C-TAG Guidance Document

Secure Deployment of Microsoft 365

Principal Author: Mark Brett

Version 2.0 June 2020

Background

Microsoft 365 (formerly Office 365), has brought a great deal of freedom to organisations, allowing them to virtualise their Office application environment. MS365 is a cloud-based Software as a Service (SaaS), which means that Microsoft host the applications and environment in their cloud, as opposed to local server-based deployment or virtualised desktop deployment such as Citrix. This means that any authorised person can access their corporate information and office applications from anywhere with an internet connection.

The Microsoft Office applications can be either accessed through a web browser or on a locally installed copy of the application. Microsoft have published specific guidance relating to securing MS365 in the cloud [2]. The email services such as Exchange are hosted in the cloud, as is the active directory, which can be synchronised with local network-based active directory services. The Office files are stored on a virtual cloud-based file system, called OneDrive, and again there can be local storage on devices and synchronisation between them. Corporate Intranets of shared file systems (for knowledge or records management), can be established using MS SharePoint and MS Teams, which provides a simplified integration from end to SharePoint. Teams also uses OneDrive for personal chat file storage rather than just SharePoint for Teams channels/chats, as OneDrive has a separate admin panel with configuration options. It is also worth noting that MFA is supported by MS Teams, but it is enforced through Azure AD Conditional Access that Teams integrates with as a target application.

'The Implementation of Security' also encompasses a few of the other steps such as setting up identities, mobile device management (MDM), and service configuration as outlined in the resources they link to. MS365 has been the target for attacks and compromises and will continue to be an attractive target for cyber adversaries, as highlighted by the NCSC in December 2018 [6]. This does not mean that it is unsafe to deploy, but it does mean the built-in security options need to be implemented, and configured to keep it as secure as possible.

Overall, this provides a very powerful and easily accessible suite of Office applications, with secure configuration, access control, digital rights management and audit.

Advice and Guidance

This guidance document primarily pulls together and signposts to trusted advice from third parties, including the National Cyber Security Centre (the UK's National Technical Authority for Cyber Security and Information Assurance). NCSC have written specific guidance to secure office 365 [5]. All of the sources are referenced below, and it is suggested that the reader downloads those documents and understands them thoroughly, or engages with a solutions architect to do so. Data Privacy requirements must always be considered, and the organisation's Senior Information Risk

Officer (SIRO) must sign off on any residual business risks. Any solution must also consider P3T (Personnel, Physical, Procedural and Technical) risks.

Implementing MS365 well requires staff training, guidance and procedures on correct usage, and should be supported by the relevant policies. Some examples are below.

- Acceptable Usage Policy
- End User Device Policy
- Home Working Policy
- Data Transfer Policy
- Video Conferencing Applications and Usage
- Email and Internet Access Policies

The solution will need a data protection impact assessment (DPIA), as personally identifiable information (PII) will be transmitted and received over the link. The Corporate Risk Register may need updating, and an Information Risk Assessment is recommended. Microsoft Office 365 is appropriate to use at OFFICIAL level in accordance with the HMG threat profile. Over 90% of Local Government work comes under this classification. This is also considered commercial good practice and is suitable for most interactions between Councils, their suppliers, citizens and businesses. Protecting Data [14] must always be the main focus.

There is detailed Microsoft guidance for file sharing outside of the organisation in MS365 [8]. There is also an explainer video [7].The recommended approach is to have an Information Governance Framework in place. You should start with the NCSC Cloud Security Principles. This gives an overarching framework that covers the technical requirements for a good cloud services provider. Microsoft have published Cloud Principles assertion documents [3], that details how MS365 meets the NCSC Cloud Principles [1]. The second Microsoft document provides detailed guidance on how to implement the Cloud Principles [4] and provides a policy framework check list.

Securing MS Teams

Teams for Administrators explainer video [10]

There has been a sharp rise in the use of Microsoft Teams, that, again, is a secure application when properly configured and used. There is guidance here on securely using MS Teams [9]. Microsoft Teams is built on the Office 365 hyper-scale, enterprise-grade Cloud, delivering the advanced security and compliance capabilities expected. For more information on planning for security in Office 365, the Office 365 security roadmap is a good place to start. For more information on planning for compliance in Office 365, you can start with the plan for security and compliance article. This article will provide further information about Teams-specific security and compliance. There are also these Microsoft Mechanics videos about security and compliance:

- Microsoft Teams Essentials for IT: Security and Compliance (12:42 min)
- Microsoft Teams Controls for Security and Compliance (10:54 min)

MS Teams enforces team-wide and organisation-wide two-factor authentication, single sign-on through active directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption. Notes are stored in OneNote and are backed by OneNote encryption. The OneNote data is stored in the team SharePoint site. The Wiki tab can also be used for note taking and its content is also stored within the SharePoint site.

Read identity models and authentication for more insight into MS Team authentication, and how modern authentication works will particularly help with modern authentication.

Because MS Teams works in partnership with SharePoint, OneNote, Exchange, and other apps, you should be comfortable managing security in Office 365. To learn more about Office 365 security, read Configure your Office 365 organization for increased security.

Retention Policies

Retention policies in Microsoft Teams allow you to both retain data that is important for your organisation to keep, for regulatory, legal, business, or other reasons, and also to remove content and communications that are not relevant to be retained. You can also use retention policies to keep data for a period of time and then delete it. For further information, review the Retention policies in Microsoft Teams article.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) in Microsoft Teams, as well as the larger DLP for Office 365, revolves around business readiness when it comes to protecting sensitive documents and data in Office 365. Whether you have concerns around sensitive information in messages or documents, DLP policies will be able to help ensure your users do not share this sensitive data with the wrong people. For information on Data Loss Prevention in Teams, please review DLP for Microsoft Teams. There is also this article for O36 DLP concerns called 'overview of data loss prevention'.

Source: https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview

Secure Enterprise deployment: The secure deployment of Office 365 is described on the Microsoft Deployment website.

Do-it-yourself Guided Deployment of Office 365 Enterprise

Deploying Office 365 Enterprise on your own requires detailed research to make the design decisions that streamline Office 365 service configuration and user adoption. Start your planning here.

Following the planning stage, the following steps are useful when deploying Office 365 Enterprise:

1. Set up your network

   Includes adding your Internet domains and optimising the network performance for your on-premises users.

2. Set up your identities

   Includes determining an identity model (cloud-only or hybrid), and for hybrid identity, setting up directory synchronisation between your on-premises Active Directory Domain Services (AD DS) and your Office 365 subscription.

3. Implement security

   Includes configuring and rolling out basic and enhanced security, threat, and information protections for your tenant and identities in the first 30 days, 90 days, and beyond.

4. Deploy client software

   Includes deploying Microsoft 365 Apps for Enterprise (previously named Office 365 ProPlus), the cloud-updated and always-current version of the Office suite (Word, Excel, PowerPoint, and others) on your devices. Every Office 365 client license includes a license for Microsoft 365 Apps for Enterprise.

5. Set up mobile device management

   Office 365 Enterprise includes mobile device management capabilities that help you secure and manage your users' mobile devices.

6. Configure services and applications

   Includes information on migration of your data and links to articles that get you started on key Office 365 services such as Exchange Online, SharePoint Online, and Teams.

7. Train your users

   Includes short videos that help your users get the most out of Office 365 quickly.

Source: https://docs.microsoft.com/en-us/office365/enterprise/setup-overview-for-enterprises

Disclaimer:

This document was produced by bringing together guidance from trusted government agencies, providers and third parties. The information contained in it is accurate and technically correct at the point of publication. Any application of the guidance is solely the discretion of the reader. The authors are not responsible for any consequences of applying the guidance.

Glossary:

DPIA Data Protection Impact Assessment
MS365 Microsoft 365, the new name for Office 365
O365 Office 365 Microsoft office the cloud based productivity suite, now called MS365
PII Personally Identifiable Information under the Data Protection Act

Related Microsoft Guidance:

Alternative Ways for Security Professionals and IT to Achieve Modern Security Controls in Today's Unique Remote Work Scenarios (Microsoft Security Team Blog)
Office 365 Network Connectivity Principles
Assessing Office 365 Network Connectivity
Microsoft 365 Connectivity Test

References:

[1] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
[2] https://news.microsoft.com/en-gb/2019/01/07/government-backs-office-365-cloud-move-after-microsoft-guidance/
[3] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MCCr
[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MHP5
[5] https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration
[6] https://www.ncsc.gov.uk/news/rise-microsoft-office-365-compromise
[7] https://www.microsoft.com/en-gb/videoplayer/embed/RE22Yf0
[8] https://support.office.com/en-gb/article/share-files-outside-your-organization-with-secure-links-7266f44e-3e06-4736-b9d3-0580c24bba34
[9] https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview
[10] https://www.microsoft.com/en-us/videoplayer/embed/RE47cdp
[11] https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide
[12] https://docs.microsoft.com/en-us/office365/enterprise/setup-overview-for-enterprises
[13] https://www.gov.uk/government/publications/government-security-classifications
[14] https://ico.org.uk/for-organisations/guide-to-data-protection/

NB: All links correct as of June 2020.