MICROSOFT 365
TEAMS SECURITY BASELINES (SAMPLE)

Version 1.0

May 2023

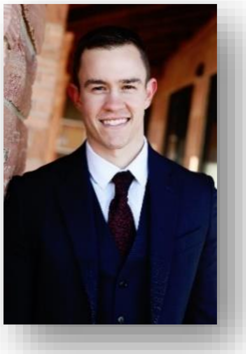
NICK ROSS

Contents

1.0 Introduction

1.1

About the Author



My name is Nick Ross and I have been publishing educational Microsoft Content for over 3 years now. I have been helping IT Admins architect Microsoft 365 solutions for 6 years and I am a Microsoft MVP. I have a YouTube channel called T-minus365 where I post new educational videos weekly, primarily for Managed Service Providers (MSPs).

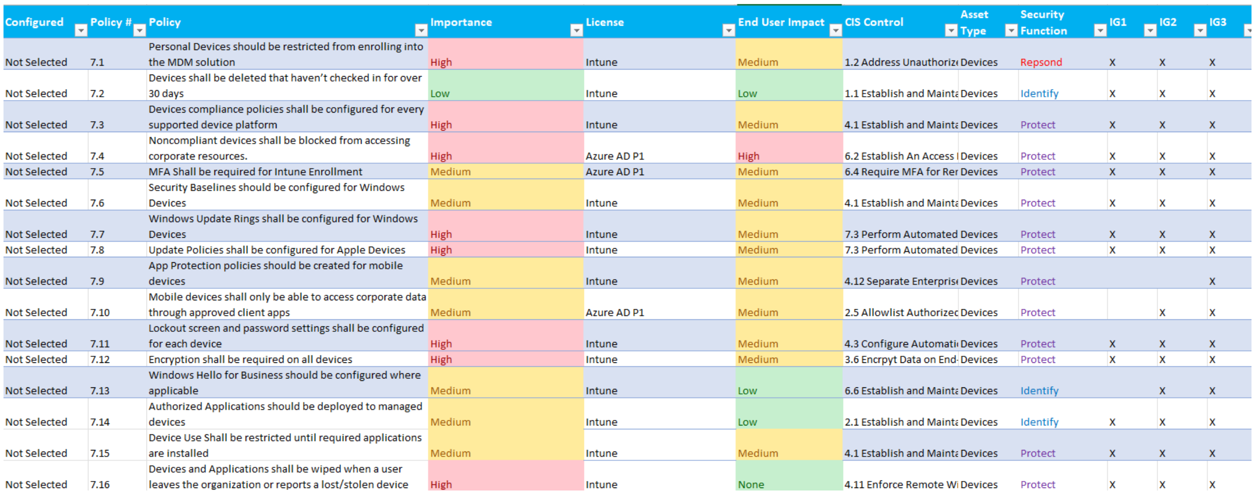
1.2

Format

The document contains sections for each of the key Microsoft 365 Product offerings. Each section contains the following format:

- Control Summary
- Policy Definition
- Licensing Considerations
- Set up instructions.
- End-User Impact/Notifications
- Tips
- PowerShell Scripts
- Video Demonstrations

Compliance Mappings can be found in the Appendix section.



Configured	Policy #	Policy	Importance	License	End User Impact	CIS Control	Asset Type	Security Function	IG1	IG2	IG3
Not Selected	7.1	Personal Devices should be restricted from enrolling into the MDM solution	High	Intune	Medium	1.2 Address Unauthoriz	Devices	Repsond	X	X	X
Not Selected	7.2	Devices shall be deleted that haven't checked in for over 30 days	Low	Intune	Low	1.1 Establish and Mainta	Devices	Identify	X	X	X
Not Selected	7.3	Devices compliance policies shall be configured for every supported device platform	High	Intune	Medium	4.1 Establish and Mainta	Devices	Protect	X	X	X
Not Selected	7.4	Noncompliant devices shall be blocked from accessing corporate resources.	High	Azure AD P1	High	6.2 Establish An Access I	Devices	Protect	X	X	X
Not Selected	7.5	MFA Shall be required for Intune Enrollment	Medium	Azure AD P1	Medium	6.4 Require MFA for Rer	Devices	Protect	X	X	X
Not Selected	7.6	Security Baselines should be configured for Windows Devices	Medium	Intune	Medium	4.1 Establish and Mainta	Devices	Protect	X	X	X
Not Selected	7.7	Windows Update Rings shall be configured for Windows Devices	High	Intune	Medium	7.3 Perform Automated	Devices	Protect	X	X	X
Not Selected	7.8	Update Policies shall be configured for Apple Devices	High	Intune	Medium	7.3 Perform Automated	Devices	Protect	X	X	X
Not Selected	7.9	App Protection policies should be created for mobile devices	Medium	Intune	Medium	4.12 Separate Enterpris	Devices	Protect			X
Not Selected	7.10	Mobile devices shall only be able to access corporate data through approved client apps	Medium	Azure AD P1	Medium	2.5 Allowlist Authorizec	Devices	Protect		X	X
Not Selected	7.11	Lockout screen and password settings shall be configured for each device	High	Intune	Medium	4.3 Configure Automati	Devices	Protect	X	X	X
Not Selected	7.12	Encryption shall be required on all devices	High	Intune	Medium	3.6 Encrpyt Data on End-	Devices	Protect	X	X	X
Not Selected	7.13	Windows Hello for Business should be configured where applicable	Medium	Intune	Low	6.6 Establish and Mainta	Devices	Identify		X	X
Not Selected	7.14	Authorized Applications should be deployed to managed devices	Medium	Intune	Low	2.1 Establish and Mainta	Devices	Identify	X	X	X
Not Selected	7.15	Device Use Shall be restricted until required applications are installed	Medium	Intune	Medium	4.1 Establish and Mainta	Devices	Protect	X	X	X
Not Selected	7.16	Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device	High	Intune	None	4.11 Enforce Remote Wi	Devices	Protect	X	X	X

If you are looking for a more detailed License Consideration breakdown, check out the free feature matrix here: Feature Matrix | M365 Maps

Updates

I will be reviewing this document on a quarterly basis for updates. Subscribe to my monthly newsletter (right hand nav) if you'd like to receive updates to the documentation.

1.3

Disclaimer

License Compliance and Copyright. This document is expanding off of the Secure Cloud Business applications (SCuBA) project from the Cybersecurity & Infrastructure Security Agency (CISA). Many of the recommendations made from that project are replicated in this document and have additions outlined in the format section (1.2). Portions of this document are adapted from documents in Microsoft 365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The recommendations and mapping of compliance controls provided in this article are for informational purposes only and should not be considered legal advice or a substitute for professional judgment.

2.0 Microsoft Teams

2.1 Private Channels shall be utilized to restrict access to sensitive information

Access controls are a fundamental part of any compliance regulation. Giving access to certain Teams channels where users are collaborating on sensitive topics or sharing critical documents should follow a model of least privilege. Microsoft Teams allows you to create private channels where users can request access to the owners and all other users are prohibited from seeing the content.

2.1.1

Policy

- When creating new Teams channels, a proper evaluation should be done to determine if a private channel should be selected.

2.1.2

Licensing Considerations

Creating Private channels does not require any premium licensing. Any base plan with Teams included will have access to create a Teams Private Channel.

2.1.3

Set-Up Instructions

Follow these steps to create a private channel in Teams

Overview of Private Channels: Private channels in Microsoft Teams - Microsoft Teams | Microsoft Learn

2.1.4

End-User Impact

Level: Medium

Content within a private channel is restricted to the owners and members of that channel. Users will not be able to share any documents part of the channel with any members of the org not part of the channel.

2.1.5

Tips

Best practices for organizing teams in Microsoft Teams: Best practices for organizing teams - Microsoft Teams | Microsoft Learn

2.1.6

PowerShell Scripts

Create Private channel in Microsoft Teams using PowerShell (morgantechspace.com)

New-TeamChannel (MicrosoftTeamsPowerShell) | Microsoft Learn

2.1.7

Videos

- Best Practices for Organizing Microsoft Teams
- How to make a Private Channel in Teams

2.2 External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings

This setting controls whether external meeting participants can request control of the shared desktop or window during the meeting. In this instance, the term “external participants” includes external users, B2B guest users, unmanaged users, and anonymous users.

While there is some inherent risk in granting an external participant control of a shared screen, legitimate use cases for this exist. Furthermore, the risk is minimal as users cannot gain control of another user's screen unless the user giving control explicitly accepts a control request. As such, while enabling external participants to request control is discouraged, it may be done, depending on organizational need.

2.2.1 Policy

External participants SHOULD NOT be enabled to request control of shared desktops or windows in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

2.2.2 Licensing Considerations

Any Teams licensing supports this configuration.

2.2.3 Set-Up Instructions

Follow these steps to configure desktop sharing settings in the Teams admin center.

To ensure external participants do not have the ability to request control of the shared desktop or window in the meeting

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings** -> **Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Content sharing** section, set **Allow an external participant** to give or request control to **Off.**
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3

2.2.4 End-User Impact

Level: Low

The number of occurrences where an external participant should need to control the screen is limited. If this is something that is required for a long-term engagement, you could set up a policy to temporarily enable it for certain users within the organization.

2.2.5

Tips

- N/A

2.2.6

PowerShell Scripts

Configure Meeting Policy Set-CsTeamsMeetingPolicy (SkypeForBusiness) | Microsoft Learn

2.2.7

Videos

Giving or Requesting Control of Screens

2.3 Anonymous Users SHALL NOT Be Enabled to Start Meetings

This setting controls which meeting participants can start a meeting. In this instance, the term “anonymous users” refers to any Teams users joining calls that are not authenticated through the company’s tenant.

2.3.1

Policy

Anonymous users SHALL NOT be enabled to start meetings in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

2.3.2

Licensing Considerations

Any Teams licensing supports this configuration.

2.3.3

Set-Up Instructions

Microsoft Resources: Control who can bypass the meeting lobby in Microsoft Teams - Microsoft Teams | Microsoft Learn

To configure settings for anonymous users:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Meetings** -> **Meeting policies.**
3. Select the **Global** (Org-wide default) policy.
4. Under the **Participants & guests** section, set **Let anonymous people start a meeting** to **Off**.
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3

2.3.4

End-User Impact

Level: Low

This is only affecting external users who enter a meeting as anonymous.

2.3.5

Tips

- N/A

2.3.6

PowerShell Scripts

- Configure Meeting Policy Set-CsTeamsMeetingPolicy (SkypeForBusiness) | Microsoft Learn