

Microsoft 365 Security Best Practice Checklist

This checklist consolidates all critical security domains including identity, access, data, devices, and monitoring into one comprehensive tool. Use it as a living document to regularly evaluate and strengthen your Microsoft 365 security posture.

Action Item	Assigned to	Due Date	Notes	✓
IAM BEST PRACTICE				
MFA enabled for all users and monitor MFA status				
Prioritize admin accounts				
Require use of authenticator app and phishing-resistant methods				
Offer user communication and training				
Strengthen password policies and introduce passwordless authentication where possible				
Introduce risk-based conditional access policies				
Enforce privileged identity management (PIM), i.e., limit admin accounts, adopt delegated permissions, RBAC				
Control external and guest access				
Reduce privileged Entra app access, review regularly				
Continuously examine your least privilege posture				
ATP BEST PRACTICE				
Configure safe attachments				
Enable safe links				
Block high-risk file types and OLE macros				
Block external email auto-forwarding				
Enable zero-hour auto purge (ZAP)				
Enable Threat Explorer for hunting				
Enable anti-phishing policies				

Action Item	Assigned to	Due Date	Notes	✓
Enable domain protection				
Configure email authentication				
Enable Defender for Endpoint EDR				
Enable alert policies for suspicious patterns				
INFORMATION PROTECTION AND GOVERNANCE BEST PRACTICE				
Define data classification taxonomy				
Implement Sensitivity Labels with encryption and monitoring				
Deploy auto-labeling policies				
Implement DLP policies				
Integrate DLP with Sensitivity Labels				
Configure retention labels and policies				
Encrypt sensitive content at rest and in transit				
Use Microsoft Purview Information Protection Scanner				
Configure insider risk management				
Block download of sensitive content to unmanaged devices				
Apply file block settings in Office apps				
Set default link types for sharing				
Choose a vendor for tenant configuration backup				
Inventory critical M365 tenant configurations				
Establish tenant security baselines				
Initiate full tenant configuration backup				
Enable continuous drift detection				
Store and version backups				

Action Item	Assigned to	Due Date	Notes	✓
Test and validate restore procedures				
Automate tenant configuration backup and response				
Enable records management for regulatory data				
Enable audit log retention beyond defaults				
Configure alerts for suspicious file activity				
DEVICE MANAGEMENT BEST PRACTICE				
Require device enrollment and management				
Enforce device compliance policies				
Require OS and security patch compliance				
Remove unused or stale devices				
Enforce device integrity checks				
Use conditional access to enforce compliance				
Enable full disk encryption				
Limit admin access to managed devices only				
Enforce device risk-based access control for dynamic security				
Apply app protection policies for BYOD				
Deploy MS Defender for Endpoint (MDE)				
Configure attack surface reduction (ASR) rules				
Enable mobile threat defense integration for mobile security				
Block unsupported or jailbroken devices				
Implement device risk scoring and alerts				

Action Item	Assigned to	Due Date	Notes	✓
APPLICATION AND COLLABORATION HARDENING BEST PRACTICE				
Limit and manage external sharing				
Enforce guest access controls and expiration				
Configure Teams security and governance policies				
Monitor and alert on suspicious file sharing				
Apply default link types and expiration dates				
Block tenant creation and unapproved app registrations				
Enable Safe Links and Safe Attachments across M365 ecosystem				
Disable OLE package and risky embedding features				
Limit creation of public Teams/SharePoint sites				
Block legacy Office add-ins and unsigned macros				
Apply Sensitivity Labels to shared files				
Block downloads of sensitive files to unmanaged devices				
Enable file type blocking in SharePoint and OneDrive				
Require admin approval for app consent				
Use client app policies for mobile access				
Harden Office apps via policy				
MONITORING AND RESPONSE BEST PRACTICE				
Enable and retain unified audit logs (UAL)				
Extend audit log retention beyond defaults				
Configure Admin activity alerts				
Enable user activity alerts for high-risk actions				
Monitor suspicious sign-in activity				

Action Item	Assigned to	Due Date	Notes	✓
Detect and alert on suspicious email activity				
Monitor file activity and data movement				
Configure Automated Incident Response (AIR)				
Integrate with Microsoft Sentinel				
Enable Defender for Cloud Apps (MCAS) alerts				
Implement real-time risk detection with Entra ID protection				
Conduct regular threat hunts				
Create and test incident response playbooks				
SYSTEM SECURITY AND OPERATIONS BEST PRACTICE				
Regularly review Microsoft Secure Score				
Map controls to security frameworks (NIST, CIS, ISO)				
Conduct periodic phishing simulations				
Automate security reporting for executives				
Schedule security audits and access reviews				
Run Zero Trust gap analyses regularly				
Maintain and enforce security baselines				
Implement change control and documentation				
Perform regular patch management				
Test and validate backups for M365 data and tenant configurations				