Rialtas na hÉireann
Government of Ireland

Office 365 Secure Configuration Framework

February 2023

Prepared by the Department of
the Environment, Climate and Communications
gov.ie

EKCO
Microsoft

1. Contents

Tables

Figures

2. Overview

2.1. Introduction

The National Cyber Security Centre (NCSC), in coordination with Microsoft and Ekco, have developed this Secure Configuration Framework for Office 365 a component of the Microsoft 365 services. The objective of this framework is to guide and support Irish Government departments in configuring Office 365 to ensure a high level of security and leverage the features and capabilities that are present within the service. This framework is influenced by, and aligns with, the existing best practice that is published by the NCSC and Microsoft.

This document provides Office365 specific guidance to those implementing the Cyber Security Baseline Standards. The controls & maturity levels described in this document are guidance and, as per the Public Sector Cyber Security Baseline Standards, are intended to create an acceptable security standard and form a broad framework for a set of measures which can be revised over time. The framework model follows a holistic and comprehensive approach to the issues related to Cyber Security which combines the best of various standards to address the needs of key stakeholders.

As Office 365 makes up such a significant component of many organisations' technology portfolio, it is critical that the Microsoft 365 platform is secured and managed to meet the standards set in Government's Cyber Security Baseline Standards. Those standards and other best practices, such as mentioned above, help guide an organisation to define the appropriate level of security that must be met to protect their data.

Where organisations have already invested in Microsoft 365 technologies, this guide also helps provide a roadmap to achieve a greater security posture and compliance value out of existing Microsoft licensing and features. It is recommended to continually mature your security posture to protect against evolving threats, and the levels outlined here can be used as advancements in that journey.

The Government does not endorse any commercial product or service; however, this secure configuration framework has been developed in collaboration with Microsoft and Ecko in order to ensure that organisations that are using Office 365 are doing so in a secure manner.

Important

This guidance does not provide absolute assurance of security. Rather the controls described in this document are intended to help the reader understand why the specific security controls are recommended. It also provides links to configuration guidance allowing organisations to understand how the features and capabilities in Microsoft 365 can be used to ensure that a common bar has been achieved for their Microsoft 365 tenant. In the event of a discrepancy between this guidance and the measures set out in the Cyber Security Baseline Standards, organisations should default to the measures in the CSBS.

3. Office 365 Security Principles

This security framework has been designed to support organisations and sectors to safeguard their people, data, and infrastructure when adopting Microsoft 365 services. The purpose of this document is to help government organisations use Office 365 in a secure manner aligned with the Cyber Security Baseline Standards and to help utilise the services available with their Microsoft 365 license. The following sections outline the scope and methods to enable and embed these services.

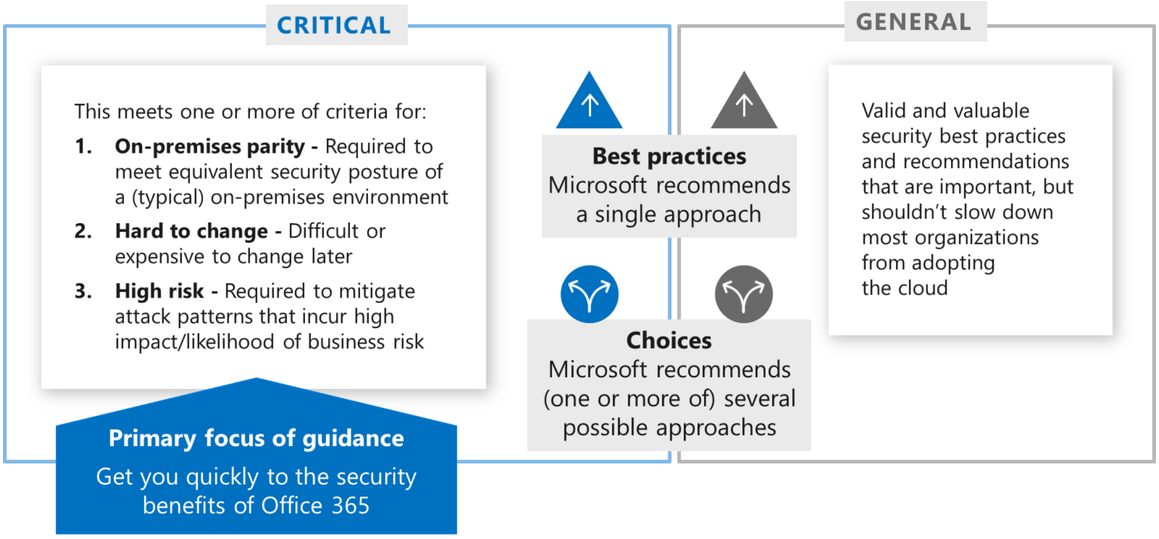
3.1. Secure Design Best Practices

This document defines a layered security model that is aligned to Microsoft and Industry best practices. The framework identifies a set of controls that organisations should consider adapting to secure their Microsoft 365 tenant, however some organisations may require deviation from the standard due to a specific use case and/or current requirements.

If there is specific guidance or controls that do not meet your estate requirements, alternative compensating or mitigating controls should be carefully considered. Such deviations may arise where single applications or services exist where the best practice controls or guidance are not technically practical or feasible to implement.

An organisational governance structure / steering board should be established for Microsoft 365 which includes business and security representatives. Their responsibilities should include reviewing and approving exemptions in line with the organisations risk appetite.

The below diagram provides some guidance around these considerations.


CRITICAL
GENERAL
Best practices
Microsoft recommends a single approach
Choices
Microsoft recommends (one or more of) several possible approaches
Primary focus of guidance
Get you quickly to the security benefits of Office 365

This meets one or more of criteria for:

1. **On-premises parity -** Required to meet equivalent security posture of a (typical) on-premises environment
2. **Hard to change -** Difficult or expensive to change later
3. **High risk -** Required to mitigate attack patterns that incur high impact/likelihood of business risk

Valid and valuable security best practices and recommendations that are important, but shouldn't slow down most organizations from adopting the cloud

Note: *These represent Microsoft's default opinion based on our experience and knowledge. Your organisation may prioritise risk and mitigations differently based on your unique business needs, business risks, or other factors.*

Figure 1 – Secure Design Considerations

3.2. Secure Administration of Cloud Services

With remote access for cloud services, and a lack of traditional physical or logical organisation perimeters to rely on, it is key to have a defined strategy for Administrator and other Privileged access. Once defined, IT and organisation management must be committed to maintaining a strict management state. Many of the foundational controls below relate to the following recommended industry best practice strategy:

1. Always separate Administrator accounts or any other privileged access roles from standard end-user accounts and end-user features, such as email.
2. Implement dedicated Privileged Access Workstations, or Jump Servers, to perform critical administrative tasks to sensitive infrastructure, databases, and systems.
3. In Hybrid environments, ensure on-premise accounts do not have Azure AD Admin privileges to reduce the impact of a successful cyber-attack.
4. Connect as many applications and services as appropriate to Azure AD. This allows for significant simplification and ability to implement M365 and Azure security controls across a large portion of your estate.

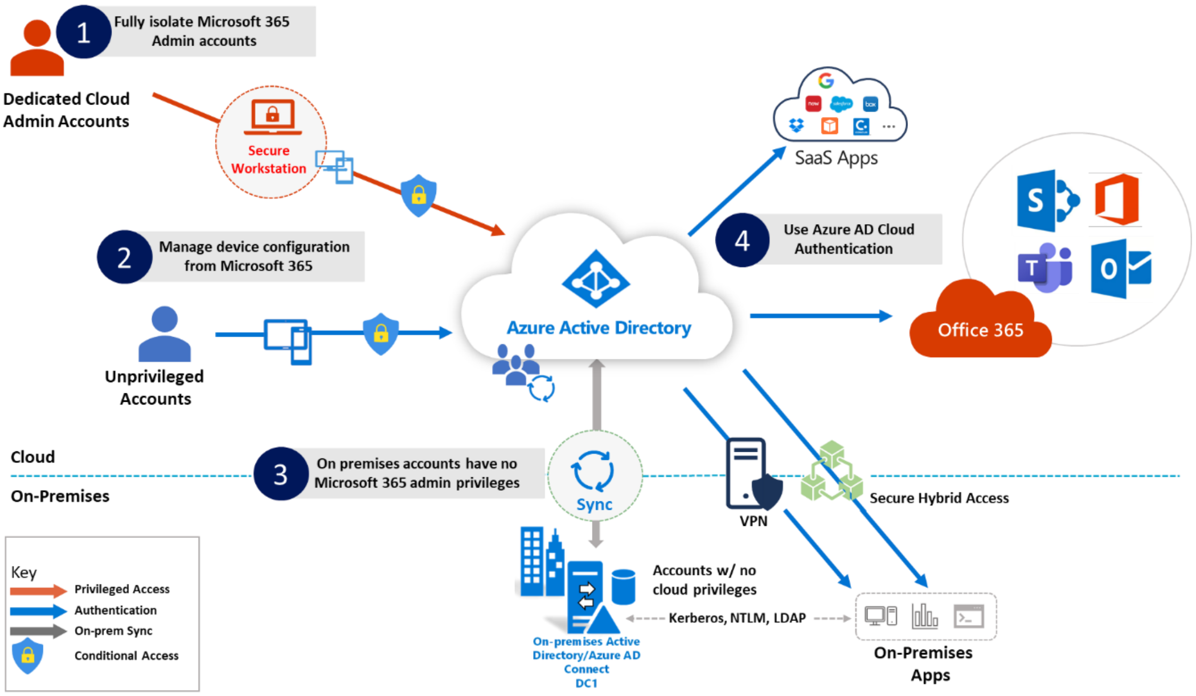

1 Fully isolate Microsoft 365 Admin accounts
Dedicated Cloud Admin Accounts
Secure Workstation
SaaS Apps
2 Manage device configuration from Microsoft 365
4 Use Azure AD Cloud Authentication
Azure Active Directory
Office 365
Unprivileged Accounts
Cloud
On-Premises
3 On premises accounts have no Microsoft 365 admin privileges
Sync
VPN
Secure Hybrid Access
Key
Privileged Access
Authentication
On-prem Sync
Conditional Access
Accounts w/ no cloud privileges
Kerberos, NTLM, LDAP
On-premises Active Directory/Azure AD Connect DC1
On-Premises Apps

Figure 2 – Secure Connectivity to the Cloud

3.3. Zero Trust

Certain Microsoft technologies may be used by an organisation to clearly tie identities to system and data access, while continuously validating key security metrics, such as user behaviour, device health and compliance, and risk.

At the core of Zero Trust for Microsoft sits Azure Active Directory Identities and Conditional Access controls. An organisation should focus on implementing these core controls in their environment with foundational governance and controls as a priority. Zero Trust principles are built upon continuously verifying access to all resources, applying the principle of least privilege, and enforcing protection controls based on the type of user/data. This allows for more tightly managed user access and protection of data, using controls such as Data Classification and Encryption.

Applying Zero Trust principles can be a challenging journey for many organisations, especially for those with a large on-premise footprint. Applying the controls within this document will support organisations transitioning to Zero Trust principles in Microsoft 365.

Microsoft's Architecture Model provides guidance to help organisations plan their Zero Trust journey. Zero Trust Model - Modern Security Architecture | Microsoft Security.

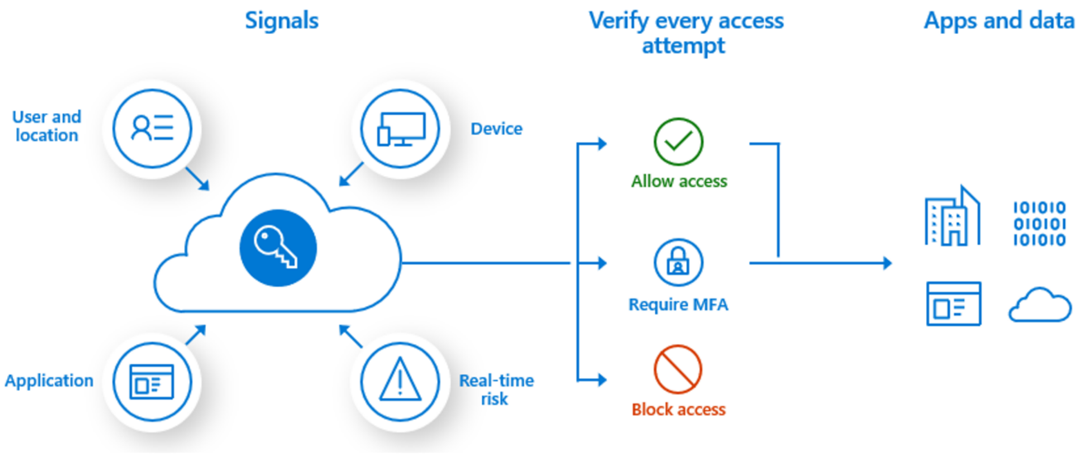


Figure 3 – Zero Trust Principles

Using the Microsoft Purview and Security features, organisations can protect the privacy of data These features include:

- Granting and restricting access to data and applications for users who meet compliance standards – i.e. meeting geographical/location conditions, meeting device standards (e.g. minimum OS versions), permitting access only to company-managed devices.
- Utilise security controls and encryption to protect data on-premise and in the cloud.

- Detect and mitigate data breaches before they cause damage using data protection controls.

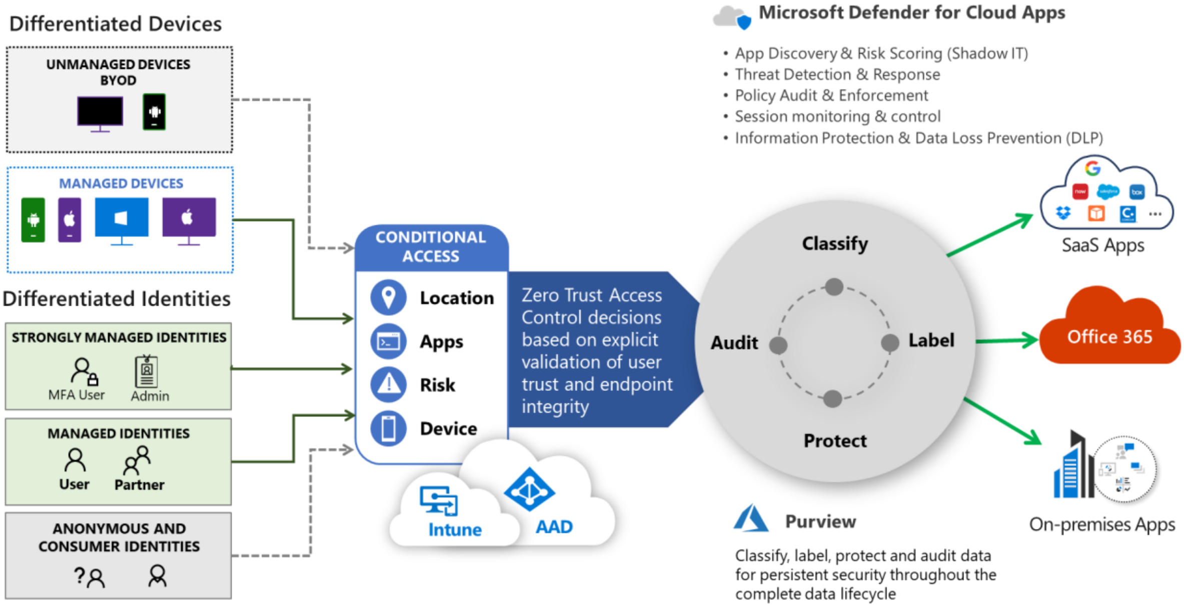

Differentiated Devices
UNMANAGED DEVICES BYOD
MANAGED DEVICES
Differentiated Identities
STRONGLY MANAGED IDENTITIES
MFA User
Admin
MANAGED IDENTITIES
User
Partner
ANONYMOUS AND CONSUMER IDENTITIES
CONDITIONAL ACCESS
Location
Apps
Risk
Device
Intune
AAD
Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Microsoft Defender for Cloud Apps
• App Discovery & Risk Scoring (Shadow IT)
• Threat Detection & Response
• Policy Audit & Enforcement
• Session monitoring & control
• Information Protection & Data Loss Prevention (DLP)
Classify
Audit
Label
Protect
Purview
Classify, label, protect and audit data for persistent security throughout the complete data lifecycle
SaaS Apps
Office 365
On-premises Apps

Figure 4 – Data Protection through conditional access and zero trust principles

4. Secure Framework

This framework has been developed to support organisations and sectors in adopting the recommended security controls when configuring and operating their Microsoft 365 tenant. It is designed as a comprehensive framework for businesses and organisations to identify, assess and address the cyber security risks they face, in line with the Microsoft services they are utilising and their risk appetite.

Organisations or sectors are encouraged to review and consider the framework as a helpful tool in managing cybersecurity risks. This framework is intended to help organisations reach an acceptable security baseline for Microsoft 365 technologies. This should be complemented by documented good-practice security operations processes and procedures to attain a broad level of cybersecurity protection,

Control Level	Guidance Criteria
Foundational Controls (Level 0)	Foundation is the minimum level of controls that all organisations should implement for their Microsoft 365 tenant.
	Foundational controls can be implemented using simple configuration tasks.
	Device Management / Hybrid Azure AD should be implemented.
	Privileged Access Accounts should use defined, separate accounts with strict controls to ensure integrity of the Microsoft 365 tenant.
	Built on Zero Trust Security principles with MFA, strong authentication, and least privilege access controls.
	Requires Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts)
	As Foundational controls are the minimum level of controls that all organisations should implement, they represent the highest level of residual risk, compared to other control levels.

Standard Controls (Level 1)	Standard control level adopts greater protective controls and introduces recommended detective controls in areas such as access management, device controls and data security controls. This should be seen as the minimum control strength for organisations using Exchange Online, SharePoint and Teams.
	Available with Microsoft 365 E3 license and Azure Active Directory (Azure AD) P1 and P2 (For Administrative Accounts).
	Can be implemented using simple configuration tasks.
	Use of Conditional Access with MFA and Restricted Session Controls in Exchange Online and SharePoint Online.
	Standard controls represent a lower residual risk than Foundational controls but retain higher residual risk than achieving either Advanced or Optimal controls levels.

Advanced Controls (Level 2)	Forms the level of configuration that organisations should aspire to. This control builds upon the earlier control levels and enhances protective, detective, and
	Available with Microsoft 365 Security and Compliance Package components or Microsoft 365 E3 with Microsoft 365 E5 Security.
	Might require more complex configuration tasks.
	Enforcement using Conditional Access to require a managed PC, Mac or mobile device to access Microsoft 365 services using the Office client applications.
	Includes security functionality to control and mitigate some data access risks from BYOD devices.
	More flexible and granular control of user policies, session controls using Microsoft Cloud App Security.
	Minimum control level for organisations allowing access to services from unmanaged devices.
	Advanced controls reduce residual risk compared to Foundational and Standard control levels, but higher than Optimised controls.
Optimised Controls (Level 3)	Forms the most complete protection available and is the lowest risk approach.
	Greatest utilisation of E5 licencing features to maximise value.
	Available with Microsoft 365 E3 with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance or Microsoft 365 E5.
	More flexible and granular control of user policies, session controls using Microsoft Cloud App Security.
	Enforcement using Conditional Access to require a managed PC, Mac or mobile device to access Office 365 services using the Office client applications. Consider when using unmanaged devices.
	Often requires more complex configuration tasks that also require integration between features.

Table 1 – Framework Criteria

Important

Irish Public Sector and Commercial organisation's ability to provide additional capabilities to their employees to facilitate remote working by allowing personal unmanaged devices (Bring Your Own Device, BYOD) to connect to Microsoft 365 services should be completed in a risk-based manner. Organisations should complete this in a way that helps them meet their obligations and leverages the features and capabilities that are present within the service.

A separate control layer has been developed which focuses on BYOD, specifically the controls that are available through Mobile Access Management (MAM) and Microsoft 365 Cloud App Security Application Session Controls.

Each of the Foundational, Standard, Advanced and Optimised sections contain guidance for the following areas:

- **Identity** – recommended controls describing how to secure the identities that are used to authenticate against Microsoft 365 services.
- **Microsoft 365 Service Configuration** – recommended controls for Microsoft 365 environment that describe specific settings to secure the service thus raising the security posture of the organisation's Microsoft 365 tenant.

This guidance applies to Microsoft 365 services unless otherwise specified. This will allow full use of all the newest features, such as Microsoft 365 Groups and Teams, as well as the controls that more directly replace on-premise services such as Exchange and SharePoint.

4.1. Control Levels

The features described in the Foundational, Standard, Advanced and Optimised control groups described in Table 2 below are designed to help organisations determine which of the controls described in this document should be used.

Foundational Controls	
Residual Risk	Highest Residual Risk
License Type	Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts)
Notes	Managed Devices Only

- Use dedicated accounts to perform Administrative Tasks
- Configure Microsoft 365 Global Administrator role members
- Use non - global admin accounts to perform M365 administrative tasks
- Configure break glass accounts in Azure AD
- Enforce MFA for all Global Admins
- Enable audit logging
- Enable mailbox auditing
- Do not use legacy authentication protocols
- Set Appropriate Default Custom Password Policies
- Disable inactive accounts
- Enable MFA Registration for All Users
- Implement Conditional Access
- Control access to managed devices

Standard Controls	
Residual Risk	Second Highest Residual Risk
License Type	Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts)
Notes	Managed Devices Only

- Enhance Conditional Access
- Use Cloud Compliance Checks
- Implement Cloud Authentication
- Enable Client Rules Forwarding Block
- Do not allow anonymous calendar sharing
- Secure external mail flow
- Secure inbound email by configuring mail flow rules (transport rules) for malicious files
- Configure anti - malware protection in your tenant
- Utilise Microsoft Teams External Access (Federation) to configure external meetings
- Invite external users to Teams using Microsoft Teams Guest Access
- Allow SharePoint users to invite and share with new and existing Guests
- Enable Microsoft 365 Cloud App Consent for Data Access
- Intune Basic Mobile Device Management Controls

<table>
<tr><th colspan="2">Advanced Controls</th></tr>
<tr><td><b>Residual Risk</b></td><td>Second Lowest Residual Risk</td></tr>
<tr><td><b>License Type</b></td><td>Microsoft 365 E3 and Azure Active Directory Premium (AAD) P1 and P2 (For Administrative Accounts) or Microsoft 365 E5 and E5 Security</td></tr>
<tr><td><b>Notes</b></td><td>Managed Devices Only / BYOD</td></tr>
<tr><td colspan="2">• Security Azure AD Identity Protection
• Monitor user accounts for suspicious activity
• Azure AD Privileged Identity Management access reviews for privileged roles
• Azure AD Entitlement Management
• Enhance External Mail Flow
• Configure Microsoft 365 Advanced Threat Protection Safe Attachments feature
• Configure Microsoft 365 Advanced Threat Protection Safe Links feature
• Microsoft Purview Information Protection Labelling / Visible marking
• Perform a simulated Attack campaign
• Advanced Intune Endpoint Reporting
• Intune Advanced MAM/MDM rules
• Advanced Privileged Access Controls
• Advanced Teams Security Configuration
• Enhanced SharePoint Controls</td></tr>
<tr><th colspan="2">Optimised Controls</th></tr>
<tr><td><b>Residual Risk</b></td><td>Lowest Residual Risk</td></tr>
<tr><td><b>License Type</b></td><td>Microsoft 365 E5, E5 Security & E5 Compliance</td></tr>
<tr><td><b>Notes</b></td><td>Managed Devices Only / BYOD</td></tr>
<tr><td colspan="2">• Enable options for Passwordless Microsoft Accounts
• Enable Customer Lockbox to control Microsoft access to organisational data
• Microsoft 365 Cloud Data Loss Prevention
• Endpoint Data Loss Prevention
• Configure Email Message Encryption
• Insider risk management
• Protect against data loss from cloud apps using Microsoft Defender for Cloud Apps
• Restrict access to content by using sensitivity labels
• Connect Microsoft 365 Defender to Azure Sentinel
• Limit BYOD data loss risks using granular context-based restrictions
• Utilise Microsoft Threat Intelligence to be aware of new threats and attacks</td></tr>
</table>

Table 2 – Framework control levels & components

Bring Your Own Device (BYOD)
• Configure Device Enrolment Restrictions • Setup BYOD Specific Conditional Access Policies • Configure App Protection Policies • Define Allowed BYOD Apps • Set Intune Compliance Policies for BYOD • Enable Microsoft Defender for Endpoint on App Protection Policies • Protect data when accessed by unmanaged workstations

Table 3 – BYOD Security Controls

5. Where to Start

Before beginning the journey of implementing this secure configuration framework, it is essential that organisations and sectors understand their current level of operational maturity & have robust processes and controls in place to support the implementation.

This section includes best practice guidelines and recommendations on implementing a governance framework that organisations should consider before embarking on the journey to improve their Microsoft 365 security configuration. It is essential to not only enable these features but operationalise and embed in line with the organisations current processes and procedures.

5.1. Scope

The framework covers privileged access and four primary configuration settings that have been identified as meeting the requirement to allow managed devices to access corporate data in Microsoft 365 services, these are:

- Office 365 Apps on managed and BYOD Android or iOS devices.
- Office 365 Web Application access on managed PC or Mac.
- Office 365 desktop client applications access on managed PC or Mac.
- Office 365 desktop client using Windows Virtual Desktop from a PC or Mac.

The following list provides a set of prerequisite requirements where this baseline standard assumes that the following are in place:

- The baseline standard assumes that the End User Devices that are used to connect to the Microsoft 365 services have been configured in accordance with the CIS Controls for mobile and PC devices.
- Secure management of applications on mobile devices accessing the estate.
- Only allow managed PC or Mac to access using web apps or desktop client applications.
- Require MFA and Compliant or Hybrid Azure AD joined devices to access Microsoft 365 services.

5.2. Implementation Planning

5.2.1. Risk Appetite

Risk appetite is the level of risk that an organisation is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of new features and the threats which change inevitably brings.

It is necessary to assess your organisation’s risk appetite in protecting its corporate assets and sensitive data. It is essential for organisations and sectors to define and agree their security and data requirements in line with legal and data protection and security regulatory requirements. Such regulatory requirements include:

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Irish Data Protection Acts 1988 - 2018
- The 2011 “ePrivacy Regulations” (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011)
- The Network and Information Security (NIS) Directive (EU) 2016/1148
- S.I. No. 360 of 2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018

Within Microsoft 365, organisations and sectors can define settings and configurations that enable them to adhere to their legal and data protection requirements.

For example, Microsoft’s standard retention periods alone may not be enough to meet an organisation’s particular compliance requirements.

5.2.2. Understand the data exchange in the organisation

Individuals, businesses, and governments face common challenges when data is accessed and shared. When data transfer is poorly organised and lacking sufficient monitoring and protection, the risk of a data breach is greatly increased. Although this area of risk is commonly known across organisations, failures to address this risk result in data breaches occurring regularly. Key considerations include:

- Understanding what data is in place across the organisation.
- Identifying organisational and regulatory requirements.
- Identifying data owners.
- Consideration of data classification & retention requirements.

Your Microsoft Office 365 applications and data can be accessed in many ways: whether you’re working in the office, at home, on the road or from your laptop, phone or tablet device. There are now many ways to access sensitive organisational data so it’s imperative to ensure the security and integrity of this data within your organisation’s Microsoft Office 365 suite.

Microsoft offers various solutions within Office 365 to share files and documents with colleagues, external contacts, and/or trusted organisations. Organisations and sectors should assess and enable data sharing in line with their risk appetite and must account for certain risks, including:

- Accidental sharing of sensitive content.
- Sharing of content with other unintended external users (external users with full control might be able to do this).

- Changes made by anonymous users, which cannot be tracked.

While these risks – and potentially others – may apply to your organisation, there are processes, configurable settings, and tools within Microsoft 365 that can help mitigate the risks.

5.2.3. *Assess your current state*

Understanding your current Microsoft 365 security posture is critical in order to identify gaps & prioritise a roadmap for security controls that will reduce your risk of cyber threats through utilising Microsoft 365 apps and security services.

5.2.4. *Decide goals and set target security objectives*

Informed with the assessment of your current security posture, organisations can build a more proactive and comprehensive action plan, including the controls listed in this framework. Build a remediation plan with a prioritised set of mitigation actions based on the security and control gap analysis. Build an ongoing security roadmap that matches your organisation's risk-tolerance level, skills, resources and budgets. This plan should include estimations of impact of remediation (determining which areas reduce the most risk) and key interdependencies. Organisations should also consider reviewing current Microsoft skills to securely manage technologies and invest in upskilling and certifications as needed.

5.2.5. *Matrix of current organisational needs and mapping to levels*

An efficient way to visualise the current state of your organisation, and to help with enhancement planning, is to develop a matrix of your current posture and desired controls. This is recommended to determine the priority of these controls for your organisation, as some will be more difficult than others to implement, depending on your specific environment.

5.2.6. *User Communications*

Implementing the controls described in this framework will change the way your users interact with Microsoft 365 services. It will be critical to liaise with key stakeholders across the organisation when planning control implementations to ensure all staff understand why controls are being implemented and what benefits they will have for both individual users & the wider organisation. Clear communication to all users of changes or impacts to their experience will enable a smoother update and reduce support requirements.

5.3. Information Governance Best Practices

5.3.1. *Change Management*

All changes to the security & operation of your Microsoft 365 tenancy should be planned, tested, and implemented in accordance with your existing Change Management process. Change Management is designed to provide a structured, repeatable, and adaptable approach to managing changes to your IT environment and following your existing processes will help ensure the controls are implemented effectively and with the minimal disruption to your organisation.

5.3.2. Solution Design

Implementing the controls detailed in this framework should be approached within your solution design processes, and all elements of the solutions design lifecycle should be considered when planning control implementations, for example:

- Analysis
- Design
- Development
- Testing
- Deployment

There is detailed guidance available from Microsoft online that can help in this process: Microsoft 365 solution and architecture centre | Microsoft Learn.

5.3.3. Operationalise and Standardise

Improving the security posture of your organisation is an ongoing process. Utilise risk management to ensure that cyber security is embedded in your continual improvement programmes. Utilising the Microsoft Secure Score application (refer to 6.3.2 - Use Secure Score) is an ideal way to track your security posture over time.

Your Microsoft Secure Score represents an overall scoring of security across five key Microsoft 365 areas: identities, data, apps, devices, and infrastructure, each with its own associated score. The higher the score, the more secure these are. It is a good check of overall system security health. Assessing each area will raise the individual and overall scores.

Planning and tuning security settings over time will ensure your environment and your staff are safer from the risk of attacks. A monthly review of logs and quarterly planning to implement improvements would represent a good operational cycle.

5.3.4. Exemption Process

Not all business applications, access, or processes will fit with all proposed controls defined in this document. As with other security technologies, your organisation should have a documented exemption process. It is recommended this follows the same process defined for the rest of the organisation. A key consideration is the exemption does not become the standard control and exemptions are limited to reduce environment risk and complexity.

Where an exemption is needed, it should be reviewed and agreed what other mitigations can be used to help meet the control intent and ensure this exemption design is limited in usage and scope. This exemption should then be reviewed and agreed with at least IT and Security teams, as well as Compliance, Legal, Privacy, or Risk teams as needed. Once approved, each exemption should be tracked in a central location.

An organisational governance structure / steering board should be established for Microsoft 365 which includes organisation and security representatives. Their responsibilities include reviewing and approving exemptions in line with the organisation's risk appetite.

It is recommended to regularly review exemptions, at least annually, as Microsoft 365 technology frequently changes and new ways of supporting business use cases emerge that may resolve the need for the exemption.

5.4. Management Consoles

Microsoft 365 tenant is a dedicated instance of the services of Microsoft 365 and your organisation's data stored within a specific default location, such as Europe or North America. This location is specified when the tenant for your organisation is created and should be agreed with your organisation to ensure geo-location of data is appropriate to your regulatory compliance needs. Each Microsoft 365 tenant is distinct, unique, and separate from all other Microsoft 365 tenants. You create a Microsoft 365 tenant when you purchase one or more products from Microsoft, such as Microsoft 365 E3 or E5, and a set of licenses for each.

Your Microsoft 365 tenant also includes an Azure Active Directory (Azure AD) tenant, which is a dedicated instance of Azure AD for user accounts, groups, and other objects. Each Azure AD tenant is distinct, unique, and separate from all other Azure AD tenants. While your organisation can have multiple Azure AD tenants that can be set up with Azure subscriptions, Microsoft 365 tenants can only use a single Azure AD tenant, the one that was created when you created the tenant.

In order to protect your Microsoft 365 environment, it is recommended to manage portals outside of Microsoft 365.

5.4.1. Azure Admin Centre

The primary usage of the Azure portal will be to manage identities, multi-factor authentication and conditional access.

Example roles for using the portal to protect M365: Global Admins, User administrators, Multi factor admins, Helpdesk administrators.

https://portal.azure.com

5.4.2. Microsoft Security

For the purpose of this baseline the security portal is where secure scores can be reviewed, however it does also cover general security administration for the entire tenant.

Example roles for using the portal to protect M365: Global Admins, security administrators, security readers.

https://security.microsoft.com

5.4.3. Microsoft Compliance

Within the Microsoft 365 baseline the compliance portal (Purview Portal) will be best used for Information protection tools. After configuration this will mostly be used by compliance or governance teams. Tools such as DLP and eDiscovery will be particularly useful in monitoring and reporting. For example, on GDPR requirements or data loss response.

https://compliance.microsoft.com/homepage

5.4.4. Microsoft Endpoint Manager

The endpoint management portal is used within this baseline for ensuing the devices used to connect to your tenant are compliant with your standards.

Example roles for using the portal to protect M365: Global Admins, Security Administrators, Helpdesk administrators.

https://endpoint.microsoft.com/

6. Foundational Controls

6.1. Overview

The Foundational Controls are the minimum required level your organisation must configure when enabling any service within Microsoft 365. These controls are defined based on industry best practices and mitigation against the most common security attack vectors and compliance risks. The following controls protect your user, data, and privileged account administration.

The license required is Microsoft 365 E3 and Azure Active Directory Premium P1 and P2. They represent the highest level of residual risk.

6.2. Controls List

Control	Implication & Risk	Reference
Use dedicated accounts to perform Administrative Tasks	Creating a separation between standard and administrative accounts will help protect the tenant from a standard user breach.	Refer to 6.3.1
Configure Microsoft 365 Global Administrator role members	Global Administrators have tenant wide near unrestricted access to O365 and Azure, therefore choosing the correct people and number of Global Administrators is essential in order to ensure continued operational access and to suitably reduce the targets of attack.	Refer to 6.3.2
Use non - global admin accounts to perform 0365 administrative tasks	Best practice is for administrative users to be granted the least amount of privileged access in order to perform their jobs/tasks.	Refer to 6.3.3
Configure break glass accounts in Azure AD	Mitigate the impact of accidental lack of administrative access by creating two or more emergency access accounts in your organisation.	Refer to 6.3.4
Enforce MFA for all Admins	Require Azure AD Multi-Factor Authentication (MFA) at sign-in for all individual users who are permanently assigned to one or more of the Azure AD administrator roles.	Refer to 6.3.5
Enable audit logging	Microsoft 365 Services are built with extensive logging capabilities to enable customers to meet their organisational requirements.	Refer to 6.3.6
Enable mailbox auditing	This is a requirement to ensure your organisation has logs and auditing for data protection and security incident response.	Refer to 6.3.7
Do not use legacy authentication protocols	In order to comply with other controls, as legacy authentication doesn't support required features such as multifactor authentication (MFA) and increases security risk.	Refer to 6.3.8

Control	Implication & Risk	Reference
Set Appropriate Default Custom Password Policies	Most organisations will have different password requirements and should modify these Azure AD settings to suit their needs to meet policies and standards.	Refer to 6.3.9
Disable Inactive Accounts	To meet the practices of least-privilege, inactive accounts that are not required anymore should be removed. Leaving accounts in place creates potential unmonitored targets.	Refer to 6.3.10
Enable MFA Registration for All Users	Azure AD recommends that you require multi-factor authentication (MFA) for all users.	Refer to 6.3.11
Implement Conditional Access	Conditional Access policies at their simplest are if-then statements. If a user wants to access a resource, then they must satisfy specific requirements.	Refer to 6.3.12
Control access to managed devices	Combining device access with other controls helps build a holistic approach to securing O365 data.	Refer to 6.3.13

Table 4 – Foundational Controls

6.3. Key Considerations

6.3.1. Use dedicated accounts to perform Administrative Tasks

Microsoft best practices recommend that organisations should configure administrative accounts as follows.

- Create dedicated, privileged*, cloud-based accounts for sensitive actions and use them only when necessary.
- Use built-in Azure Active Directory privileged roles to scope permissions.
- Be sure these accounts have their email forwarded to a working mailbox as they will be the default accounts to receive important notifications.

These accounts should not be secured with the same password as the corresponding standard user and should always use a strong second factor of authentication which is preferably always required. In addition, these accounts should be restrictive in their ability to reach outside the Microsoft cloud environment e.g., they should not be able to make changes to on-premises systems or generally access the internet.

* If you have Azure Active Directory Premium P2 (also included with Microsoft 365 E5), then assign all permissions via Azure AD Privileged Identity Management.

For more information and for general information on administration, refer to Separate accounts for admins | Microsoft Docs.

6.3.2. Configure Microsoft 365 Global Administrator role members

Each administrative account represents a potential attack surface that an attacker can target, so minimising the number of administrative accounts helps limit the overall organisational risk. Industry best practices recommends:

- Assign at least two accounts to the privileged group for business continuity.
- When two or more accounts are required, provide justification for each member, including the original two.
- Regularly review membership & justification for each group member.

For more information, refer to Minimise number of critical impact admins | Microsoft Docs.

For guidance on how to assign admin roles in Microsoft 365, refer to Assign admin roles the Microsoft 365 admin centre - Microsoft 365 admin | Microsoft Learn.

To see guidance supplied by the NCSC on this control, refer to section 2.1.1: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.3. Use non - global admin accounts to perform Microsoft 365 administrative tasks

Operating a least privilege model reduces risk by limiting access to critical systems and reducing the potential damage caused by the compromise of a user's account. If a malicious actor gains access to a standard user account with limited privileges, the impact of the attack will be confined to the minimal privileges assigned to that user. It is recommended to assign granular permissions aligned to a user's role, providing only the privileges necessary to perform required functions. In-built Microsoft 365 roles available and commonly used roles in organisations include:

- Billing admin
- Exchange admin
- Global reader
- Helpdesk admin
- SharePoint admin
- Teams admin
- User admin
- Multi-factor admin

For information on admin roles, refer to Commonly used Microsoft 365 admin centre roles | Microsoft Docs

For information regarding roles in the Azure Active Directory, refer to Roles for Microsoft 365 services in Azure Active Directory | Microsoft Docs

The NCSC have recommendations on appropriate access control, refer to section 1.8.1: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie)

6.3.4. Configure break glass accounts in Azure AD

In an emergency, business continuity and/or disaster recovery plans will likely involve regaining access without any impediments. In the event of errors causing a lockout, such as misconfiguring a conditional access rule, it is strongly recommended that these accounts are excluded from all conditional access policies.

An organisation might need to use an emergency access account in the following situations:

- The user accounts are federated, and federation is currently unavailable because of a network break or an identity-provider outage.
- The administrators are registered through Azure AD Multi-Factor Authentication, and all their individual devices are unavailable, or the service is unavailable.
- Each person with Global Administrator access has left the organisation.
- Unforeseen circumstances such as a natural disaster, during which a mobile phone or other networks might be unavailable.

When configuring these accounts, the following requirements must be met:

- The emergency access accounts should not be associated with any individual user in the organisation.
- No more than three break glass accounts should be established to limit attack surface.
- Set a very strong, complex password and, if available, utilise offline MFA such as FIDO tokens or OTP codes. This includes bypassing Conditional Access MFA policies and ensuring phone-based and Microsoft Authenticator MFA are not in use.
- The device or credential must not expire or be in scope of automated clean-up due to lack of use.
- In Azure AD Privileged Identity Management, make the Global Administrator role assignment permanent rather than eligible for your emergency access accounts.
- Exclude break-glass accounts from all Conditional Access policies.
- Store account credentials safely such as offline password vaults or splitting of password between two parties in the organisation to establish dual-control.
- Monitor sign-in and audit logs and setup high-priority alerts whenever these accounts are used.
- Validate accounts and access regularly.

For more information, refer to Emergency access accounts | Microsoft Docs.

For further information on emergency accounts and guidance in how to configure one, refer to Manage emergency access accounts in Azure AD | Microsoft Docs.

6.3.5. Enforce MFA for all Admins

When you require a second form of authentication, security is increased because this additional factor is not easy for an attacker to obtain or duplicate. This is recommended for all users and essential for admins.

It would not be recommended to use two weak factors e.g., password and SMS confirmation; despite technically being MFA this would be the least secure implementation of MFA for Admins.

To see how MFA works in Azure AD, refer to Azure AD Multi-Factor Authentication | Microsoft Docs.

For guidance on how to configure MFA for admins, refer to Conditional Access - Require MFA for administrators - Azure Active Directory - Microsoft Learn.

The NCSC has provided guidance on access control policies, refer to section 2.1.2, Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.6. Enable Audit Logging

Auditing is configured in the Microsoft Purview compliance portal. When it is turned on, user and admin activity from your organisation is recorded in the audit log and retained for 90 days, and up to one year depending on the license assigned to users. Your organisation should review your required auditing responsibilities and set this retention accordingly.

For a configuration guide on enabling audit logging, please see Turn auditing on or off | Microsoft Docs.

Consult section 2.7 in the NCSC document for information on logging/auditing, Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.7. Enable Mailbox Auditing

Mailbox auditing allows you to track actions that users take within their own and other's mailboxes. Using this feature enables the ability to search the Microsoft 365 Unified Audit logs by mailbox actions and the users that performed them. Mailbox auditing is enabled by default.

For details on enabling mailbox auditing, refer to Manage mailbox auditing - Microsoft 365 Compliance | Microsoft Docs.

6.3.8. Do not use legacy authentication

It's an industry best practice to not use legacy basic authentication mechanisms and use modern authentication instead. Incorporating modern authentication instead of basic authentication can help protect your Exchange Online instance from brute force or password spray attacks.

Disabling basic authentication in Exchange Online can be achieved by creating and assigning authentication policies to individual users. The authentication policy can be enforced at tenant level. From 2023, all new Microsoft tenants have legacy authentication disabled by default.

- Legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA, making them preferred entry points for adversaries attacking your organisation.
- More than 99 percent of password spray attacks use legacy authentication protocols.
- More than 97 percent of credential stuffing attacks use legacy authentication.

Azure AD accounts in organisations that don't use legacy authentication experience 67 percent fewer compromises than those where legacy authentication is enabled.

For guidance on how to disable legacy authentication, refer to Block legacy authentication | Microsoft Docs.

Refer to section 2.11.2 in the NCSC document for information on password policies, Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.9. Set Appropriate Default Custom Password Policies

By default, Azure AD configures the following settings for account that are either created in or hybrid accounts synchronised with from on-premise systems:

- Account lockout duration: 30
- Number of failed logon attempts allowed: 5
- Reset failed logon attempts count after: 2 minutes
- Maximum password age (lifetime): 90 days

Most organisations will have different password requirements and should modify these Azure AD settings to suit their needs to meet policies and standards set. To do this, you set a higher priority custom Azure AD password policy to apply to all user accounts. Note that these settings only apply to accounts associated within Azure AD and do not apply to on-premise accounts configured in Active Directory or accounts not synchronised through AD Connect. Where similar accounts are split between local and cloud management, it is recommended to keep password policies in parity to reduce confusion in password management for users.

It is also strongly recommended to create more strict password policies for more sensitive accounts, such as privileged accounts with Microsoft 365 administrator access. Recommended settings to modify from your baseline for these types of accounts are a lower password expiration frequency and an increased failed logon attempt reset timer to reduce the risk of guessing attacks. To accomplish this, high-priority fine-grained password policies can be assigned to AD groups associated with these accounts.

For implementation steps to configure custom Azure AD password policies, refer to Create and use password policies in Azure AD Domain Services | Microsoft Learn.

Refer to section 2.11.2 in the NCSC document for information on password policies, Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.10. Disable inactive accounts

By leaving inactive accounts enabled there is a greater risk of the account being compromised unnoticed. This will be especially true if there is no monitoring of account usage or risk being utilised. Although it is more likely to be an inactive user account that is targeted, inactive service accounts are an equal risk to the environment.

For further information, refer to Remove a former employee - Overview - Microsoft 365 admin | Microsoft Learn.

6.3.11. Enable MFA Registration for all users

Enabling MFA is best practice for everyone, not just administrators. End users who have access to sensitive or confidential information can also be targeted by attackers. Intellectual Property is one of the most valuable types of information these days and is therefore a rich target worth protecting.

Phishing campaigns can be effective against users for different reasons, but users can also be spear phished (specifically targeted) which is in theory easier to fall for. Adding an MFA component to a standard user sign-in is a good way to reduce the risk of compromise even if a username and password combination are successfully obtained.

It should be noted that enablement of MFA for all accounts can have an impact on unattended or non-interactive accounts. Take steps to mitigate this through conditional access policies, however as a foundation simply allowing users to register themselves will avoid issues caused by enforcing registration for all accounts.

For information on how combined registration works for MFA and SSPR, refer to Combined registration for SSPR and Azure AD Multi-Factor Authentication - Azure Active Directory.

Consult section 2.12 for guidance from the NCSC on Multi-Factor Authentication: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

6.3.12. Implement Conditional Access

Conditional Access policies allow you to build conditions that manage security controls that can block access, require multifactor authentication, or restrict the user's session when needed and stay out of the user's way when not. Microsoft best practices are as follows:

- Ensure that every app has at least one Conditional Access policy applied.
- Implement an Admin-specific policy to restrict Azure Management access to only defined Privileged Accounts.
- Block countries from which you never expect a sign-in.
- Require Multifactor Authentication and/or connection from designated work network.
- Test your policy.
- Monitor your policy.

Attackers compromising Azure Admin accounts can cause significant harm. Conditional Access can significantly reduce that risk by enforcing security hygiene before allowing access to Azure management. Ensuring that only defined privileged accounts can access management portals will also enforce separate account hygiene. Configure Conditional Access policy for Azure management that meets your organisation’s risk appetite and operational needs.

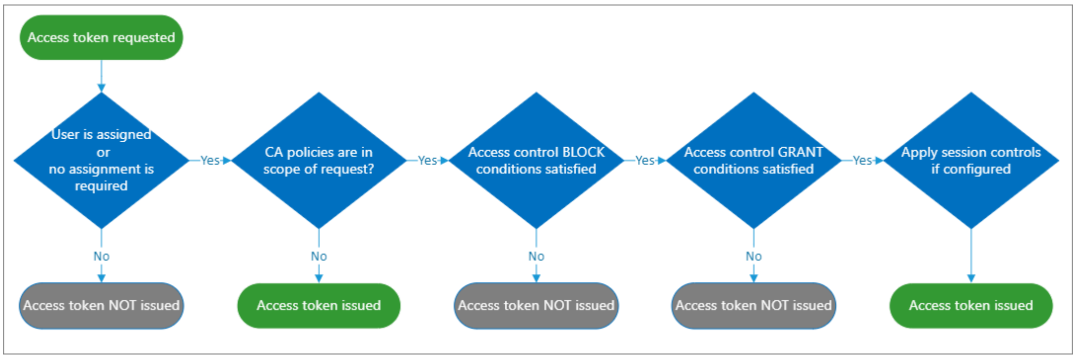

Access token requested
User is assigned or no assignment is required
Yes
CA policies are in scope of request?
Yes
Access control BLOCK conditions satisfied
Yes
Access control GRANT conditions satisfied
Yes
Apply session controls if configured
No
No
No
No
Access token NOT issued
Access token issued
Access token NOT issued
Access token NOT issued
Access token issued

Figure 5 – Conditional Access Policy Evaluation Process

For information on planning a conditional access deployment, refer to Plan an Azure Active Directory Conditional Access deployment - Microsoft Learn.

Refer to Conditional Access - Require MFA for administrators | Microsoft Learn and Enforce conditional access for admins - Zero Trust| Microsoft Docs for information on conditional access for amins.

6.3.13. Control access to managed devices

Within a Conditional Access policy, an administrator can use access controls to grant or block access to resources. Mobile Device Management (MDM) allows organisations to control, secure and enforce policies on smartphones, tablets, and other endpoints. MDM provides organisations assurances that their devices meet the security requirements for their organisation in line with their risk appetite. In line with the NCSC security baseline for endpoint devices, it is recommended to assess the compliance state of devices before granting them access to resources.

Microsoft Intune can add compliance state data to Azure Active Directory (Azure AD) for the devices you manage with one or more third-party device compliance partners.

For additional information, refer to Grant controls in Conditional Access policy | Microsoft Docs.

Refer to Device compliance partners in Microsoft Intune | Microsoft Docs for information on third-party device compliance partners in Intune.

Refer to section 2.8 in the NCSC document for guidance on End Point Devices, Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

7. Standard Controls

7.1. Overview

The Standard Controls offer more protection in access management, device controls and data security controls. It should be the minimum control level for organisations using Exchange Online, SharePoint and Teams. Organisations should adopt as many of these controls as possible unless the resulting residual risk is organisationally acceptable, and your organisation will still meet compliance obligations. The license required is Microsoft 365 E3 and Azure AD P1 and P2.

7.2. Controls List

Control	Implication & Risk	Reference
Enhance Conditional Access	Enhance conditional access by adding multiple policies. All policies must be satisfied in order to access the particular service.	Refer to 7.3.1
Use Cloud Compliance Checks	Implement Secure Score to reveal a list of security recommendations for a product. It is a useful tool to understand your organisation's best practices.	Refer to 7.3.2
Implement Cloud Authentication	Use Cloud Authentication to allow Azure AD to handle users sign-in process. It enables users to access cloud apps without having to re-enter their credentials as it incorporates single sign-on (SSO).	Refer to 7.3.3
Enable Client Rules Forwarding Block	Configure policies to block automatic external email forwarding in Exchange Online Protection at a user mailbox level.	Refer to 7.3.4
Do not allow anonymous calendar sharing	Anonymous calendar sharing allows employee calendars to be shared publicly, which could have the unintended consequence of providing information that could be used by cyber attackers. Disable the option to "Allow anyone to access calendars with an email invitation" in the Microsoft 365 admin centre.	Refer to 7.3.5
Secure external mail flow	Configure Exchange Online to use SPF, DKIM and DMARC will help to reduce spoofing of emails.	Refer to 7.3.6
Secure Inbound Email	To protect against malicious files, which can cause ransomware, create one or more mail flow rules to block file extensions that are commonly used for ransomware. Configure policies to warn users who receive these attachments in email.	Refer to 7.3.7
Configure anti - malware protection in your tenant	Define a default anti-malware policy to protect your organisation against viruses, spyware, and ransomware.	Refer to 7.3.8
Utilise Microsoft Teams External Access (Federation)	Review this control to change policies in which your organisation's users can find, chat, or set up meetings with external Teams users.	Refer to 7.3.9

Control	Implication & Risk	Reference
Invite external users to Teams using Microsoft Teams Guest Access	As an alternative to Microsoft Teams External Access, use Guest Access to provide access to external users while maintaining control over your organisation's data.	Refer to 7.3.10
Allow SharePoint users to invite and share with new and Existing Guests	Change the settings for Microsoft SharePoint to allow external sharing, and then restrict external sharing for other sites.	Refer to 7.3.11
Enable Microsoft 365 Cloud App Consent for Data Access	Configure rules to allow users to only allow consent to verified applications. This prevents unwanted or unverified applications and third parties from accessing your Microsoft 365 environment.	Refer to 7.3.12
Intune Basic Mobile Device Management Controls	Manage corporate-owned mobile devices and mobile applications using Microsoft Intune Mobile Device Management. These put basic device controls into place to reduce the risk of unwanted device access while ensuring only managed devices can access your data.	Refer to 7.3.13

Table 5 – Standard Controls

7.3. Key Considerations

7.3.1. Enhance Conditional Access

Multiple Conditional Access policies may apply to an individual user at any time. In this case, all policies that apply must be satisfied. For example, if one policy requires multi-factor authentication (MFA) and another requires a compliant device, you must complete MFA, and use a compliant device in that order. All assignments are logically ANDed. If you've more than one assignment configured, all assignments must be satisfied to trigger a policy.

To learn more, refer to Plan an Azure Active Directory Conditional Access deployment | Microsoft Learn.

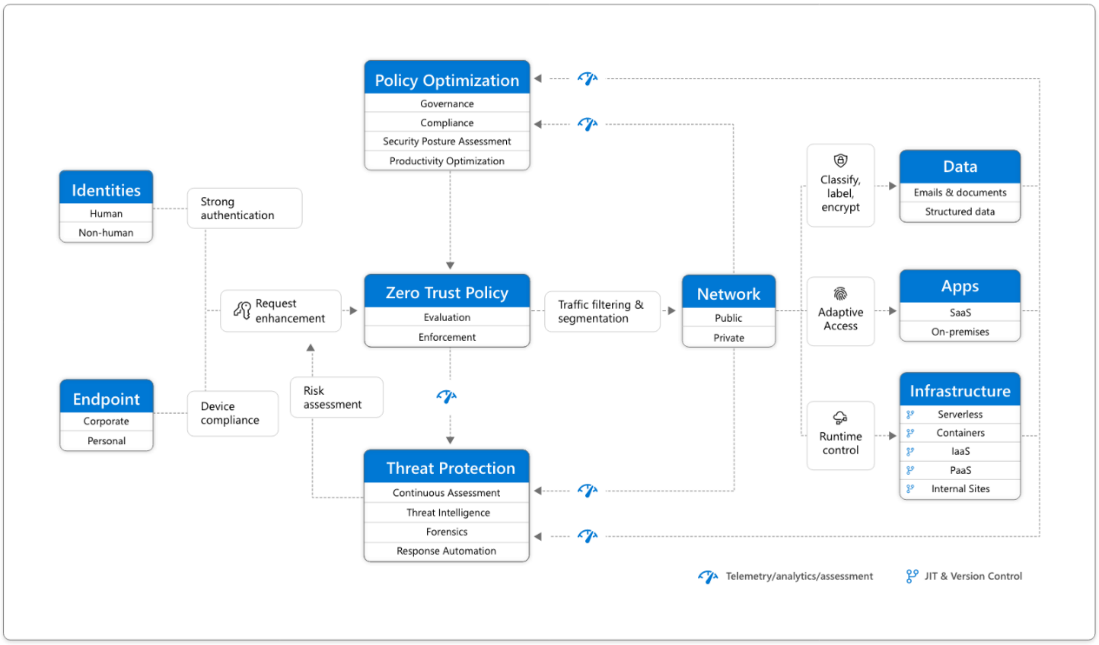


Figure 6 – Microsoft Zero Trust Structure

7.3.2. Use Cloud Compliance Checks

Microsoft 365 Secure Score is a security analytics tool that measures an organisation's security and computes a score accordingly. A higher score indicates that the organisation has implemented a number of recommended security practices, while a lower score shows that an organisation is more vulnerable to attacks. Secure Score helps organisations:

- Report on the current state of the organisation's security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

For more information, refer to What is identity secure score? Microsoft Learn.

Follow the link, Microsoft Secure Score - Microsoft 365 security, to navigate to the Microsoft Defender portal to get started with Secure Score.

7.3.3. Implement Cloud authentication

There are two methods to implement Cloud Authentication:

Azure AD password hash synchronisation. This is the simplest way to enable authentication for on-premises directory objects in Azure AD. The Active Directory domain stores passwords in the form of a hash value representation, of the actual user password. As the name suggests it implements a hash function to encrypt the passwords, which takes data of variable length and converts it to a fixed length which is encrypted using a hash key. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.

For more information and for configuration guidance, refer to Implement password hash synchronisation with Azure AD Connect sync | Microsoft Docs.

Azure AD Pass-through Authentication. Enabling this allows users to sign into both on-premises and cloud-based applications using the same password. It uses a software agent that runs on one or more on-premises servers. The servers validate the password directly with your on-premises Active Directory, ensuring password validation doesn't happen in the cloud.

For more information and configuration guidance, refer to Azure AD Connect: Pass-through Authentication | Microsoft Docs.

Refer to section 2.2 of the NCSC document for guidance on identification and authentication: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

7.3.4. Enable Client Rules Forwarding Block

Client created rules, that Auto-Forward email from user mailboxes to an external email address, are becoming an increasingly common and fruitful data exfiltration method being used by bad actors today.

There are a lot of legitimate reasons for using rules that externally Auto-Forward email, such as mergers & acquisitions etc. However, they also represent a risk that needs careful and vigilant management by the admins of your tenant to ensure they are not being misused.

Email forwarding can pose a significant security and data protection risk in the form of data exfiltration from a compromised O365 user account, as well as from staff who are knowingly or unknowingly forwarding sensitive data to external addresses. Apply strict policies for restricting email forwarding at a user mailbox level. Email forwarding should be allowed only by exception, and should be configured through Exchange Online transport rules. Run weekly reports to review user email forwarding activities. Email forwarding can be restricted and controlled through Outbound Spam policies in Exchange Online Protection (EOP).

For information on controlling automatic external email forwarding, refer to Configuring and controlling external email forwarding in Microsoft 365 - Office 365.

For information on auto forwarded messages reporting, refer to Auto forwarded messages report in the new Exchange admin centre (EAC) | Microsoft Docs.

7.3.5. Do not allow anonymous calendar sharing

Anonymous calendar sharing can be used by malicious actors during the reconnaissance phase before launching an attack. Publicly available calendars can be used to create a picture of an organisation's internal structure/relationships and provide clues to attackers when a person is more vulnerable to an attack (for ex. During business/private travelling trips) or assist in social engineering.

Ensure anonymous calendar sharing is disabled at O365 tenant level by using a sharing policy: Create a sharing policy in Exchange Online | Microsoft Learn.

7.3.6. Secure external mail flow

Microsoft 365 and Office 365 give you flexibility in determining the best arrangement for how email is delivered to your organisation's mailboxes. The path email takes from the internet to a mailbox and vice versa is called mail flow. Most organisations want Microsoft 365 to manage all their mailboxes and filtering, while some organisations need more complex mail flow setups to make sure that they comply with specific regulatory or organisational needs.

For guidance on how to configure mail flow rules, refer to Manage mail flow rules in Exchange Online | Microsoft Learn.

Configure and leverage Email Authentication protocols to protect against Spoofing / Phishing and brand reputation attacks.

- **Configure Sender Policy Framework (SPF)**

  SPF identifies which mail servers can send mail on your behalf. SPF is added as a TXT record to your domain's public DNS. Recipient mail systems refer to this SPF record to determine whether a message from your custom domain comes from an authorised messaging server.

  Refer to Set up SPF to help prevent spoofing | Microsoft Docs, for more information and for configuration.
  The NCSC provides guidance on configuring SPF in section 2.9.3:
  Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

- **Enforce TLS Inbound / Outbound for trusted 3rd parties**

  Configure TLS enforced connectors to force TLS on SMTP connections between your organisation and the trusted partner organisations.

  Exchange Online uses opportunistic TLS by default. For organisation that have compliance requirements such as medical, banking, or government organisations, configure Exchange Online to require, or force, TLS.

For more information, refer to Configure mail flow using connectors in Office 365 | Microsoft Docs.

For instructions, please see Set up connectors for secure mail flow with a partner organisation in Exchange Online | Microsoft Docs.

Refer to section 2.9.1/2.9.2 for guidance on Transport Layer Security and E-mail TLS Recommendations: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

7.3.7. Secure Inbound Email

Mail flow / transport rules are similar to the Inbox rules that are available in Outlook and Outlook on the web (formerly known as Outlook Web App). The main difference is mail flow rules act on messages while they're in transit, not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.

Hard coded Exchange Online Transport rules:

- **Anti-Phishing Policy**

  By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. In addition, organisations must set up anti-phishing polices to increase anti-spoofing and phishing protection. For example, refine the settings to better detect and prevent impersonation and spoofing attacks. Organisations should also enable unauthenticated sender indicators and first contact safety tips.

  Refer to Anti-phishing policies - Office 365 | Microsoft Learn, for more information.

- **Anti-spam Policy**

  To help reduce junk email, Exchange Online includes junk email protection that uses spam filtering technologies to identify and separate junk email from legitimate email. This spam filtering learns from known spam and phishing threats and user feedback.

  Default anti-spam protection policies for Inbound and Outbound email traffic apply at an organisational level. Custom policies for a specific domain or subset of users can be used to accommodate specific cases when the default policy is not suitable.

  Refer to Anti-Spam protection in EOP for more documentation and for configuration, consult Configure anti-spam policies in EOP.

- **Ransomware Protection**

  Block attachments that carry executable payloads. The list should be reviewed and updated on a regular basis as the threat landscape continues to develop.

  Refer to Use mail flow rules to inspect message attachments and block messages with executable attachments in EOP.

- **Block Encrypted Attachments**

  Password protected attachments should be blocked by default and allowed by exception only for messages that pass the email authentication checks.

  Refer to User mail flow rules to inspect message attachments.

- **Email setup – 3rd party Email Security Gateways + O365.**

  In cases where a 3rd party email security gateway is used in combination with O365, mail flow controls should be built into Exchange Online to allow external inbound messages only from the IP addresses of the 3rd party email security gateway.

  Refer to Mail flow rules (transport rules) in EOP to configure this control.

- **Zero-Hour Auto Purge (ZAP)**

  Enable the Zero-hour Auto Purge (ZAP) feature to retroactively remove malicious emails that have already been delivered to Exchange Online mailboxes. Refer to Zero-hour auto purge in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn.

7.3.8. Configure anti - malware protection in your M365 tenant

EOP offers multi-layered malware protection that's designed to catch all known malware in Windows, Linux, and Mac that travels into or out of your organisation.

Define a default anti-malware policy to protect your organisation against viruses, spyware, and ransomware. This must include comprehensive protection across your Microsoft 365 tenant to ensure that malware can be contained wherever it enters your organisation. This includes Teams, SharePoint Online, and OneDrive.

For more information, refer to Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams - Office 365 | Microsoft Learn.

It is optional but recommended to apply for Endpoint Attack notifications to get support from Microsoft Threat Experts. This functionality allows you to get insights from Microsoft experts to better understand complex threats and targeted attack notifications received from your Defender security tooling. They can also provide more information about the alerts, a potentially compromised device, or a threat intelligence context that you see on your portal dashboard.

To learn more, see Configure and manage Microsoft Threat Experts capabilities | Microsoft Learn.

The NCSC has published information on how to “break the chain” of ransomware: NCSC_Quick_Guide_Ransomware.

7.3.9. Utilise Microsoft Teams External Access (Federation)

Allowing federated external access to your tenancy allows users to find, call, and chat with people in other organisations. These people cannot be added to a team unless they are invited as guests. By default, external access is enabled for all domains. Restrict external access by:

- **Allowing all external domains:** This is the default settings, it allows members of your organisation find, call, chat, and set up meetings with external users.
- **Allow only specific external domains:** Add domains to the “Allow” list, all other domains will be blocked.
- **Block specific domains:** Add domains to the “Block” list, all other domains will be allowed.
- **Block all external domains:** Prevents people in your organisation from having any connection with external users.

For information on configuration, refer to Manage external meetings and chat - Microsoft Teams | Microsoft Docs.

7.3.10. Invite external users to Teams using Microsoft Teams Guest Access

As opposed to Federated External Access described above, Guest Access allows you to invite people from outside your organisation to join a team. Invited people get a guest account in Azure Active Directory. Use guest access to add a person from outside your organisation to a team, where they can chat, call, meet, and collaborate on files. A guest can be given nearly all the same Teams capabilities as a native team member.

Guests are added to your organisation's Azure Active Directory as B2B collaboration users and must sign into Teams using their guest account. This means that they may have to sign out of their own organisation to sign into your organisation.

For more information, refer to Collaborate with guests in a team | Microsoft Docs and Guest access in Microsoft Teams | Microsoft Docs.

7.3.11. Allow SharePoint users to invite and share with new and existing Guests

SharePoint has external sharing settings at both the organisation level and the site level (previously called the "site collection" level). To allow external sharing on any site, you must allow it at the organisation level, then restrict external sharing for all other sites. If a site's external sharing option and the organisation-level sharing option don't match, the most restrictive value will always be applied.

Even if your organisation-level setting allows external sharing, not all new sites allow it by default. The default sharing setting for Microsoft 365 group-connected team sites is "New and existing guests." The default for communication sites and classic sites is "Only people in your organisation."

To learn more, refer to Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Docs.

7.3.12. Enable Microsoft 365 Cloud App Consent for Data Access

Before an application can access your organisation's data, a user must grant the application permissions to do so. Different permissions allow different levels of access. By default, all users are allowed to consent to applications for permissions that don't require administrator consent. For example, by default, a user can consent to allow an app to access their mailbox but can't consent to allow an app unfettered access to read and write to all files in your organisation.

To reduce the risk of malicious applications attempting to trick users into granting them access to your organisation's data, organisations must ensure user consent is allowed only for applications that have been published by a verified publisher.

See Manage consent to applications and evaluate consent requests | Microsoft Learn for steps to enable this setting.

7.3.13. Intune Basic Mobile Device Management Controls

Where your organisation is utilising corporate owned iOS or Android mobile devices, you must ensure that remote access to your estate is permitted for these trusted devices only, and denied for personally owned or non-organisation devices.

No matter what mobile devices you are using, ensure that the Intune Compliance Policy tenant setting is configured to mark as "Not Compliant" devices that are not assigned a device compliance policy. This ensures that un-enrolled devices are not accidently allowed.

The first control step is to create Device Configuration Management policies in Microsoft Intune to manage common security settings. This level of control is focused on securing the device itself to mitigate the physical device being lost, stolen, or misused. A policy per mobile device type you are allowing will need to be put in place with at least the following settings:

- Require authentication when accessing the device.
- Regularly lock the device when not in use.
- Encrypt the device and device cloud backups.
- Require regular device updates.

With basic device management policies in place, you will need to create a basic Compliance policy to ensure the device is meeting the controls as set in the configuration above.

For information on configuration, refer to Device compliance policies in Microsoft Intune | Microsoft Learn.

Once the policies are set, you need to configure a Conditional Access policy to allow the expected device types that meet the Compliance Policy into the Microsoft 365 tenant. This should only allow the desired Mobile device types in use by your organisation and require the device to be marked compliant per the above Compliance policy.

For configuration instructions, refer to Set up device-based Conditional Access policies with Intune | Microsoft Learn.

For instructions in how to use device compliance policies with Conditional Access, refer to Tutorial - Protect Exchange Online email on managed devices | Microsoft Learn.

8. Advanced Controls

8.1. Overview

This is the Control Level organisations should aspire to. It builds on the previous control levels by enhancing the protective, detective, and responsive controls. It is necessary for more centralised government organisations with a higher threat profile. It includes enforcing conditional access, security functionality to mitigate some BYOB risks, and provides a more flexible and granular control of polices. The license required is the Microsoft 365 Security and Compliance Package or Microsoft 365 E3 with Microsoft 365 E5 Security.

8.2. Controls List

Control	Implication & Risk	Reference
Security Azure AD Identity Protection	Implement Azure AD Identity Protection to help detect users whose accounts have been compromised. Azure AD Identity Protection provides detection, investigation and remediation capabilities.	Refer to 8.3.1
Monitor user accounts for suspicious activity	Implement Microsoft Defender for Identity to gather behavioural information from your organisation's Active Directory. It detects anomalies and suspicious activity for your SecOps or SIEM team to investigate.	Refer to 8.3.2
Azure AD Privileged Identity Management access reviews for privileged roles	Incorporate regular access reviews for privileged roles to ensure that only the right users have continued access at the right time. This helps organisations lower the risk of data leakage.	Refer to 8.3.3
Azure AD Entitlement Management	Implement Azure AD Entitlement Management to give users access to the files and resources they need while preventing them from accessing information they don't.	Refer to 8.3.4
Enhance External Mail Flow	Configure Domain Keys identified Mail (DKIM) for outbound messages to ensure incoming messages haven't been tampered with in transit. Configure Domain-Based Message Authentication, Reporting, and Conformance (DMARC) to further enhance protection against phishing/spoofing.	Refer to 8.3.5
Configure Microsoft 365 Advanced Threat Protection Safe Attachments feature	Safe Attachments is a feature in Microsoft Defender for Microsoft 365 that uses a virtual environment to check attachments in inbound email messages after they've been scanned by anti-malware protection in Exchange Online Protection (EOP), but before delivery to recipients.	Refer to 8.3.6
Configure Microsoft 365 Advanced Threat Protection Safe Links feature	The Safe Links feature allows users to click links to an URL in an email safely. It does this by running the URL through a Microsoft proxy server to validate if the link is malicious.	Refer to 8.3.7

Control	Implication & Risk	Reference
Microsoft Purview Information Protection Labelling / Visible marking	Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels. These information protection capabilities give you the tools to know your data, protect your data, and prevent data loss.	Refer to 8.3.8
Perform a simulated Attack campaign	Schedule regular Attack campaigns in the Microsoft 365 Security Centre. The results of these campaigns should be used to train your users to be more vigilant to threats they are exposed to.	Refer to 8.3.9
Advanced Intune Endpoint Reporting	Enable Device Discovery to find unmanaged devices in your estate. Use Device Inventory to assign tags to manage your organisation's devices, exclude devices that pose security risks, and utilise event flags to filter and organise specific events. Utilise Intune Reports to monitor the health and activity of all endpoints and endpoint applications in your organisation.	Refer to 8.3.10
Intune Advanced MAM/MDM rules	Mature your organisation-owned devices with more granular application and data security controls while easing device on-boarding and compliance.	Refer to 8.3.11
Advanced Privileged Access Controls	Implement further controls on Privileged Accounts to reduce risk of compromise or malicious use. These include stricter MFA and session controls, risk-based rules to enforce Zero Trust models, and Privileged Access Workstations.	Refer to 8.3.12
Advanced Teams Security Configuration	Implementing a secure configuration of Microsoft Teams policies, permissions and settings allows for a reduced risk of intrusion against teams calls and video conferencing. These include Microsoft templates for ease of configuration.	Refer to 8.3.13
Enhanced SharePoint Controls	Implementing a granular control of SharePoint permissions allows for organisations to control how users view, edit, download and update SharePoint libraries. Secure architecture of SharePoint and user roles are detailed to reduce risk of unauthorized or unintended access to organisational data.	Refer to 8.3.14

Table 6 – Advanced Controls

8.3. Key Considerations

8.3.1. Security Azure AD Identity Protection

Azure Active Directory (AD) Identity Protection helps organisations detect anomalies and automatically protect against identity compromise by taking advantage of cloud intelligence powered by advanced detections based on heuristics, User and Entity Behaviour Analytics

(UEBA), and machine learning (ML) across the Microsoft ecosystem. The process works as follows:

- Identifies suspicious sign-in and user activity
- Prevents user identities from being compromised
- Generates alerts when risk thresholds are exceeded
- Mitigates risks automatically

With heuristics and ML-based signals, Azure AD Identity Protection performs identity risk assessment every time a user signs in. If these signals—both real-time and offline— trigger your policies, then the user attempting to sign in will be blocked or asked for additional identification via multi-factor authentication (MFA).

Configuring Azure AD Identity Protection reduces the volume of risk data and alerts by configuring risk-based policies in your organisation.

Refer to Configure and enable risk policies | Microsoft Docs for more information.

Sign-in risks represents the probability that a given authentication request isn’t authorised by the identity owner. To create conditional access policies to protect against this threat, refer to Sign-in risk-based Conditional Access – Azure Active Directory | Microsoft Learn.

Microsoft works with researchers, law enforcement, and other trusted sources to find leaked and password pairs. User risk-based access uses this data. Enable this policy to block rather than reset the password: User risk-based Conditional Access – Azure Active Directory | Microsoft Learn.

Refer to Azure Active Directory Identity Protection notifications | Microsoft Learn to learn how Azure AD Identity Protection helps your organisation manage user risk and risk detections by sending two types of automated emails (Users at risk, Weekly digest).

8.3.2. Monitor user accounts for suspicious activity

Microsoft Defender for Identity monitors information generated from your organisation’s Active Directory, network activity and security events to detect suspicious behaviour. The monitored activity information enables Defender for Identity to help you determine the validity of each potential threat and correctly triage and respond.

In the case of a valid threat, or true positive, Microsoft Defender for Identity (MDI) enables you to discover the scope of the breach for each incident, investigate which entities are involved, and determine how to remediate them.

For customers with an active Microsoft 365 E5 subscription or the Threat Intelligence add-on, enable the integration between Microsoft Defender for Endpoint and Microsoft Defender for Office 365. When you turn on this feature, you'll be able to incorporate data from Microsoft Defender for Office 365 into Microsoft 365 Defender to conduct a comprehensive security investigation across Office 365 mailboxes and Windows devices.

Refer to Use Microsoft Defender for Office 365 together with Microsoft Defender for Endpoint for information on how these two services integrated can help monitor and take action if a user's device is at risk.

Refer to Microsoft Defender for Identity security alert guide | Microsoft Docs to understand how MDI alerts you of suspicious activity.

Refer to section 2.11.7 for information on logging and analysing suspicious behaviour: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

8.3.3. Azure AD Privileged Identity Management access reviews for privileged roles

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) should be used to create access reviews for privileged access to Azure resources. It should also be configured to complete recurring access reviews automatically.

Azure AD Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources. Use the Azure AD PIM to create timely access reviews for privileged roles to mitigate these risks. Regular access reviews should be created for the following roles:

- Global administrator
- Privileged role administrator
- Privileged authentication administrator
- Security administrator
- Compliance administrator
- Conditional access administrator
- Application administrator
- Cloud application administrator
- Intune administrator
- Exchange administrator
- Teams administrator
- SharePoint administrator

For a configuration guide in how to set up regular access reviews refer to Create an access review of Azure resource and Azure AD roles in PIM - Azure AD - Microsoft Docs.

8.3.4. Azure AD Entitlement Management

Azure Active Directory (Azure AD) entitlement management is an identity governance feature that enables organisations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

Employees in organisations need access to various groups, applications, and SharePoint Online sites to perform their job. Managing this access is challenging, as requirements change. New applications are added, or users need more access rights. This scenario gets more complicated when you collaborate with outside organisations. You may not know who in the other organisation needs access to your organisation's resources, and they won't know what applications, groups, or sites your organisation is using.

Azure AD Entitlement Management can help you more efficiently manage access to groups, applications, and SharePoint Online sites for internal users, and for users outside your organisation who need access to those resources.

Refer to What is entitlement management? - Microsoft Docs for more information.

For information on how to share access to collaborate with people outside your organisation, refer to Govern access for external users in Azure AD entitlement management | Microsoft Docs.

8.3.5. Enhance external mail flow

Configure Domain Keys Identified Mail (DKIM) for outbound messages

DKIM is an email authentication mechanism that guarantees the message hasn’t been tampered with in transit. DKIM keys should be configured for domains and subdomains of an organisation.

For more information, please see How to use DKIM for email in your custom domain | Microsoft Docs.

Consult section 2.9.5 of the NCSC document: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

Configure Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Build a DMARC DNS record for all your domains and subdomains. DMARC offers additional protection against spoofing and phishing emails and offers email reputation protection for your organisation. DMARC works with SPF and DKIM to authenticate senders and ensure that destination email systems trust messages sent from your domain.

For more information, please see Use DMARC to validate email | Microsoft Docs.

Consult section 2.9.5/2.9.6 of the NCSC document: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie)

Email authentication checks on SPF = Fail and DMARC = Quarantine / Reject results.

Define EOP mail flow rules to quarantine messages that fail email authentication mechanism on SPF and DMARC. This should be done carefully after evaluating the potential impact, to avoid any trusted third-parties or regular senders of email to your organisation from failing these checks.

For more information, please see, Refer to Mail flow rules (transport rules) in EOP to configure the rules for SPF and DMARC failures.

8.3.6. *Configure Microsoft 365 Advanced Threat Protection Safe Attachments feature*

Safe Attachments in Microsoft Defender for Office 365 provides an additional layer of protection for email attachments that have already been scanned by anti-malware protection in Exchange Online Protection (EOP). Specifically, Safe Attachments uses a virtual environment to check attachments in email messages before they're delivered to recipients (a process known as *detonation*).

Define a default safe attachment policy based on your organisation security policies. In global settings enable the integration of Safe Attachments feature with SharePoint, OneDrive and Microsoft Teams.

Refer to Safe Attachments in Microsoft Defender for Office 365 for an overview of this Microsoft Office 365 feature.

For guidance on how to configure this control, refer to Set up Safe Attachments policies in Microsoft Defender for Office 365 | Microsoft Learn.

8.3.7. *Configure Microsoft 365 Advanced Threat Protection Safe Links feature*

Safe Links helps prevents users from following links in email and documents that go to web sites recognised as malicious. This feature provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages and other locations. Define a default safe links policy based on your organisation security policies. Enable the integration of this feature with Teams and Office 365 Apps.

Refer to Safe Links in Microsoft Defender for Office 365 for an overview of this feature and Set up Safe Links policies in Microsoft Defender for Office 365 for information on configuration.

8.3.8. *Azure Information protection Labelling / Visible marking*

Data is an asset, which, like other important business assets, has value to an organisation requiring suitable protection. Preserving the confidentiality, integrity and availability of Information and supporting Information Assets is vital and prudent to all organisations and sectors.

Data Classification involves identifying the types of data that are being processed, stored and operated by your organisation and involves the categorisation and sensitivity of the data and the likely impact arising from compromise, loss, or misuse.

Identifying and classifying sensitive items that are under your organisations control is the first step in the Information Protection discipline. Microsoft Purview provides three ways of identifying items so that they can be classified:

- **Manually by users**

  Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organisation's data, while making sure that user productivity and their ability to collaborate isn't hindered.

- **Automated pattern recognition**

  Microsoft uses sensitive information types (SIT) which are pattern-based classifiers. They detect sensitive information like social security, credit card, or bank account numbers to identify sensitive items. See Sensitive information types of entity definitions for a complete list of all SITs.

- **Machine Learning**

  The Microsoft labelling and classification tool scans documents and/or data sources to identify sensitive data patterns. These patterns can be targeted and defined by the user or more broadly detected by the tool using an extensive library.

To learn how to configure sensitivity labels and policies refer to Create and publish sensitivity labels | Microsoft Learn.

Sensitivity labels can also be applied to Microsoft Teams, Microsoft 365 groups and SharePoint sites. To learn more about this refer to Use sensitivity labels with Microsoft Teams, Microsoft 365 Groups, and SharePoint sites | Microsoft Docs.

Refer to section 1.5.1 for NCSC guidance on data and system identification that this control can help meet: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

8.3.9. Perform a simulated Attack campaign

Use Attack simulation training in the Microsoft 365 Defender portal to run realistic attack scenarios in your organisation. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line. Target your simulations by setting custom criteria and creating tailored payloads to fit your organisation. Access numerous premade email payloads to save time and effort. Microsoft offers relevant training exercises after the campaign in the areas your users need assistance with.

To see more information and for a guideline on how to get started, refer to Get started using Attack simulation training - Office 365 | Microsoft Docs.

8.3.10. Advanced Intune Endpoint Reporting

Unknown and unmanaged devices introduce significant risk to your network, whether it's an unpatched printer, network devices with weak security configurations, or a server with no security control. Onboard, group and assign policies to newly discovered devices. For further information, refer to Device discovery overview | Microsoft Learn.

Device Inventory provides analytics on your devices where alerts have been generated in the last 30 days. After seeing the report of vulnerable devices, Microsoft Device Inventory provides means to remediate these threats:

- **Exclude Devices:** Devices that are inactive, duplicates, or out of scope should be excluded from your estate. Enable this feature to focus on finding vulnerabilities on your active devices.
- **Device Timeline Event Flags:** In the event of an investigation into a potential attack, use Event Flags to filter and organise specific events. This saves time and resources.
- **Tags:** Add tags to devices to efficiently navigate your inventory when necessary.

For more information on Device Inventory, refer to Device inventory | Microsoft Learn.

Intune Reports are a great way to analyse the health and activity of all endpoints in your organisation. Intune reports provide insight into device compliance, device health, and device trends. You also have the ability to create custom reports. There are four report types:

- **Operational:** Timely, targeted reports. These will be most useful for admins and SME's
- **Organisational:** This is a broader, more general report, such reports include device management state. Useful for managers and admins.
- **Historical:** This provides an indication of patterns or trends over a certain period of time. Managers and admins will find this report most useful.
- **Specialist:** Allows you to use raw data to create your own custom reports. Most applicable to admins.

For more information and a configuration guideline, refer to Microsoft Intune reports | Microsoft Learn.

To help ensure devices are kept up to date with the latest security patches, Update Rings provide organisations with the ability to manage their IT Assets and organise how updates are delivered within specific time scales or maintenance windows.

8.3.11. Intune Advanced MAM/MDM rules

To introduce more granular data control and mitigate against more advanced mobile device risks, organisations should implement Mobile App Management (MAM) protection policies for any iOS and Android devices. This is similar to what you would configure with BYOD but should allow all Microsoft Office mobile applications and integrate any business applications where possible.

Recommended controls are as follows, but you should consider if any of these conflict with current user actions required:

- Encrypt organisation data.
- Require biometric or other authentication regularly when accessing policy managed apps and data.
- Block printing of organisational data.
- Block backup of organisation data to backup services.
- Only allow links to open in Microsoft Edge or policy-managed browsers.
- Restrict cut, copy, paste, file transfer, and saving from managed apps to any other app.
- Block screen capture.
- Only allow trusted, specific keyboards.
- Detect iOS jail-broken devices or rooted Android devices.

In addition to App Protection, your existing Conditional Access policies should be updated to require both Compliant devices as well as App Protection-controlled applications.

For more information, refer to App protection policies overview | Microsoft Learn and for configuration guidance, please see Create and deploy app protection policies - Microsoft Intune | Microsoft Learn.

To further ensure compliance with security standards as well as ease operational burden, organisations should enable auto-enrolment of organisation managed devices. This is configured in Intune and setup as a connection between your mobile phone provider(s), device resellers, and other solutions to seamlessly assign corporate control and policies when devices are purchased. This ensures your policies are always pushed to in-scope devices and the user experience out of the box needs little to no IT involvement.

For more information, refer to Enrol iOS/iPadOS devices by using ADE - Microsoft Intune | Microsoft Learn and Setup Intune enrolment for Android Enterprise fully managed devices | Microsoft Learn.

For devices under corporate control with MDM, it is recommended to utilise Endpoint Detection and Response (EDR) through Defender for Endpoint and controlled by InTune. Organisations can also avail of InTune's Attack Surface Reduction (ASR) rules that target suspicious behaviours around Office apps and Windows that may indicate malicious activity. These provide further protection on top of standard Defender for Endpoint anti-malware functionality. See Manage attack surface reduction settings with endpoint security policies in Microsoft Intune | Microsoft Learn for configuration details.

To assist with device security, InTune Security Baselines can be referred to for pre-configured strong settings for a variety of managed devices: Learn about Windows security baselines you can deploy with Microsoft Intune | Microsoft Learn

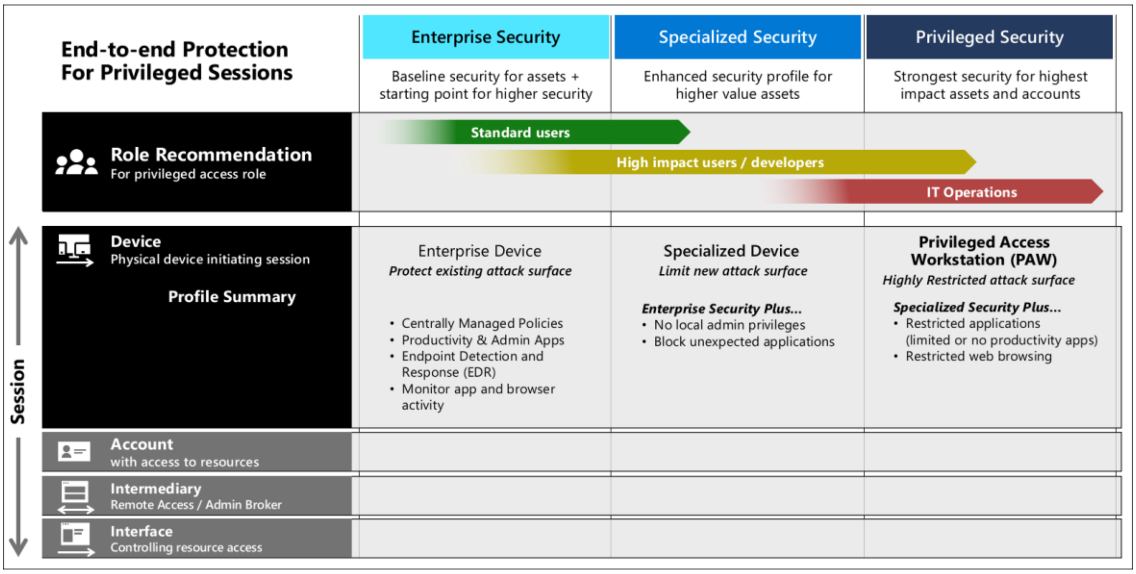
For information regarding end user devices from the NCSC consult section 2.8.7/2.8.8 of the NCSC document: Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

8.3.12. Advanced Privileged Access Controls

Administrator accounts are the most sensitive in an estate and as organisational security and Microsoft 365 usage grows, it is recommended to further secure this privileged access with the following steps:

- Enable session-restrictions in Conditional Access rules to require more frequent authentication and limit session token persistence. Specifically, this should be set to require authentication at every sign-in, require multi-factor authentication at each sign-in, and limit session persistence to no longer than twelve hours. These Conditional Access policies should be scoped using Role Inclusion to define all Directory Roles but "Guest Inviter".
- Enable risk-based Conditional Access policy rules to block Administrator access if sign-in or account risk is High. Modify existing Conditional Access Admin policy to reset Admin passwords when user risk is Medium or higher.
- Enable Number Matching MFA on Administrator accounts to ensure Microsoft Authenticator push notifications are only requested by the admin approving and not accidentally approving malicious access.
- Separate Administrator activity from standard, more vulnerable workflows by implementing Privileged Access Workstations (PAW). These should be logically separate machines from the device(s) that your Administrators use for day-to-day user tasks, such as not accessing email, communication, and document editing.

- Deployment of these PAW devices will differ by organisation based on needs, but generally they are “Jump Boxes”, or Virtual Desktop instances managed separately that Admins use their normal machine to access. Conditional Access rules then must be enabled to restrict Administration access to only these devices. Refer to Why are privileged access devices important | Microsoft Learn.



End-to-end Protection For Privileged Sessions	Enterprise Security Baseline security for assets + starting point for higher security	Specialized Security Enhanced security profile for higher value assets	Privileged Security Strongest security for highest impact assets and accounts
Role Recommendation For privileged access role	Standard users High impact users / developers	Standard users High impact users / developers	High impact users / developers IT Operations
Device Physical device initiating session Profile Summary	Enterprise Device *Protect existing attack surface* • Centrally Managed Policies • Productivity & Admin Apps • Endpoint Detection and Response (EDR) • Monitor app and browser activity	Specialized Device *Limit new attack surface* ***Enterprise Security Plus...*** • No local admin privileges • Block unexpected applications	**Privileged Access Workstation (PAW)** ***Highly Restricted attack surface*** ***Specialized Security Plus...*** • Restricted applications (limited or no productivity apps) • Restricted web browsing
Account with access to resources			
Intermediary Remote Access / Admin Broker			
Interface Controlling resource access			

Figure 7 – Privileged Access Sessions

8.3.13. Advanced Teams Security Configuration

With the communication and data handled by Microsoft Teams, it is important to configure Teams securely to meet organisational requirements and least privilege. The below recommendations highlight a few key areas to configure, along with predefined configurations that can be used to accelerate this process:

- Securing Microsoft Teams can be done by utilising the relevant Microsoft Policy Packages, These predefined packages help with the secure and speedy deployment of Teams by providing an organisation recommended settings for common industry use cases, including Public Sector.

- Protecting the data shared within Teams should also be done through the use of Teams Templates. These are predefined templates with relevant settings for teams, channels, and apps. Utilising these templates allow organisations to further restrict use of teams and implement the recommended settings for each layer and purpose of communication. Some Teams templates include but are not limited to: incident response, patient care, quality control, and safety.

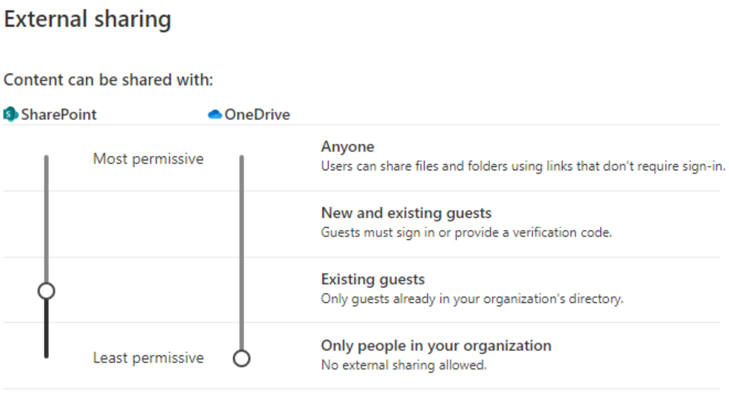
- Team Live event policies and settings should be configured through the Teams Admin centre. Configuring these ensures only permitted individuals can run live events in your organisation. Additionally, the live event settings policy allows an organisation to configure relevant third-party distribution out to social media platforms where required.

- Teams Messaging policies should be configured and tailored to allow control over message creation, deletion, and content to suit the organisation.

8.3.14. Enhanced SharePoint Controls

A key element to data security in SharePoint are permission levels and structures and how inheritance works for SharePoint sites and site collections. Utilising a methodical layer-based approach with permissions and structure allows organisations to implement a zero-trust approach in SharePoint architecture.

- SharePoint default permissions should be reviewed and configured as needed to provide a secure structure to site and data access in the platform.
- Both permission levels and SharePoint groups work together to provide an organisation with a methodical approach to permissions structure. It is recommended to account for the difference between site permissions and dependent permissions. More information can be found here to securely architect a SharePoint site.
- External sharing should be set to restrict individuals outside your organisation accessing sensitive data. The controls below can be used to limit OneDrive to internal only, and SharePoint to only deliberately invited guests. This still allows the ability to share data but in a more controllable manner. It is also strongly recommended to setup separate sites for internal-only versus externally shared data.



External sharing

Content can be shared with:

SharePoint: Existing guests

OneDrive: Only people in your organization

Most permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

Least permissive

Figure 8 – Privileged Access Sessions

- The SharePoint Admin role should be given to as few individuals as possible as the role allows the user to create sites, delete sites, configure storage limits, and manage sharing at an organisational level. It is recommended to limit this role to a few core IT Administrators. Where additional users require specific permissions, such as creating new sites, these should be given more limited custom roles.

9. Optimised Controls

9.1. Overview

The Optimised Control level provides the highest level of protection and provides the lowest residual risk approach. It entails more complex configurations but provides the greatest utilisation of the E5 package. It is available with the Microsoft 365 E3 license with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance or the Microsoft E5 license.

9.2. Controls List

Control	Implication & Risk	Reference
Enable options for Passwordless Microsoft Accounts	Allow end-users to register for and utilise passwordless authentication for their standard Microsoft accounts. This reduces the risk of account compromise from password theft while reducing log-in friction for end-users.	Refer to 9.3.1
Enable Customer Lockbox to control Microsoft access to organisational data.	Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests by Microsoft to the customer Microsoft 365 tenant, where needed for support and troubleshooting. This additional control helps organisations meet third-party compliance needs by ensuring they are in full control and have detailed tracking of when and why Microsoft accessed their data.	Refer to 9.3.2
Microsoft 365 Cloud Data Loss Prevention	Employ Microsoft Purview Data Loss Prevention (DLP) to define policies that prevent people from sharing sensitive information in a Microsoft Teams channel or chat session.	Refer to 9.3.3
Endpoint Data Loss Prevention	Use Microsoft Data Loss Prevention (DLP) to monitor the actions that are being taken on items you've determined to be sensitive and to help prevent the unintentional sharing of those items.	Refer to 9.3.4
Configure Email Message Encryption	With Office 365 Message Encryption, your organisation can send and receive encrypted email messages between people inside and outside your organisation based on Microsoft identities. This allows users to secure sensitive communications while not needing to manage other encryption technologies or document passwords.	Refer to 9.3.5
Insider risk management	Microsoft Insider Risk Management is a compliance solution that helps minimise internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organisation. Insider risk policies allow you to define the types of risks to identify and detect in your organisation, including acting on cases and escalating cases to Microsoft eDiscovery (Premium) if needed.	Refer to 9.3.6
Protect against data loss from cloud apps using	Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse	Refer to 9.3.7

Control	Implication & Risk	Reference
Microsoft Defender for Cloud Apps	proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Microsoft Defender for Cloud Apps natively integrates with leading Microsoft solutions and is designed with security professionals in mind. It provides simple deployment, centralised management, and innovative automation capabilities.	
Restrict access to content by using sensitivity labels	When you create sensitivity labels and mature your data classification programmes, it is recommended to apply encryption and protection to your most sensitive files. This mitigates data access risks if it is mistakenly sent outside your organisation or accessed maliciously.	Refer to 9.3.8
Connect Microsoft 365 Defender to Azure Sentinel	Where Security teams are utilising Sentinel, Microsoft Sentinel's Microsoft 365 Defender connector with incident integration allows you to stream all Microsoft 365 Defender incidents and alerts into Sentinel, and keeps the incidents synchronised between both portals for ease of investigation and management.	Refer to 9.3.9
Utilise Microsoft Threat Intelligence to be aware of new threats and attacks	It is important that organisations invest in proactive prevention rather than just recovery from a security breach. Advanced threats can also be difficult to detect and escape regular security detections. To assist organisations in responding and defending against these threats, Threat Intelligence and Threat Hunting tooling located in the Microsoft platforms should be built into your wider Security Operations and Risk programmes.	Refer to 9.3.10

Table 7 – Optimised Controls

9.3. Key Considerations

9.3.1. Enable option for Passwordless Microsoft Accounts

With the many threats to password-based authentication, as well as the complexity of users manging passwords, Microsoft recommends moving to other authentication methods for standard user experiences. While there are some hardware requirements, especially if you desire to use biometrics or phones, most organisation environments will support enabling this functionality. Implementing passwordless authentication provides a more secure and efficient authentication process.

For further information, refer to Plan a passwordless authentication deployment in Azure Active Directory | Microsoft Docs.

Passwordless functionality involves enabling Windows Hello and multiple authentication factors for a user's Azure Active Directory login that allows the systems to securely establish user identity without passwords. This involves two factors of something you have and something you are or know.

It is recommended to start with this enabled but not enforced for end-users while an awareness campaign is run to inform and train users. Following a period of availability, the organisation can decide if they want to enforce users to move away from passwords for standard use.

For further information, refer to Azure Active Directory passwordless sign-in | Microsoft Learn.
For information on the Microsoft Authenticator, refer to Passwordless sign-in with Microsoft Authenticator - Azure Active Directory | Microsoft Learn.

9.3.2. Enable Customer Lockbox to control Microsoft's access to organisational data.

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft.

It is recommended to enable this feature and have IT Management, Compliance, Security, or other appropriate parties be involved with reviewing the requests when needed. This include a documented process within your organisation detailing how and why requests are approved.

For more information and for a configuration guideline, refer to *Customer Lockbox requests | Microsoft Docs*.

9.3.3. Microsoft 365 Cloud Data Loss Prevention

Microsoft Cloud data loss prevention enables data loss monitoring, alerting, and preventions across the Exchange, Teams, OneDrive, SharePoint, and other Microsoft Cloud tools in your tenant.

It should be noted that while Microsoft tooling makes Data Loss Prevention easy to implement, DLP programmes can be complicated to operationalise and manage due to dealing with unstructured data and user actions. Any organisation starting on DLP implementation should prioritise their data protection on a risk-based approach, specifically targeting the most sensitive data types for policies and the strictest controls. It is also recommended that your first implementations begin where data most commonly leaves your organisation, specifically email, instant messaging, collaboration tooling, and any guest or other external-facing document shares.

When implementing, it is strongly recommended that policies be set for monitoring-only or transparent modes that do not block or alert end-users. This gives IT teams time to analyse and tune the policies to ensure false positives are minimised. Once initial tuning is done, you can use the risk-based approach to implement further controls such as user notification or, in some cases, full blocking.

The scope of areas that are possible to control with Microsoft DLP are as follows:

- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive.
- Office applications such as Word, Excel, and PowerPoint.
- Non-Microsoft cloud apps where integrations are supported and configured.
- On-premises file shares and on-premises SharePoint.

Key data loss policies to investigate configuring are as follows:

- Sending of sensitive data outside the organisation by Outlook or Teams.
- Uploading of internal-only confidential data to external SharePoint sites.
- Egress of internal-only confidential data to 3rd party websites or locations.
- Identification of non-Microsoft encrypted attachments.
- Detection of sensitive unstructured data, including:
  - Financial Identifiers
  - Credit Card Numbers
  - PII Data
  - CV Detection
  - Medical Data

For every DLP policy, you will likely have exceptions for standard or otherwise expected workflows. A defined and documented process should be put in place to review, approve, and regularly manage these, including being clear to end-users how to submit requests where any user alerting or blocking is active.

Refer to Data loss prevention in Exchange Online | Microsoft Docs for information on DLP policies in Exchange Online.

Refer to Sensitive information type entity definitions | Microsoft Docs to find a list of all SIT entity definitions with information on what a DLP policy would look like to detect each one.

With DLP, define policies that prevent users from sharing sensitive information in Teams. Refer to Data loss prevention and Microsoft Teams | Microsoft Docs.

9.3.4. Endpoint Data Loss Prevention

Microsoft Endpoint data loss prevention (Endpoint DLP) is an extension of the Microsoft 365 data loss prevention service. Microsoft Endpoint DLP allows you to monitor endpoint devices and detect when sensitive items are used and shared. To utilise Microsoft Endpoint DLP the devices must be Azure AD or Hybrid Azure AD joined.

When sensitive information is detected as being access or sent in a method against defined policy, controls are available to audit, notify, or restrict:

- Upload to cloud services, e.g., OneDrive Personal, Drobox, Google Drive, or access by unauthorised browser
- Copy to clipboard
- Copy to a network share
- Access by unallowed apps
- Copy to Bluetooth or removable storage
- Print

DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analysed for primary data matches to keywords, by the evaluation of regular expressions, by internal function validation, and by secondary data matches that are in proximity to the primary data match. Beyond that DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies.

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

For details on configuring Endpoint DLP policies, refer to Using Endpoint DLP | Microsoft Docs.

9.3.5. Configure Email Message Encryption

Email Message encryption allows users to leverage Microsoft Information Protection (MIP) to securely encrypt email messages to recipients both inside and outside your organisation. It is strongly recommended to configure this as an option and make your end-users aware, so they have the ability to secure messages where they deem necessary.

For more information, refer to Set up Microsoft Purview Message Encryption | Microsoft Learn.

Where encryption is required to meet organisational or regulatory needs, administrators can define flow rules to specify where Exchange will force encryption by default.

To learn more, please see Define mail flow rules to encrypt email messages | Microsoft Learn.

9.3.6. Insider risk management

Insider Risk Management allows an organisation to detect and respond to data risk or compliance events within the environment. These policies and protections are generally a collaboration between Compliance, HR, Legal, and Security teams to meet compliance and data handling requirements. This technology is used in conjunction with Data Classification and Data Loss Prevention but expands on those other defences by enriching policies and protections to focus on internal user behaviour and organisation data context.

Some examples of risks that can be managed are transfer of data from a secure team collaboration location to a wider SharePoint share, or an employee who will soon be exiting the organisation moving or sending data to personal storage. It is recommended to focus implementation on those use cases, as well as data that you are most concerned about as an organisation, such as HR or legal documents.

Consult Insider risk management policies | Microsoft Docs for more information on policies.

For information on configuring insider risk management, refer to Get started with insider risk management | Microsoft Docs.

9.3.7. Protect against data loss from cloud apps using Microsoft Cloud App Security

Organisations that allow guest access or want to strictly control data egress from Microsoft collaboration sites, like SharePoint, should configure Microsoft Cloud App Security download and data controls.

These should be setup to block all data download to unmanaged devices at a minimum. Further, file downloading can be blocked based on sensitivity labels or file types (such as very sensitive code) to ensure it does not leave your M365 tenant, even to managed machines.

For more information, refer to Protect with Microsoft Defender for Cloud Apps Conditional Access App Control | Microsoft Docs and Block downloads from unmanaged devices with Defender for Cloud Apps Conditional Access App Control tutorial | Microsoft Learn.

9.3.8. Restrict access to content by using sensitivity labels

When you create a sensitivity label using Microsoft Data Classification, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

- Only users within your organisation can open a confidential document or email.
- Only users in the marketing department can edit and print the promotion announcement document or email, while all other users in your organisation can only read it.

- Users can't forward an email or copy information from it that contains news about an internal reorganisation.
- The current price list that is sent to business partners can't be opened after a specified date.

When a document or email is encrypted using the native Microsoft data protection encryption, access to the content is restricted, so that it:

- Can be decrypted only by users authorised by the label's encryption settings.
- Remains encrypted no matter where it resides, inside or outside your organisation, even if the file is renamed.
- Is encrypted both at rest (for example, in a OneDrive account) and in transit (for example, email as it traverses the internet).
- Allows for a relatively transparent end-user experience and can continue to be edited by multiple users in Microsoft 365 cloud platforms.

As an admin, when you configure a sensitivity label to apply encryption, you can choose either to:

- Assign permissions to the file, so that you determine exactly which users get which permissions to content with that label. For example, a highly sensitive legal team assigned by AAD Groups.
- Let users assign permissions when they apply the label to content. This way, you can allow people in your organisation some flexibility that they might need to collaborate and get their work done.

To get started with this control, see Apply encryption using sensitivity labels | Microsoft Docs.

9.3.9. Connect Microsoft Defender for Office to Microsoft Sentinel

For those organisations who have chosen Sentinel as their Security Management tooling, Microsoft Sentinel's Microsoft 365 Defender connector allows you to stream all Microsoft 365 Defender incidents and alerts into Microsoft Sentinel, and keeps the incidents synchronised between both portals.

Microsoft 365 Defender alerts are enriched by additional alerts from component services such as Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Defender for Cloud Apps, and Microsoft Purview Data Loss Prevention (DLP).

For further information, refer to Connect Microsoft 365 Defender data to Microsoft Sentinel | Microsoft Docs.

9.3.10. Utilise Microsoft Threat Intelligence to be aware of new threats and attacks

To be proactive in defence measures and better understand complex threats to your organisation, you should utilise Microsoft Threat Intelligence and Advanced Threat Hunting.

Threat Intelligence are regular reports and dashboards from Microsoft to understand and help you respond to the following:

- Active threat actors and their campaigns
- Popular and new attack techniques
- Critical and other vulnerabilities in your estate
- Common attack surfaces
- Prevalent malware

Email notification rules should also be configured as part of this for threat insights that you deem as a priority, such as critical vulnerabilities or threat actors exploiting areas where you are vulnerable. For more information on how to access these threat dashboards and reports see Track and respond to emerging threats with Microsoft Defender for Endpoint threat analytics | Microsoft Learn.

Advanced Hunting is a technology from Microsoft that allows you to conduct advanced queries and alerting on Defender and other security information in your tenant. These can be used in a proactive manner to search for potential malicious activity as well as reactively to validate any impact from emerging threats. It is recommended that at least shared Microsoft queries be investigated to determine their applicability to your environment and how to best monitor them, such as notifications into SOC ticketing systems. Otherwise, this tooling can be incorporated into a tier 3 SOC threat-hunting programme.

For more information, consult Overview of advanced hunting in Microsoft Defender for Endpoint | Microsoft Learn

10. Bring Your Own Device (BYOD)

10.1. Overview

This portion of the framework defines the settings, controls, and considerations for organisations wishing to allow personal or other non-organisation owned and controlled user devices into their estate. This is generally referred to as Bring Your Own Device, or BYOD. Examples of devices could be personally owned Android devices, iPhones, or tablets. Alternatively, and generally in more risk-tolerant organisations, it may also include personal Windows or MacOS workstations.

It is worth noting that allowing BYOD into your estate does change and potentially increase your security risk profile. The organisation does not have technical ownership of the device and generally cannot dictate what, where, or how the device is otherwise used. Therefore, it is recommended to be thorough in planning of BYOD use-cases and ensure you are aware of the risk that accompany them. For further information on making technology decisions, refer to this guidance: Technology decisions for BYOD with EMS | Microsoft Learn and How a BYOD policy can reduce security risk in the public sector (microsoft.com).

Further, while steps have been taken below to minimise privacy impact, all deployments or interaction with BYOD devices must consider how employee privacy and rights have been suitably protected. Consult with your Data Protection Officer or similar privacy specialist to ensure all privacy requirements are met.

10.2. Controls List

Control	Implication & Risk	Reference
Configure Device Enrolment Restrictions	Without controlling enrolment, you potentially allow users or attackers to bypass Conditional Access and other controls. To prevent this, set Intune Device enrolment settings to meet your organisation's device and BYOD profile.	Refer to 10.3.1
Setup BYOD Specific Conditional Access Policies	Standard organisation Conditional Access policies should deny personal and other non-corporate managed devices. To enable BYOD access, specific policies and exceptions need to be created to allow just your intended use-cases. Failure to adequately control this access can open significant data exfiltration risks.	Refer to 10.3.2
Configure App Protection Policies	Mobile Application Management policies pushed to BYOD devices by Intune establish a secure and isolated container on unmanaged devices, allowing for the protection of company data without touching a user's personal data.	Refer to 10.3.3
Define Allowed BYOD Apps	Scope corporate BYOD controls to allow only specific company applications on BYOD devices. This should be based on the use-cases desired by the organisation, such as a requirement for only basic communication apps.	Refer to 10.3.4

Control	Implication & Risk	Reference
Set Intune Compliance Policies for BYOD	Specific Intune Compliance Policies should be setup to detect, evaluate, and mark BYOD devices compliant with organisational security controls. These compliance decisions are then used by Conditional Access and other controls to allow or deny environment and data access.	Refer to 10.3.5
Enable Microsoft Defender for Endpoint on App Protection Policies	Allow Intune to deploy Microsoft Defender functionality into the MAM App Protection containers running on BYOD devices to secure and detect threats against data running in those containers.	Refer to 10.3.6
Protect Data when accessed by unmanaged workstations	Allowing BYOD workstations access to organisational data represents a particular risk due to more limited management controls than mobile devices. If this access method is needed, some mitigations with CASB technology can be implemented to prevent removal of data from your environment from these devices.	Refer to 10.3.7

Table 8 – BYOD Controls

10.3. Key Considerations

10.3.1. Configure Device Enrolment Restrictions

By default, Microsoft Intune allows both personal and Administrator enrolment of all supported device types. This includes Windows, MacOS, as well as Android and iOS mobile devices. Enrolling a device in Intune allows for asset inventory tracking, reporting, and the ability to apply Configuration Policies.

Your enrolment restrictions should only allow the specific BYOD platforms you desire to access the estate. Due to how much control Intune enrolment gives over personal devices and the increased user actions needed to enable, it is recommended that all personal mobile device enrolment be blocked, and organisations rely solely on Mobile App Management (MAM) policies instead of device controls.

For further information, refer to Overview of enrolment restrictions | Microsoft Learn.

10.3.2. Setup BYOD Specific Conditional Access Policies

Conditional Access Policies provide some of the strongest controls available to ensure your Microsoft 365 tenant and associated data is protected from unwanted access. Therefore, it is essential to enforce a least-access strategy for BYOD prior to configuring access policies.

Policies should be setup to deny unwanted devices, with exemptions for the specific platforms you wish to allow. For these unmanaged devices you want to permit, specific Grant policies should be established with controls to validate devices are accessing resources using approved methods only, such as enforcing use of Microsoft Outlook to access corporate email, which is further secured with Intune App Protection policies.

Note: to properly evaluate and control Conditional Access, you will need Intune App Protection and/or Compliance Policies configured. Guidance for these can be found in sections below.

For information on getting started, refer to Plan an Azure Active Directory Conditional Access deployment | Microsoft Learn.

Consult Conditional Access - Require approved app or app protection policy - Azure Active Directory | Microsoft Learn for guidance on creating policies on app protection.

10.3.3. Configure App Protection Policies

Intune App Protection Policies specify protections around application and organisation data on mobile devices. While these can be used in conjunction with other controls, their primary purpose is to tightly enforce strong organisational security around data and the applications interacting with that data, while not requiring control or management of the entire device. This maintains a reasonable level of security while also protecting user privacy.

Where mobile BYOD is desired in an organisation, it is recommended to configure and apply App Protection policies for both Android and iOS devices that control the following:

- Encrypt organisational data.
- Require biometric or other authentication regularly when accessing policy managed apps and data.
- Block printing of organisational data.
- Block backup of organisational data to unmanaged backup services.
- Only allow links to open in Microsoft Edge or policy-managed browsers.
- Restrict cut, copy, paste, file transfer, and saving from managed apps to any other app.
- Block screen capture.
- Only allow trusted, specific keyboards.
- Detect iOS jail-broken devices.

For further information, refer to App protection policies overview | Microsoft Learn.

For guidance on configuration, refer to Create and deploy app protection policies | Microsoft Learn.

Refer to section 2.8.7/2.8.8 in the NCSC document for guidance on app protection policies Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

10.3.4. Define Allowed BYOD Apps

Using App Protection Policies, you will need to define the applications in the secured container. This list of applications defines the types of data and use-cases that your BYOD users will be able to interact with. It is recommended to limit this to the minimum applications needed to accomplish BYOD and remote access goals.

If an organisation only needs mobile BYOD users to have basic communication, it is recommended to only allow Microsoft Teams, Outlook, and Edge as managed applications. Where greater application access is needed, the full Microsoft Office mobile suite can be allowed, but this should be considered alongside how much file access and editing is genuinely required on a BYOD device.

Where other business applications require a mobile application and will be accessed from BYOD, such as third-party cloud storage applications, these can be included in the protection container. However, be aware there are a limited number of these application types that can be protected and it may be easier to leverage the Microsoft Edge browser to access company portals.

Refer to Create and deploy app protection policies | Microsoft Learn to learn how to create app protection policies for iOS and Android.

For further information, refer to:

- Android app protection policy settings | Microsoft Learn
- iOS/iPadOS app protection policy settings | Microsoft Learn

10.3.5. Set Intune Compliance Policies for BYOD

If your organisation has chosen to manage BYOD devices using Intune enrolment and Mobile Device Management, you will need Compliance Policies to properly evaluate Intune Conditional Access.

However, for any organisation the best practice recommendation is to configure Compliance Policies that apply to all Intune supported device platforms. This to ensure organisational security standards are still met in-case of an unexpected device platform being enrolled in Intune.

It should also be ensured that the Intune setting to mark devices not assigned a device compliance policy as “Not Compliant” is set. This ensures that un-enrolled devices are not accidently allowed.

For more information, refer to Device compliance policies in Microsoft Intune | Microsoft Learn.

10.3.6.Enable Microsoft Defender for Endpoint on App Protection Policies

To ensure data protected by App Protection Policies is secured and BYOD devices are mitigated as a malware source, it is strongly recommended to enable Microsoft Defender for Endpoint within App Protection. This functionality extends Defender protection to all managed apps and data within the MAM container while not impacting the wider device or user privacy. This is enabled in the Android and iOS App Protection policies configured above.

For further information, refer to

- Microsoft Defender for Endpoint on Android | Microsoft Learn
- Deploy Microsoft Defender for Endpoint on iOS features | Microsoft Learn

For guidance from the NCSC, refer to section 2.8.1/2.8.2:
Cyber_Security_Baseline_Standards.pdf (ncsc.gov.ie).

10.3.7. Protect Data when accessed by unmanaged workstations

In certain use cases, IT may be required to allow access to Microsoft 365 or other organisation platforms from unmanaged or BYOD workstation devices.

It should be noted that this is a high-risk requirement and, despite the controls mentioned here, should be approached with the utmost caution, and only be used where absolutely required. In secure environments where it is not possible to supply a fully managed device, it is recommended to use a Virtual Desktop platform, such as Microsoft's Azure Virtual Desktop, to allow users to interact with organisational data in a managed and secure way.

Where unmanaged device access to Microsoft 365 is required, some control can be placed over the access by using Cloud App protections. This requires the configuration of some Conditional Access and Defender policies that should be configured to do the following:

- Limit unmanaged device access to very specific applications, such as only Outlook Online, Teams, OneDrive and SharePoint Online.
- Limit unmanaged device access to specific sub-set of users, such as employees requiring temporary remote access.
- Prevent data exfiltration by blocking download, copy/paste, and printing of organisational data. This effectively restricts Microsoft 365 access to in-browser tooling only.
- Block upload of files, or where they cannot be blocked, ensure all files uploaded are scanned by Microsoft threat intelligence.
- Where your organisation has data classification configured, block access to highly sensitive files and data (Documented further in Optimised control 9.3.8)

To learn how to create policies to block downloads from unmanaged devices, refer to Block downloads from unmanaged devices with Defender for Cloud Apps Conditional Access App Control tutorial | Microsoft Learn.

11. Incident Response

This section covers steps that can be taken to prepare for a potential cyber incident as well as the immediate steps an organisation should take if they are experiencing an attack. Annex 3 of the Cyber Security Baseline Standard contains a Cyber Incident Response Checklist and should be used by Public Sector Bodies to prepare their response to cyber incidents.

11.1. Incident Response Planning

A Cyber Incident Response Plan is an organised approach to handling cybersecurity incidents. Cyber Incident response should be executed in a way that mitigates damage, reduces recovery time, and minimises costs. There are 6 phases of Incident Response, as described in table 8 below:

Phase	Description
1. Preparation	Preparing the security staff to handle potential incidents. This includes training, equipping, and practicing.
2. Identification	Detecting and deciding if an incident fulfils the conditions to be considered a security incident by the organisation, and its severity. The severity level will inform how quickly the incident needs to be handled and who it might need to be escalated to.
3. Containment	Containing the incident by isolating compromised systems to prevent future damage.
4. Eradication	Detecting the cause of the incident and eliminating the threats from affected systems.
5. Recovery	Restoring affected systems and making sure no threat remains.
6. Lessons Learned	Analysing the incident logs, updating the response plan, and completing the incident documentation.

Table 9 - Phases of Incident Response

The first step is to have an incident response plan in place that encompasses both internal and external processes for responding to cybersecurity incidents. The plan should detail how your organisation should:

- Address attacks that vary with the organisational risk and impact of the incident, which can vary from an isolated web site that is no longer available to the compromise of administrator-level credentials.
- Define the purpose of the response, such as a return to service or to handle legal or public relations aspects of the attack.
- Prioritise the work that needs to get done in terms of how many people should be working on the incident and their tasks.
- Ensure that Microsoft 365 audit logging is configured correctly, refer to Section 6.4.6 - Enable Audit Logging.

For additional detailed industry guidance, see the NIST Computer Security Incident Handling Guide:

Computer Security Incident Handling Guide (nist.gov).

11.2. Immediate Actions

Although each organisation's incident response process may be different based on organisational structure, capabilities and historical experience, consider these recommendations and best practices for responding to security incidents. During an incident, it is critical to:

Keep calm

Incidents are extremely disruptive and can become emotionally charged. Stay calm and focus on prioritising your efforts on the most impactful actions first.

Do no harm

Confirm that your response is designed and executed in a way that avoids loss of data, loss of business-critical functionality, and loss of evidence. Avoid decisions which can damage your ability to create forensic timelines, identify root cause, and learn critical lessons.

Involve your legal department

Determine whether your legal team plan to involve law enforcement in the event of any significant breach, so that you can plan your investigation and recovery procedures appropriately.

Be careful when sharing information about the incident publicly

Confirm that anything you share with your customers and the public is based on the advice of your legal department.

Align to relevant legislation

If a Cyber Security Incident is known to have led to a data breach or data loss, this must be notified to your organisation's DPO without undue delay in line with the requirement of GDPR.

Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

Breach Notification | Data Protection Commissioner

Log a security incident with Microsoft

Log a Security Incident in the Microsoft 365 Admin Portal or with your Technical Account Manager.

Report a security with the NCSC

The level of support given by NCSC will vary depending on the type and severity of the incident, the constituent and/or constituents impacted and available resources. Further information:

NCSC: Incident Reporting

Get help when needed

Tap into deep expertise and experience when investigating and responding to attacks from sophisticated attackers.

11.3. Incident Response Resources

Resource	Description
Incident Response Planning Checklist	Use this table as a checklist to prepare your Security Operations Centre (SOC) to respond to cybersecurity incidents. Incident response planning | Microsoft Learn
Incident Response with Microsoft 365 Defender	Manage incidents from Incidents & alerts > Incidents on the quick launch of the Microsoft 365 Defender portal. Incident response with Microsoft 365 Defender | Microsoft Learn
Microsoft security best practices for security operations	Security operations (SecOps) maintain and restore the security assurances of the system as live adversaries attack it. Security operations in Azure | Microsoft Learn
Microsoft Cybersecurity Reference Architectures	The Microsoft Cybersecurity Reference Architectures (MCRA) describe Microsoft's cybersecurity capabilities. Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

Table 10 - Incident Response Resources

Learn More.

National Cyber Security Centre - www.ncsc.gov.ie

Microsoft - www.microsoft.com/en-ie/security/

Ekco - www.ek.co