Office 365

aztech IT Solutions

Microsoft 365 Security Audit

Analysis and review for best practices

Ensuring your organisation is protected and secure from cyberthreats is crucial in this modern age.

You need to safeguard your organisation against both internal and external threats, especially when the majority of security breaches in organisations are due to unintentional internal mishaps.

With that in mind, Microsoft 365 is no exception, and making sure your organisation is protected is imperative in keeping your data safe.

Our Microsoft 365 Security Audit is designed to analyse how secure your O365 setup is and discover any vulnerabilities.

We will review your Microsoft 365 tenant to find any areas of concern as well as areas that could be improved upon.

Then we will review your Secure Score to see your organisation's security posture.

The results will highlight areas that need immediate attention and should be corrected to meet best practice standards, as well as areas that are recommended to be updated.

Next, we will compile our findings from the Security Audit and prepare a report.

Our security experts will go through this with you, explaining the results and providing advice and recommendations for security hardening and best practices.

In addition to this, if necessary, further guidance will be provided on how you can continue to improve your cloud security and keep your data safe.

What's Included?

- **Review of your Microsoft 365 Tenant**
  We will analyse and review your O365 tenant
- **Review of your Secure Score**
  We will analyse and review your Secure Score
- **Detailed Report**
  We will provide you with a report and analysis of potential issues we uncover
- **Recommendations and Advice**
  We will discuss the results and provide recommendations for security hardening and best practices

Enhance your security today with an Microsoft 365 Audit from AZTech IT Solutions

www.aztechIT.co.uk | email: info@aztechIT.co.uk | phone: 03300 949 420

aztech IT Solutions

Areas to be reviewed:

Account/Authentication Policies - Recommendations related to setting the appropriate account and authentication policies

- Review multifactor authentication is enabled for all users in administrative roles
- Review multifactor authentication is enabled for all users in all roles
- Review that between two and four global admins are designated
- Review self-service password reset is enabled
- Review modern authentication for Exchange Online is enabled
- Review modern authentication for SharePoint applications is required
- Review modern authentication for Skype for Business Online is enabled
- Review that Microsoft 365 Passwords Are Not Set to Expire

Application Permissions - Recommendations related to the configuration of application permissions within Microsoft 365

- Review third party integrated applications are not allowed (User Settings > No App Registrations)
- Review calendar details sharing with external users is disabled
- Review O365 ATP Safe Links for Office Applications is Enabled
- Review Microsoft 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled (blocks malicious files)

Data Management - Recommendations for setting data management policies

- Review the customer lockbox feature is enabled
- Review SharePoint Online data classification policies are set up and used
- Review external domains are not allowed in Skype or Teams
- Review DLP policies are enabled
- Review that external users cannot share files, folders, and sites they do not own
- Review external file sharing in Teams is enabled for only approved cloud storage services

Email security/Exchange Online - Recommendations related to the configuration of Exchange Online and email security

- Review the Common Attachment Types Filter is enabled
- Review Exchange Online Spam Policies are set correctly
- Review mail transport rules do not forward email to external domains
- Review mail transport rules do not whitelist specific domains
- Review the Client Rules Forwarding Block is enabled
- Review the Advanced Threat Protection Safe Links policy is enabled
- Review the Advanced Threat Protection Safe Attachments policy is enabled
- Review basic authentication for Exchange Online is disabled
- Review that an anti-phishing policy has been created
- Review that DKIM is enabled for all Exchange Online Domains
- Review that SPF records are published for all Exchange Domains
- Review DMARC Records for all Exchange Online domains are published
- Review notifications for internal users sending malware is Enabled

Auditing Policies - Recommendations for setting auditing policies on your Microsoft 365 tenant

- Review Microsoft 365 audit log search is Enabled
- Review mailbox auditing for all users is Enabled
- Review the Azure AD 'Risky sign-ins' report is reviewed at least weekly
- Review the Application Usage report is reviewed at least weekly
- Review the self-service password reset activity report is reviewed at least weekly
- Review user role group changes are reviewed at least weekly
- Review mail forwarding rules are reviewed at least weekly
- Review the Mailbox Access by Non-Owners Report is reviewed at least biweekly
- Review the Malware Detections report is reviewed at least weekly
- Review the Account Provisioning Activity report is reviewed at least weekly
- Review non-global administrator role group assignments are reviewed at least weekly
- Review the spoofed domains report is review weekly
- Review Microsoft 365 Cloud App Security is Enabled
- Review the report of users who have had their email privileges restricted due to spamming is reviewed

Storage Policies - Recommendations for securely configuring storage policies

- Review document sharing is being controlled by domains with whitelist or blacklist
- Review expiration time for external sharing links is set

Mobile Device Management - Recommendations for managing devices connecting to Microsoft 365

- Review mobile device management polices are set to require advanced security configurations to protect from basic internet attacks
- Review that mobile device password reuse is prohibited
- Review that mobile devices are set to never expire passwords
- Review that users cannot connect from devices that are jail broken or rooted
- Review mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise
- Review that settings are enable to lock multiple devices after a period of inactivity to prevent unauthorised access
- Review that mobile device encryption is enabled to prevent unauthorised access to mobile data
- Review that mobile devices require complex passwords to prevent brute force attacks
- Review that devices connecting have AV and a local firewall enabled (Windows 10)
- Review mobile device management policies are required for email profiles
- Review mobile devices require the use of a password