CYBER PATH
POLICE & ACADEMIA
TALENT HORIZONS

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Microsoft 365 Review

Services Provided: XXXXXXXXXXXXXXX

Created for: Engineering Ltd

Report Submitted: 03/01/2026

Student Assessor: Alex Thomas

1. Content

2. Your Assessment 1
2 Microsoft 365 Review 2
2.1 Microsoft 365 Admin Centre 2
2.2 Microsoft 365 Defender 2
2.3 Microsoft Purview 2
2.4 Microsoft Intune Admin Centre 3
2.5 Microsoft Entra Admin Centre 3
2.6 Exchange Admin Centre 3
2.7 SharePoint Admin Centre 3
2.8 Microsoft Teams Admin Centre 3
2.9 Microsoft Fabric 3
About the Cyber Resilience Centre Network 4
There's more to the Cyber Resilience Centres 4
Appendix A - Full results of the Microsoft 365 Review 5

2. Your Assessment

Thank you for entrusting our team at Cyber PATH to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Assessment Information	
Service completed	[redacted]
Assessment Completed By	[redacted]
Date Completed	14/12/2025
Overseen By	Cyber PATH Student Supervisor Savva Pistolas

2 Microsoft 365 Review

[redacted] Microsoft 365 was assessed against Level 1 of the Center for Internet Security (CIS) Microsoft 365 Foundations Benchmark v3.1.0. This benchmark contains a series of suggested settings to increase security within the Microsoft 365 environment above what is provided by default without adding additional complexity to the user experience.

This assessment was conducted against the [redacted] environment using the [redacted] account created for this engagement. This user was granted the Global Reader role allowing read only access to the Microsoft 365 environment.

Forty settings differed from the recommendations from the CIS Benchmark. It is important to note that these recommendations should only be implemented after review. A change may have an impact against current systems in place and should be assessed prior to implementation.

A full list of the failed recommendations can be found in Appendix A - , however, a summary of each section of the CIS Benchmark by section is provided below.

2.1 Microsoft 365 Admin Centre

While many of the settings in this section was already hardened, it was identified that. [redacted] does not currently have any emergency access accounts for the Microsoft 365 environment. These accounts can be used in the unlikely event that the regular Administrator accounts are unavailable.

Cyber PATH identified only a single Global Administrator account had been created within Microsoft 365. Having between two and four Global Administrator accounts provides redundancy if one account becomes compromised or lost, so it is still possible to gain control of the Microsoft 365 environment.

The current configuration allows users to install their own add-ins for Word, Excel and PowerPoint. While these add-ins often add additional functionality to these applications, malicious users commonly use vulnerable or custom add-ins to access the data held in these applications.

2.2 Microsoft 365 Defender

While some of the security settings in this section had been enabled, it was identified that some of the automated blocking and reporting for email messages had not been enabled. As a result, there are currently no notifications if a [redacted] ccount starts sending malware or spam outside the organisation.

No anti-phishing policy has been created. These policies can be used to help protect the organisation against impersonation and spoofing based phishing attacks and enables safety tips to help protect users.

Neither DKIM nor DMARC were enabled. These services add additional protections to your domain name. Strengthening them prevents malicious users from using spoofing techniques to send messages that look like they are coming from your domain. They also increase the trustworthiness of any messages sent by [redacted] by adding a digital signature to all outbound email messages, allowing the recipient to verify that the message is authentic.

2.3 Microsoft Purview

It was identified that none of the policies recommended by the CIS Benchmark were enabled within Microsoft Purview, these include the Audit Role Log, Data Loss Prevention (DLP policies) and SharePoint online information protection policies. These policies ensure that user and administrator activity is recorded and logged, documents and data scanned for potentially sensitive information and all SharePoint data is correctly classified and labelled. These policies can help reduce the risk of sensitive data loss as well as providing information for incident response in the event of a breach.

2.4 Microsoft Intune Admin Centre

This section is intentional blank within the CIS benchmark and exists to ensure the structure of the benchmark is consistent.

2.5 Microsoft Entra Admin Centre

Currently the [redacted] environment uses security defaults which are a series of preconfigured security settings created by Microsoft on all Microsoft 365 instances to help protect against common attacks. This helps to ensure a good basic level of security; however, it may prohibit more advanced settings used by the CIS Benchmark. [redacted] their own requirements alongside those recommended by the benchmark to determine what level of security suits their organisation.

No conditional access policy was created. These policies are used to determine when Multi-Factor Authentication (MFA) should be used, block outdated and legacy authentication methods and apply account limitations based on user role.

2.6 Exchange Admin Centre

Many of the recommended settings from the benchmark had already been enabled for Exchange, however it was identified that Mailbox Auditing had been disabled. This setting enables logging for certain actions and these records are available to search through if required, particularly for scenarios such as incident response and general investigations.

MailTips were also disabled. MailTips are helpful prompts that appear while a user is composing an email and commonly warn users if they are about to email a large number of recipients or are about to send an email to someone outside of the organisation. These tips help users to avoid accidently disclosing sensitive information outside of the organisation and avoiding common mistakes.

2.7 SharePoint Admin Centre

A series of issues with the current sharing permissions was identified within this section. Primarily, content hosted on the SharePoint could be shared with users outside of [redacted] without any restrictions. It could also be shared without requiring authentication. As a result, a malicious user could easily share sensitive files and information outside of the organisation by sharing a link.

2.8 Microsoft Teams Admin Centre

External users can send emails to a user's Team channel, via the channel's email address which is automatically created. These channel email addresses are not under the control of [redacted] and therefore any external user with knowledge of the email address will be able to directly email this channel. This could be a security risk as the email will appear to be from an internal system/user.

Additionally, it was identified that users are currently able to install third-party and unverified apps to the Teams environment which could expose the Teams environment, and the sensitive data held within it to unnecessary risk.

The CIS Benchmark recommends removing external access to the Teams environment. This access is often used to allow members of other organisations to search for and start conversations with [redacted] users over Teams. This functionality can open [redacted] users to attack, but at the same time may also currently be used for legitimate reasons.

2.9 Microsoft Fabric

This functionality was not enabled on this instance of Microsoft 365

About the Cyber Resilience Centre Network

The National Cyber Resilience Centre Group and Cyber Resilience Centres are funded and supported by the Home Office and policing in a not-for-profit partnership with the private sector and academia to strengthen our national cyber resilience across SMEs and the supply chain.

At a national level, NCRCG is building a coalition of police, government, large employers and organisations, and academia to ensure a collaborative and coherent approach to cyber resilience.

NCRCG and its National Ambassadors and the CRC network are committed to investing in the next generation of cyber experts. As such, NCRCG has launched Cyber PATH in partnership with the CRC network and over 45 universities.

The nine CRCs operate across England and Wales. They serve SMEs in their locality helping to build cyber resilience against threats that are specific to them. Cyber PATH empowers students to work with their regional CRC in meeting the requests brought to them by local businesses.

Each CRC retains the freedoms to deliver tailored, trusted and fully funded support, with NCRCG providing insight and solutions at a macro level.

You can learn more about the work of the NCRCG here. We can help your own customers and suppliers too, so spread the word.

There's more to the Cyber Resilience Centres...

There are many additional ways to engage with your Regional CRC. If you haven't already, you can join the community, which is free of charge. This membership includes practical, government-approved guidance, as well as regular information updates to keep you informed of our other help and services on offer, including:

- **Educational Events** - CRCs run regular webinars and events on a range of topics relevant to your small business or third sector organisation.

- **Funded solutions** – CRCs offer a range of services like this one, which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.

- **Cyber Essentials Certification** - If you are planning to achieve Cyber Essentials or Cyber Essentials Plus certification, your Regional CRC can refer you to IASME who have a list of local suppliers in your region that provide this.

Find your Regional Cyber Resilience Centre here.

Get in touch with us at engagement@cyberpath.co.uk if there's anything else we can help you with.

Appendix A - Full results of the Microsoft 365 Review

Below are the full findings of the Level 1 Microsoft 365 CIS Benchmark.

CIS Microsoft 365 Foundations Benchmark - [redacted]					
Reference		**Level**	**Title**	**Finding**	**PASS /FAIL**
1 Microsoft 365 Admin Center					
1.1 Users	1.1.1	L1	Ensure Administrative accounts are separate and cloud-only	All Administrative accounts are cloud only.	PASS
	1.1.2	L1	Ensure two emergency access accounts have been defined	No Emergency Access Accounts created.	FAIL
	1.1.3	L1	Ensure that between two and four global admins are designated	1 Global Admin	FAIL
	1.1.4	L1	Ensure Guest Users are reviewed at least biweekly	Client Policy, cannot be checked.	N/A
1.2 Teams & Groups	1.2.2	L1	Ensure sign-in to shared mailboxes is blocked	Sign in to shared mailboxes is blocked.	PASS
1.3 Settings	1.3.1	L1	Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)	Never Expire	PASS
	1.3.2	L1	Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices	1 Hour	PASS
	1.3.4	L1	Ensure 'User owned apps and services' is restricted	Checked	FAIL
	1.3.5	L1	Ensure internal phishing protection for Forms is enabled	Internal Phishing Protection is checked.	PASS
2 Microsoft 365 Defender					
2.1 Email & Collaboration	2.1.2	L1	Ensure the Common Attachment Types Filter is enabled	Common Attachments filter enabled.	PASS
	2.1.3	L1	Ensure notifications for internal users sending malware is Enabled	Undelivered messages are turned off.	FAIL
	2.1.6	L1	Ensure Exchange Online Spam Policies are set to notify administrators	Outbound Messages is set to Off.	FAIL
	2.1.7	L1	Ensure that an anti-phishing policy has been created	Phishing Threshold is set to "1"	FAIL

	2.1.8	L1	Ensure that SPF records are published for all Exchange Domains	SPF Set correctly	PASS
	2.1.9	L1	Ensure that DKIM is enabled for all Exchange Online Domains	DKIM for domain is disabled.	FAIL
	2.1.10	L1	Ensure DMARC Records for all Exchange Online domains are published	DMARC is not enabled.	FAIL
	2.1.11	L1	Ensure the spoofed domains report is reviewed weekly	Client Policy, cannot be checked.	N/A
	2.1.12	L1	Ensure the 'Restricted entities' report is reviewed weekly	Client Policy, cannot be checked.	N/A
	2.1.13	L1	Ensure malware trends are reviewed at least weekly	Client Policy, cannot be checked.	N/A
2.2 Cloud Apps				No Level 1 Checks for this Section.	N/A
2.3 Audit	2.3.1	L1	Ensure the Account Provisioning Activity report is reviewed at least weekly	Client Policy, cannot be checked.	N/A
	2.3.2	L1	Ensure non-global administrator role group assignments are reviewed at least weekly	Client Policy, cannot be checked.	N/A
2.4 Settings	2.4.1	L1	Ensure Priority account protection is enabled and configured	Priority Account Protection is not enabled	FAIL
	2.4.2	L1	Ensure Priority accounts have 'Strict protection' presets applied	Strict Preset covers all users.	PASS
	2.4.4	L1	Ensure Zero-hour auto purge for Microsoft Teams is on	Teams Protection Feature Missing. Setting not available.	N/A
3 Microsoft Purview					
3.1 Audit	3.1.1	L1	Ensure Microsoft 365 audit log search is Enabled	Audit did not appear to be enabled.	FAIL
	3.1.2	L1	Ensure user role group changes are reviewed at least weekly	Audit did not appear to be enabled.	FAIL
3.2 Data Loss Protection	3.2.1	L1	Ensure DLP policies are enabled	DLP Policies are not enabled.	FAIL
	3.2.2	L1	Ensure DLP policies are enabled for Microsoft Teams	DLP Policies are not enabled.	FAIL
3.3 Information Protection	3.3.1	L1	Ensure SharePoint Online Information Protection policies are set up and used	Label Policy does not exist.	FAIL
4 Microsoft Intune Admin Center					
This section is intentional blank within the CIS benchmark and exists to ensure the structure of the benchmark is consistent.					
5 Microsoft Entra Admin Center					

5.1 Identity					
5.1.1 Overview	5.1.1.1	L1	Ensure Security Defaults is disabled on Azure Active Directory	Security Defaults is enabled	**FAIL**
5.1.2 Users	5.1.2.1	L1	Ensure 'Per-user MFA' is disabled	Per-User MFA Enforced on 15 users	**FAIL**
	5.1.2.3	L1	Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'	Restrict Non-Admin users from creating tenants is set to No	**FAIL**
	5.1.2.4	L1	Ensure 'Restrict access to the Azure AD administration portal' is set to 'Yes'	Restrict access to Microsoft Entra admin center is set to No	**FAIL**
5.1.3 Groups	5.1.3.1	L1	Ensure a dynamic group for guest users is created	Dynamic Membership rule was not created.	**FAIL**
5.1.4 Devices				No Level 1 Checks for this Section.	N/A
5.1.5 Applications	5.1.5.1	L1	Ensure the Application Usage report is reviewed at least weekly	Client Policy, cannot be checked.	N/A
	5.1.5.3	L1	Ensure the admin consent workflow is enabled	Admin Consent is set to No	**FAIL**
5.1.6 External Identities				No Level 1 Checks for this Section.	N/A
5.1.7 User Experiences				No Level 1 Checks for this Section.	N/A
5.1.8 Hybrid Management	5.1.8.1	L1	Ensure that password hash sync is enabled for hybrid deployments	Client does not use a Hybrid Environment	N/A
5.2 Protection					
5.2.1 Identity Protection					
5.2.2 Conditional Access	5.2.2.1	L1	Ensure multifactor authentication is enabled for all users in administrative roles	No conditional access policies have been created in Entra	**FAIL**
	5.2.2.2	L1	Ensure multifactor authentication is enabled for all users	No conditional access policies have been created in Entra	**FAIL**
	5.2.2.3	L1	Enable Conditional Access policies to block legacy authentication	No conditional access policies have been created in Entra	**FAIL**
	5.2.2.4	L1	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	No conditional access policies have been created in Entra	**FAIL**
	5.2.2.8	L1	Ensure admin center access is limited to administrative roles	No conditional access policies have been created in Entra	**FAIL**

5.2.3 Authentication Methods	5.2.3.1	L1	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	Microsoft Authenticator is configured correctly.	PASS
	5.2.3.2	L1	Ensure custom banned passwords lists are used	Enforce custom list is set to No	FAIL
	5.2.3.3	L1	Ensure password protection is enabled for on-prem Active Directory	Not a Hybrid deployment.	N/A
	5.2.3.4	L1	Ensure all member users are 'MFA capable'	"Youth" and "Allotment" accounts were listed as not capable.	FAIL
5.2.4 Password Reset	5.2.4.1	L1	Ensure 'Self service password reset enabled' is set to 'All'	Self Service Password Reset is not Enabled.	FAIL
	5.2.4.2	L1	Ensure the self-service password reset activity report is reviewed at least weekly	Client Policy, cannot be checked.	N/A
5.2.5 Custom Security Attributes				No Level 1 Checks for this Section.	N/A
5.2.6 Risky Activities	5.2.6.1	L1	Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly	Client Policy, cannot be checked.	N/A
5.3 Identity Governance					
	5.3.2	L1	Ensure 'Access reviews' for Guest Users are configured	No access to Access Reviews	FAIL
	5.3.3	L1	Ensure 'Access reviews' for high privileged Azure AD roles are configured	Tenant does not have a valid license	N/A
6 Exchange Admin Center					
6.1 Audit	6.1.1	L1	Ensure 'AuditDisabled' organizationally is set to 'False'	AuditDisabled is set to False.	PASS
	6.1.2	L1	Ensure mailbox auditing for E3 users is Enabled	[redacted]	FAIL
	6.1.3	L1	Ensure mailbox auditing for E5 users is Enabled	[redacted]	FAIL
	6.1.4	L1	Ensure 'AuditBypassEnabled' is not enabled on mailboxes	AuditBypassEnabled is not set on any mailbox.	PASS
6.2 Mail Flow	6.2.1	L1	Ensure all forms of mail forwarding are blocked and/or disabled	Mail Forwarding is blocked.	PASS
	6.2.2	L1	Ensure mail transport rules do not whitelist specific domains	No domains are whitelisted.	PASS
	6.2.3	L1	Ensure email from external senders is identified	Need Powershell	PASS

6.3 Roles				No Level 1 Checks for this Section.	N/A
6.4 Reports	6.4.1	L1	Ensure mail forwarding rules are reviewed at least weekly	Client Policy, cannot be checked.	N/A
6.5 Settings	6.5.1	L1	Ensure modern authentication for Exchange Online is enabled	Modern Authentication is enabled.	PASS
	6.5.2	L1	Ensure MailTips are enabled for end users	MailTipsExternalRecipientsTipsEnabled is set to False	**FAIL**
7 SharePoint Admin Center					
7.1 Sites				No Level 1 Checks for this Section.	N/A
7.2 Policies	7.2.1	L1	Ensure modern authentication for SharePoint applications is required	Legacy Authentication is still enabled.	**FAIL**
	7.2.2	L1	Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	Setting Cannot Be Assessed With GlobalReader	N/A
	7.2.3	L1	Ensure external content sharing is restricted	External Content Sharing is enabled for "Anyone"	**FAIL**
	7.2.7	L1	Ensure link sharing is restricted in SharePoint and OneDrive	Default Link is set to "Anyone with the link"	**FAIL**
	7.2.9	L1	Ensure guest access to a site or OneDrive will expire automatically	Guest access to site is not set to expire.	**FAIL**
	7.2.10	L1	Ensure reauthentication with verification code is restricted	Verification Codes are not enabled.	**FAIL**
7.3 Settings	7.3.3	L1	Ensure custom script execution is restricted on personal sites	Classic SharePoint Settings are not enabled and no active sites have custom scripts.	PASS
	7.3.4	L1	Ensure custom script execution is restricted on site collections	Setting Cannot Be Assessed With GlobalReader	N/A
8 Microsoft Teams Admin Center					
8.1 Teams	8.1.2	L1	Ensure users can't send emails to a channel email address	Users can send emails to channel address is set to "On"	**FAIL**
8.2 Users	8.2.1	L1	Ensure 'external access' is restricted in the Teams admin center	External Access from external organisations is enabled.	**FAIL**
8.3 Teams Devices				No Level 1 Checks for this Section.	N/A
8.4 Teams Apps	8.4.1	L1	Ensure app permission policies are configured	Third-Party and Custom Teams apps are allowed.	**FAIL**
8.5 Meetings	8.5.2	L1	Ensure anonymous users and dial-in callers can't start a meeting	Anonymous or Dial in users cannot start a meeting.	PASS
	8.5.3	L1	Ensure only people in my org can bypass the lobby	"People in my org and guests" can bypass the lobby.	**FAIL**

	8.5.4	L1	Ensure users dialling in can't bypass the lobby	Dialling in users are unable to bypass the lobby.	PASS
	8.5.7	L1	Ensure external participants cannot give or request control	External participants cannot give or request control.	PASS
8.6 Messaging	8.6.1	L1	Ensure users can report security concerns in Teams	Users can report security concerns in Teams.	PASS
9 Microsoft Fabric					
9.1 Tenant Settings	9.1.1	L1	Ensure guest user access is restricted	Fabric is not used on this Tenant.	N/A
	9.1.2	L1	Ensure external user invitations are restricted	Fabric is not used on this Tenant.	N/A
	9.1.3	L1	Ensure guest access to content is restricted	Fabric is not used on this Tenant.	N/A
	9.1.4	L1	Ensure 'Publish to web' is restricted	Fabric is not used on this Tenant.	N/A
	9.1.6	L1	Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'	Fabric is not used on this Tenant.	N/A
	9.1.7	L1	Ensure shareable links are restricted	Fabric is not used on this Tenant.	N/A
	9.1.8	L1	Ensure enabling of external data sharing is restricted	Fabric is not used on this Tenant.	N/A
	9.1.9	L1	Ensure 'Block ResourceKey Authentication' is 'Enabled'	Fabric is not used on this Tenant.	N/A