

## 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.

2 Turn ON unified audit log search 3 Secure Mail Flow: DFI 4 Secure Mail Flow: DKIM 5 Secure Mail Flow: DMARC 6 Secure Mail Flow: DMARC 6 Secure Mail Flow: DMARC 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 DLP (Define data exfiltration rules & restrictions) 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 3" party application integrations.	1	Enable mailbox auditing
3 Secure Mail Flow: DFF 4 Secure Mail Flow: DMARC 5 Secure Mail Flow: DMARC 6 Secure Mail Flow: DMARC 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 0365 *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 3 <sup>rd</sup> party application integrations.		<u> </u>
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 basic authentication (MFA) 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 0365 "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 3" party application integrations.	$\vdash$	•
Secure Mail Flow: DMARC  Secure Mail Flow: rDNS  Create custom banned password list  Ensure that shared mailboxes have been disabled for sign-in access  Eliminate legacy protocols  Disable basic authentication  Enable multi-factor authentication (MFA)  Disable mailbox auto-forwarding to remote domains  Block sign-in for all shared mailboxes  Adjust anti-spam, anti-malware and outbound spam policies  Configure the default Office 365 alert policies  Turn on Office 365 Advanced Threat Protection: Safe Links, Safe Attachments, Anti-Phish policy  Protect mailboxes with a retention policy or litigation hold  Configure Data Loss Prevention policy  Set up AD password sync  Disable Outlook Web Access (OWA)  Configure DLP (Define data exfiltration rules & restrictions)  Configure S/MIME Protocol  Turn on Cloud App Security  Create emergency Global Access Account (GAC)  Run Microsoft Secure Score and look for further recommendations  Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD)  Assign administrator access using RBAC (Role-based Access Controls)  Pefine GEO / IP Filtering access rules  Review O365 "Customer Lockbox" settings  Turn on Password hash synchronization  Configure identity protection  Run / verify configuration via Microsoft Secure Score  Stope auto-forwarding for email.  Enable and configure application consent and permissions		
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 3"d party application integrations.	_	
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 3"d party application integrations.		
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 integrations.		
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 integrations.		· · · · · · · · · · · · · · · · · · ·
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 0365 "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 3 <sup>rd</sup> party application integrations.		
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 3 <sup>rd</sup> party application integrations.	$\vdash$	· · · ·
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 3 <sup>rd</sup> party application integrations.		
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.		
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.	-	
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 3 <sup>rd</sup> party application integrations.		· ·
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 3 <sup>rd</sup> party application integrations.	_	• • •
Phish policy  Protect mailboxes with a retention policy or litigation hold  Configure Data Loss Prevention policy  Set up AD password sync  Disable Outlook Web Access (OWA)  Tonfigure DLP (Define data exfiltration rules & restrictions)  Configure S/MIME Protocol  Turn on Cloud App Security  Create emergency Global Access Account (GAC)  Run Microsoft Secure Score and look for further recommendations  Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD)  Assign administrator access using RBAC (Role-based Access Controls)  Define GEO / IP Filtering access rules  Review O365 "Customer Lockbox" settings  Turn on Password hash synchronization  Configure identity protection  Run / verify configuration via Microsoft Secure Score  Stop auto-forwarding for email.  Enable and configure application consent and permissions  Disable 3 <sup>rd</sup> party application integrations.	15	· · ·
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 3 <sup>rd</sup> party application integrations.	16	
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.	17	Protect mailboxes with a retention policy or litigation hold
Disable Outlook Web Access (OWA)  Configure DLP (Define data exfiltration rules & restrictions)  Configure S/MIME Protocol  Turn on Cloud App Security  Create emergency Global Access Account (GAC)  Run Microsoft Secure Score and look for further recommendations  Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD)  Assign administrator access using RBAC (Role-based Access Controls)  Befine GEO / IP Filtering access rules  Review O365 "Customer Lockbox" settings  Turn on Password hash synchronization  Configure identity protection  Run / verify configuration via Microsoft Secure Score  Stop auto-forwarding for email.  Hable and configure application consent and permissions  Disable 3 <sup>rd</sup> party application integrations.	18	Configure Data Loss Prevention policy
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 3 <sup>rd</sup> party application integrations.	19	Set up AD password sync
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 3 <sup>rd</sup> party application integrations.	20	Disable Outlook Web Access (OWA)
Turn on Cloud App Security Create emergency Global Access Account (GAC) Employed Run Microsoft Secure Score and look for further recommendations Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD) Assign administrator access using RBAC (Role-based Access Controls) Befine GEO / IP Filtering access rules Review O365 "Customer Lockbox" settings Turn on Password hash synchronization Configure identity protection Run / verify configuration via Microsoft Secure Score Stop auto-forwarding for email.  Henable and configure application consent and permissions Disable 3 <sup>rd</sup> party application integrations.	21	Configure DLP (Define data exfiltration rules & restrictions)
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 3 <sup>rd</sup> party application integrations.	22	Configure S/MIME Protocol
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 3 <sup>rd</sup> party application integrations.	23	Turn on Cloud App Security
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 3 <sup>rd</sup> party application integrations.	24	Create emergency Global Access Account (GAC)
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 3 <sup>rd</sup> party application integrations.	25	Run Microsoft Secure Score and look for further recommendations
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 3 <sup>rd</sup> party application integrations.	26	Configure mobile device policies (ActiveSync or Office 365 MDM) (TBD)
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 3 <sup>rd</sup> party application integrations.	27	Assign administrator access using RBAC (Role-based Access Controls)
<ul> <li>Turn on Password hash synchronization</li> <li>Configure identity protection</li> <li>Run / verify configuration via Microsoft Secure Score</li> <li>Stop auto-forwarding for email.</li> <li>Enable and configure application consent and permissions</li> <li>Disable 3<sup>rd</sup> party application integrations.</li> </ul>	28	Define GEO / IP Filtering access rules
<ul> <li>Configure identity protection</li> <li>Run / verify configuration via Microsoft Secure Score</li> <li>Stop auto-forwarding for email.</li> <li>Enable and configure application consent and permissions</li> <li>Disable 3<sup>rd</sup> party application integrations.</li> </ul>	29	Review 0365 "Customer Lockbox" settings
<ul> <li>Configure identity protection</li> <li>Run / verify configuration via Microsoft Secure Score</li> <li>Stop auto-forwarding for email.</li> <li>Enable and configure application consent and permissions</li> <li>Disable 3<sup>rd</sup> party application integrations.</li> </ul>	30	Turn on Password hash synchronization
<ul> <li>33 Stop auto-forwarding for email.</li> <li>34 Enable and configure application consent and permissions</li> <li>35 Disable 3<sup>rd</sup> party application integrations.</li> </ul>		Configure identity protection
<ul> <li>34 Enable and configure application consent and permissions</li> <li>35 Disable 3<sup>rd</sup> party application integrations.</li> </ul>	32	Run / verify configuration via Microsoft Secure Score
<ul> <li>Enable and configure application consent and permissions</li> <li>Disable 3<sup>rd</sup> party application integrations.</li> </ul>		
35 Disable 3 <sup>rd</sup> party application integrations.		Enable and configure application consent and permissions
		• ,,
	36	

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