advice, or a substitute for a formal security risk analysis, CMMC assessment, or incident response engagement.

Identity and access

Require MFA for all users, with stronger methods for admins. Disable legacy authentication. Use separate admin accounts. Review privileged roles monthly.

Create a break-glass account with strong controls and documented emergency use procedures.

Email protection

Configure SPF, DKIM, and DMARC. Enable anti-phishing policies, safe attachments, safe links where licensed, external sender warnings, and user reporting.

Monitor forwarding rules and suspicious inbox rules.

SharePoint and OneDrive

Review external sharing settings, anonymous links, guest access, and sensitive folders. Limit broad sharing and use expiration dates where appropriate.

Create a process for quarterly file sharing reviews for finance, HR, customer, patient, or contract data.

Device access

Require compliant or managed devices for sensitive data where possible. Enforce screen lock, encryption, patching, and endpoint protection.

Separate personal device convenience from sensitive business access.

Logging and monitoring

Enable unified audit logging, review risky sign-ins, monitor impossible travel, and retain logs based on business and compliance needs.

Small businesses do not need a massive SOC to start. They do need enough visibility to investigate suspicious activity.

Offboarding

Disable accounts quickly, revoke sessions, transfer ownership of files, remove mobile access, and review mailbox delegation.

Offboarding is one of the most common places where sensitive access lingers.

Quick-win order

First: MFA and admin review. Second: email authentication and phishing controls. Third: external sharing review. Fourth: logging and offboarding documentation.

Next step: Book a Microsoft 365 security baseline review to identify quick wins and high-risk gaps. Schedule now

Need help turning this into a practical roadmap? Book a free consultation at complyclinic.com.

ComplyClinic • Practical cybersecurity, compliance readiness, automation, app development, and AI governance support.