Integris.

Microsoft 365 security checklist

Here are the key security areas to consider for comprehensive Microsoft 365 security controls.

Authentication and identity management

- □ Verify Microsoft Entra ID (formerly Azure Active Directory) is properly configured.
- □ Enforce multifactor authentication (MFA) for all users.
- □ Implement conditional access policies (based on location, device, role).
- □ Eliminate legacy authentication protocols.
- □ Enable single sign-on (SSO) where applicable.

Data protection and loss prevention

- □ Define and implement data loss prevention (DLP) policies using Microsoft Purview.
- □ Classify and label sensitive information using Microsoft Information Protection.
- □ Ensure proper data encryption at rest and in transit.
- □ Configure data retention and deletion policies for regulatory compliance.
- □ Validate access permissions to ensure only authorized users can access sensitive data.

Email and threat protection

- □ Configure Microsoft Defender for Office 365 settings for anti-phishing, anti-malware, and spoofing protection.
- □ Block malicious email attachments and URLs.
- □ Set up safe links and safe attachments policies.

Collaboration tool security (Exchange, SharePoint, Teams)

- □ Review and update Exchange Online rules and settings.
- □ Configure secure sharing and access settings in SharePoint Online.
- □ Limit guest access in Microsoft Teams to appropriate channels.
- □ Restrict content sharing based on sensitivity labels.
- □ Monitor audit logs for suspicious collaboration activity.

Endpoint and mobile device management

- □ Deploy Microsoft Intune for centralized device management.
- □ Automate device onboarding and provisioning across platforms.
- □ Enforce device compliance policies (encryption, password strength, OS version).
- □ Enable remote device wipe for lost/stolen devices.

Endpoint and mobile device management (continued)

- □ Ensure regular deployment of updates and applications.
- □ Compliance, governance and risk management.
- □ Configure Microsoft Purview compliance portal for centralized policy management.
- □ Implement data lifecycle and retention policies.
- □ Monitor compliance scores and address improvement actions.
- □ Assign compliance roles and responsibilities.
- □ Align M365 configurations with standards like HIPAA, GDPR, or CMMC.

Licensing and optimization

- □ Review current Microsoft 365 licenses and identify underused services.
- □ Align licensing with business needs and user roles.
- □ Identify opportunities to consolidate tools and reduce costs.

Monitoring, reporting, and alerting

- □ Set up security information and event management (SIEM) integration if applicable.
- □ Monitor audit logs, activity reports, and sign-on reports for anomalies.
- □ Configure alert policies for suspicious or risky behavior.
- □ Review and adjust policies regularly based on threat intelligence.

User awareness and training

- □ Implement ongoing security awareness training for employees.
- □ Include training on phishing, password hygiene, and data handling.
- □ Provide role-specific guidance for admins and high-privilege users.

Engage a trusted managed service provider (MSP)

- □ Schedule a Microsoft 365 security assessment with a qualified MSP like Integris.
- □ Review detailed findings and recommended remediations from the assessment.
- □ Implement ongoing support, monitoring, and governance.

Next steps

Integris can help you take back the reins on your cybersecurity posture by assessing your current state, identifying gaps in your use of Microsoft 365, optimizing licensing, and centralizing management of key cybersecurity areas.

If you have any questions or need assistance with your Microsoft 365 security journey, don’t hesitate to reach out to your Integris contact or visit integrisit.com.