ECHELON
RISK +
CYBER

Managed Microsoft 365 Security Checklist

Microsoft 365 is at the heart of many organizations' operations, making robust security measures essential to protect your data and users. This checklist highlights critical steps to enhance the security of your Microsoft 365 environment, from implementing multifactor authentication to enforcing data loss prevention policies. Ensure your organization leverages Microsoft 365's advanced capabilities to safeguard against evolving threats.

- [ ] Enforce multifactor authentication (MFA) for all accounts, prioritizing privileged accounts.
- [ ] Configure Entra ID Conditional Access policies to block legacy authentication and require compliant devices.
- [ ] Implement anti-phishing, anti-spam, and anti-malware policies in Exchange Online Protection (EOP).
- [ ] Set up and enforce Data Loss Prevention (DLP) policies to monitor and protect sensitive data.
- [ ] Require and enforce email authenticationprotocols (SPF, DKIM, and DMARC) for all domains.
- [ ] Review and remove inactive user accounts regularly.
- [ ] Implement role-based access control (RBAC) and restrict administrator roles.
- [ ] Require mobile devices to be managed and encrypted via Microsoft Intune.
- [ ] Enable Safe Links and Safe Attachments in Microsoft Defender for Office 365.
- [ ] Actively monitor user activity, system events, and potential security threats through comprehensive logging capabilities within Microsoft 365.

Need help securing your Microsoft 365 environment? Explore how Echelon Risk + Cyber can simplify and strengthen your cybersecurity strategy.