Office 365

Recommended Security Policies

Protection Ongoing - Office 365 Email Hygiene

MIS has worked to develop a set of security policies to ensure your Office 365 E-mail platform strikes the right balance between convenience and security. These policies are the culmination of months of testing and research by our security experts.

Just as the security landscape is everchanging, so too will be our proscribed security policies, dictated by where the next big threat is heading.

Our Office 365 Hygiene program ensures that you are protected by configuring these policies on your behalf with bi-annual reviews to adjust based on the changing security landscape. Our program is only administered by Microsoft Essential certified engineers granting you peace of mind that the policies are configured correctly. While there is no "silver bullet" to provide absolute protection, our hygiene service ensures you are following the best practices to limit your exposure.

If you would like to learn more about how to protect your Office 365 email platform with our Office 365 email hygiene service, please contact your account manager.

1	Enable mailbox auditing
2	Turn ON unified audit log search
3	Secure Mail Flow: SPF
4	Secure Mail Flow: DKIM
5	Secure Mail Flow: DMARC
6	Secure Mail Flow: rDNS
7	Create custom banned password list
8	Ensure that shared mailboxes have been disabled for sign-in access
9	Eliminate legacy protocols
10	Disable basic authentication
11	Enable multi-factor authentication (MFA)
12	Disable mailbox auto-forwarding to remote domains
13	Block sign-in for all shared mailboxes
14	Adjust anti-spam, anti-malware and outbound spam policies
15	Configure the default Office 365 alert policies
16	Turn on Office 365 Advanced Threat Protection: Safe Links, Safe Attachments, Anti-Phish policy
17	Protect mailboxes with a retention policy or litigation hold
18	Configure Data Loss Prevention policy
19	Set up AD password sync
20	Disable Outlook Web Access (OWA)
21	Configure DLP (Define data exfiltration rules & restrictions)
22	Configure S/MIME Protocol
23	Turn on Cloud App Security
24	Create emergency Global Access Account (GAC)
25	Run Microsoft Secure Score and look for further recommendations
26	Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD)
27	Assign administrator access using RBAC (Role-based Access Controls)
28	Define GEO / IP Filtering access rules
29	Review O365 “Customer Lockbox” settings
30	Turn on Password hash synchronization
31	Configure identity protection
32	Run / verify configuration via Microsoft Secure Score
33	Stop auto-forwarding for email.
34	Enable and configure application consent and permissions
35	Disable 3rd party application integrations.
36	Enable self-service password reset policies

Contact MIS Solutions if you are concerned about gaps in your O365 security

www.mis-solutions.com | 4485 Tench Road, Suite 440, Suwanee, GA 30024 | 678-745-5109