COMPTEC I.T | NOVEMBER 2022

Microsoft 365 Security Guide

COMPTEC I.T
Melbourne, Australia
Piraeus, Greece

https://www.comptecit.com
info@comptecit.com

Table of Contents

Introduction

The purpose

This Whitepaper aims to provide I.T professionals and the Community with Best Practices in and around Microsoft 365.

Previously known as Office 365, Microsoft 365 comes with a preset configuration which includes Security Defaults.

In this Whitepaper, we discuss advanced Security Policies and Configurations to safeguard businesses and their operations further.

Most of the topics discussed apply to organisations with Microsoft Business Premium or higher licensing.

Rebranded as Microsoft 365 on April 21, 2020, Microsoft's PaaS offering has seen a number of changes concerning security settings in its lifecycle.

The above, together with a large number of different (and at times conflicting) options offered by the platform, are known to confuse I.T professionals.

In this publication, we aim to clear things out and provide insights into using the platform; straight from the field.

Below we can see the Security Defaults Microsoft makes available to everyone to enhance security.

Security defaults -Out of the Box- *

Requiring all users to register for Azure AD Multi-Factor Authentication.

Requiring administrators to do multifactor authentication.

Requiring users to do multifactor authentication when necessary.

Blocking legacy authentication protocols.

Protecting privileged activities like access to the Azure portal.

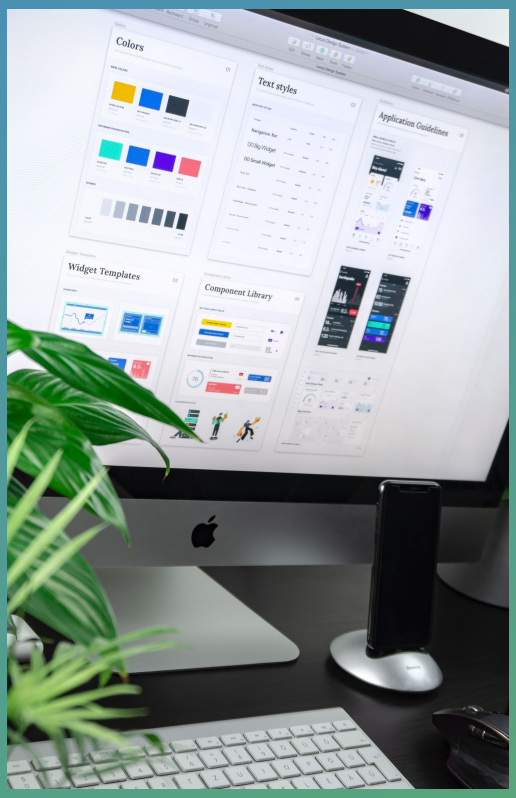
*As of October 2022 for tenants created after October 22, 2019
Source: Providing a default level of security in Azure Active Directory - Microsoft Entra | Microsoft Learn

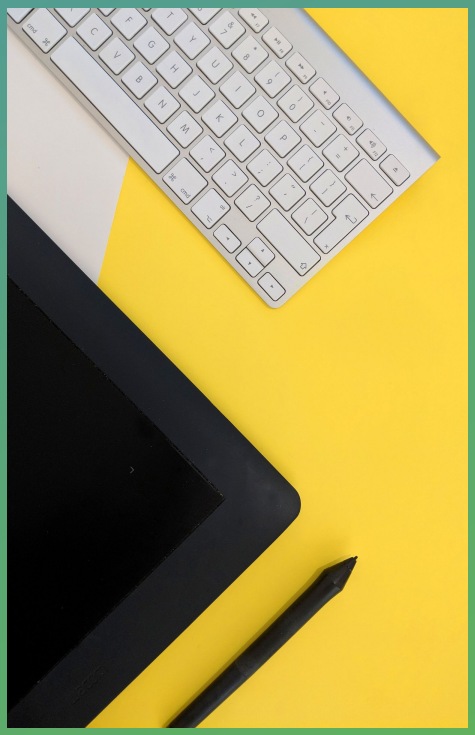
Microsoft 365 Admin portal is where we manage our users, licenses and everything else that is required for our tenant.

The portal also contains various Admin centres for different service offerings.

The highest privileged role in Microsoft 365 is the Global Admin role, equivalent to Domain/Enterprise Administrator in an on-premises Active Directory.

- The number of Global Admins must not be greater than 3 per tenant
- All Global Admins must be protected with Multi-Factor Authentication (MFA)
- Microsoft Authenticator app for Android/iOS must be used as a hardware token for MFA





Best Practices for User Passwords

Passwords should be set to Never Expire

Never Expiring passwords that are well-known to users are more difficult to get compromised

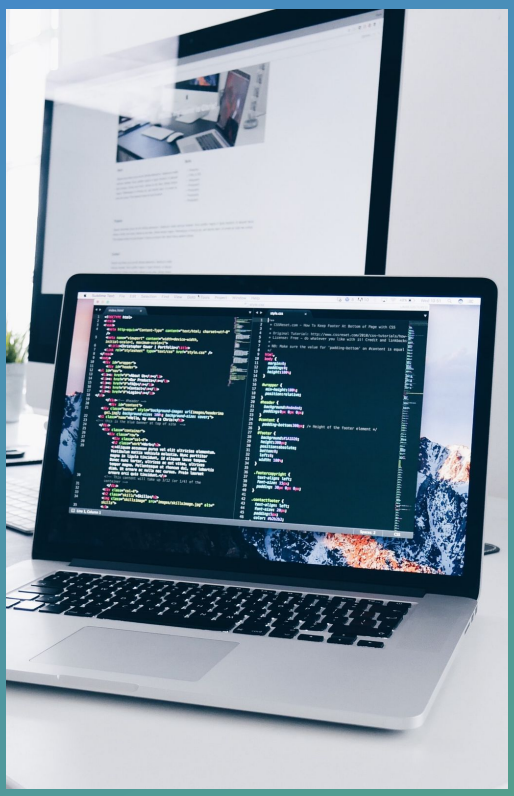
A challenging user password could contain the following:

something that the user is + something the user has + a random word separated by spaces and followed by numbers and special characters

Example: "*funny garage clock 88@!*"

Using such a combination the users won't have to write down a complex random password that most likely they won't be able to remember

Fewer password resets mean less information exposure through communication channels visible to others



Security settings in Microsoft 365 play a vital role in an organisation's digital well-being.

While countless settings are available, they must be used wisely to adapt and adjust their culture and operational requirements.

- Use Microsoft Secure Score as a representation of the organisation's security posture
- Microsoft Defender integration with Endpoint Manager must be enabled
- Email notifications for Defender & Endpoints should be enabled too
- Configure integration with a Security Information and Event Management (SIEM) solution such as Microsoft Sentinel
- The I.T department should set a routine to check on the notifications on fixed intervals

Email & collaboration Best Practices

- Review Preset security policies and pick the one you find applicable to your organisation
- Explore Configuration Analyser recommendations
- Adjust Anti-phishing and Anti-spam policies to fit your environment
- Set Anti-malware policies and enable the common attachments filter
- Create a Safe attachments policy and set a detection response
- Create a Safe links policy and enable Protection settings for apps and services
- Setup and configure Domain Keys Identified Mail (DKIM) authentication protocol
- Create and configure custom Quarantine policies

One crucial aspect of Microsoft 365 for admins is Auditing & Logging.

Microsoft 365 is a huge ecosystem, and we must find a way to track the activities happening within our tenant.

- Audit Logging on the tenant must be enabled in Microsoft Purview
- Microsoft 365 Services or Applications must be integrated with a Security Information and Event Management (SIEM) solution such as Microsoft Sentinel
- A recurring procedure for Log checking should be set to detect abnormalities
- Configure Retention policies as per your industry's requirements

Azure Active Directory (AAD) is where our Users and Groups in Microsoft 365 reside.

While parts of the configuration are available to the Free tier, too, you will want to use the AAD Premium P1 tier and onwards to get the most out of it.

- Set a routine to check on Sign-in, Audit logs and Access reviews where applied
- Consider utilising Log Analytics and Workbook
- Configure Authentication Methods to fit the requirements
- Configure Conditional Access as required

Azure Active Directory (AAD) Best Practices

- Use the Principle of Least Privilege to carry out tasks and activities
- Be mindful of Enterprise applications and App registrations
- Keep track of Delegated admin partners in your tenant
- Keep Devices up to date and maintain consistency
- Use Named Locations to contain false positives
- Configure the Company Branding option

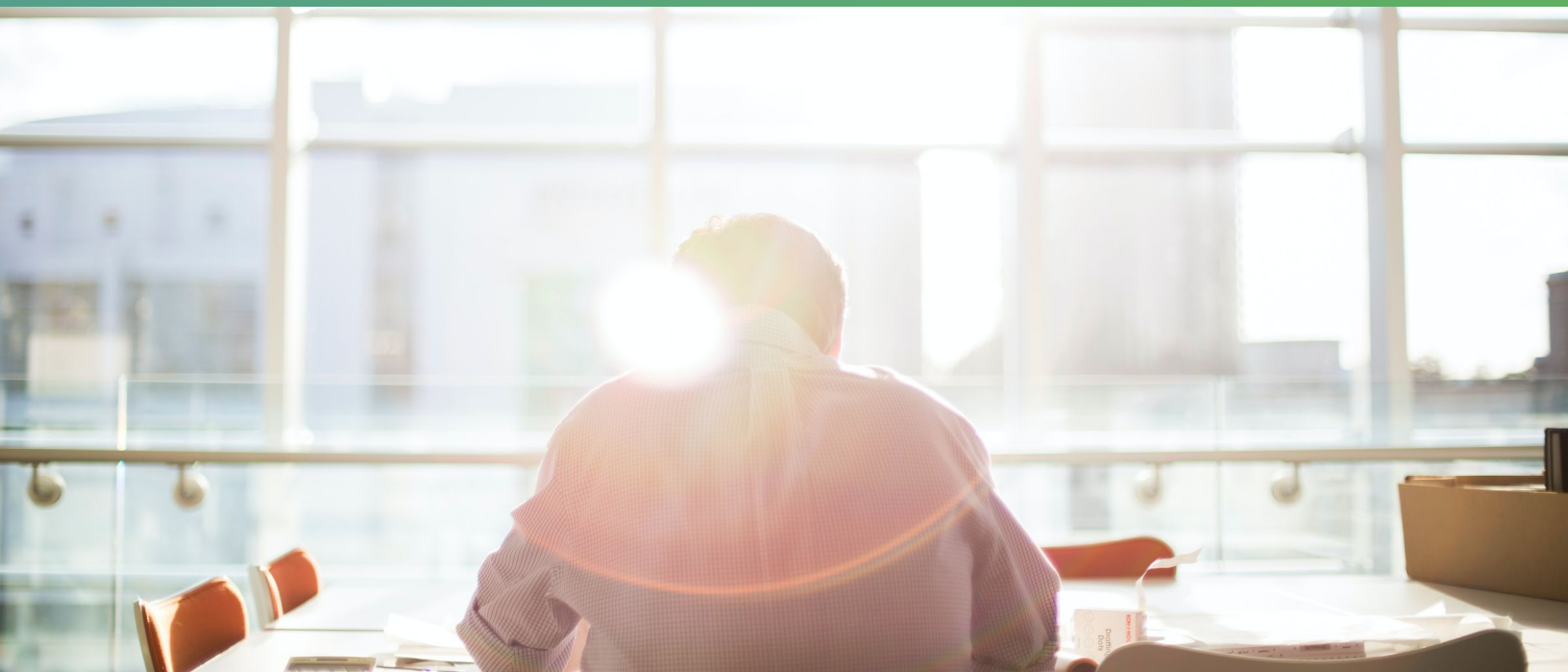
Conclusion

COMPTEC I.T created this Whitepaper to provide the Community and I.T Professionals with Best Practices utilising Microsoft 365.

Previously known as Office 365, Microsoft 365 comes with a preset configuration that includes Security Defaults but offers many more options.

This Whitepaper aims to bring to attention the topic of Advanced Security Policies and Configurations which safeguard businesses and their day-to-day operations.

The topics highlighted in this Whitepaper apply to organisations utilising Microsoft Business Premium or higher licensing.



About author

Konstantinos Xanthopoulos is a Solution Architect for COMPTEC I.T based in Greece. He comes from Enterprise Managed Services with extensive knowledge in architecture and leadership roles within the technology sector.

Konstantinos is widely recognised for his expertise in solutioning and Cyber Security within the Microsoft world.
He is also the Operations Manager for COMPTEC I.T Europe and is responsible for leading the team and driving deliverables, with innovation being high on his agenda.

About COMPTEC I.T

COMPTEC I.T is a modern Managed Services Provider offering businesses end-to-end I.T solutions and services across Australia and Europe. We specialise in System Integration and Cyber Security, and our focus is to deliver high-quality solutions empowering customers' business requirements flexibly, reliably, and securely.

We closely follow the latest technology developments to create more efficient organisations, improve alignment between business technology solutions, and assist customers in meeting their business goals.

Digital Transformation and Innovation are two vital elements for today's organisations to keep up with an ever-changing and evolving world. A successful transformation combines service delivery and solution implementation with zero interruption in day-to-day business activity and ensures 100% Business Continuity.

To learn more, visit www.comptecit.com or follow COMPTEC I.T on LinkedIn @comptecit and Twitter @iComptec.