Victorian Government Office 365 Security Guidance

Digital Victoria

Cyber Security Branch

VICTORIA State Government | Premier and Cabinet

Contents

Document management

Document	
Name	Victorian Government Office 365 Security Guidance
Reference	VG-CISO Guidance 1.4 – Office 365 Security
Approved	John O'Driscoll Victorian Government Chief Information Security Officer Cyber Security Branch, Digital Victoria
Issued	Xavier Brouwer Victorian Government Lead Security Architect Cyber Security Branch, Digital Victoria
Authority	Victorian Government Cyber Security Strategy 2021/2022 *1.5 Issue Victorian Government recommended security configuration for Office365*
Contact for updates	vicgov.ciso@dpc.vic.gov.au
Registration	Version 1.4 D21/143101

WoVG Office 365 Security Guidance

Background

Victorian Government departments and agencies are increasingly adopting Microsoft's Office 365 cloud platform for its email service, document management and collaboration capabilities, and to build and host business applications.

To protect the often sensitive government information hosted on Office 365, this guidance highlights the **minimum recommended controls** and Microsoft **Secure Score** that should be achieved and maintained for all Victorian Government Office 365 tenancies.

Scope

Agency Scope

This guidance is applicable to all Victorian Government departments and agencies including water bodies, health services, TAFEs and Local Government Authorities.

In Scope

- Minimum recommended security controls to ensure a best practice security posture
- Microsoft Secure Scores for the Identity and Applications categories
- Core Office Applications such as Email, MS Teams and SharePoint
- Power Platform
- Azure AD

Out of Scope

- Contractual, licencing and pricing arrangements with Microsoft
- Azure Infrastructure as a Service
- Endpoint Device security
- Microsoft Secure Score for the Devices category

Audience

This guidance is targeted at department and agency:

- Chief Information Security Officers (CISOs)
- Cyber Security Practitioners
- Cloud Platform/Collaboration Managers
- Office 365 Administrators
- Windows/Active Directory/Email Administrators

and assumes a basic knowledge of cloud computing, enterprise email, MFA and enterprise security architectures.

Regulatory Requirements

The following regulatory requirements apply in the context of Office 365:

Essential 8 July 2021 Compliance

Four out of the Essential Eight are relevant to Office 365, namely:

- Application Control
- Configure Microsoft Office Macro Settings
- Restrict Administrative Privileges
- Multi-factor Authentication

Victorian Protective Data Security Standards v2.0 (OVIC)

- “The organisation uses a contextualised VPDSF business impact level (BIL) table to assess the security value of public sector information” [E2.030]
- “The organisation applies appropriate protective markings to information throughout its lifecycle” [E2.50]
- “The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information” [E4.20]
- “The organisation implements logical access controls (e.g. network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know” [E4.40]
- “The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes” [E4.50]
- “The organisation limits the use of, and actively manages, privileged physical and logical access and separates these from normal access (e.g., executive office access, server room access, administrator access)” [E4.60]
- “The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes” [E4.70]
- “The organisation’s information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g. exfiltrating information to criminal associations) and investigative handover” [E6.50]
- “The organisation manages security measures (e.g. classification, labelling, usage, sanitisation, destruction, disposal) for media” [E11.80]
- “The organisation manages security measures for email systems” [E11.100]
- “The organisation logs system events and actively monitors these to detect potential security issues” [E11.110]
- “The organisation uses secure system administration practices” [E11.120]
- “The organisation designs and configures the ICT network in a secure manner (e.g. segmentation, segregation, traffic management, default accounts)” [E11.130]
- “The organisation manages a process for cryptographic keys (e.g. disk encryption, certificates)” [E11.140]
- “The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information” [E11.150]
- “The organisation manages malware prevention and detection software for ICT systems” [E11.160]
- “The organisation manages security measures for enterprise mobility” [E11.200]

Overview

Tenancy Classification

If an Office 365 tenancy only contains information classified up to OFFICIAL or OFFICIAL:Sensitive, the whole tenancy should be classified as **OFFICIAL** (using the ISM definition that includes OFFICIAL:Sensitive) for the context of this guidance. This is also the minimum possible classification for any Victorian Government Office 365 tenancy, UNOFFICIAL (previously UNCLASSIFIED) cannot be used to classify a tenancy.

If a tenancy contains information that is classified PROTECTED, or the amount of OFFICIAL:Sensitive information is aggregated in such a way that the overall Business Impact Level (as per the OVIC VPDSS) increases to “Major” (3), the whole tenancy should be classified as **PROTECTED** for the context of this guidance.

Microsoft’s underlying Office 365 infrastructure in Australia has been IRAP assessed up to and including PROTECTED. We recommend checking that your tenancy is being hosted out of a Microsoft CDC PSPF Zone 4 data centre located in Australia to benefit from this certification.

Some Office 365 applications are not yet hosted in Australia (see the latest status of these here: https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations). It is recommended that only data up to and including OFFICIAL:Sensitive be hosted in data centres outside of Australia (and preferably hosted in the US).

Departments and agencies need to enable additional controls themselves (as per this guidance) to fully realise a PROTECTED (or even OFFICIAL) security posture for their tenancies

Sensitivity Labelling

Victorian Government Office 365 tenancies should not allow the sending emails or storing of documents classified as SECRET (or above)**.** These emails and documents should be processed through other state or federal systems rated to the SECRET level.

Emails or documents labelled as SECRET should be blocked, and a prompt should be displayed explaining why it has been blocked, and the user should be referred to other relevant systems rated SECRET to use instead.

If there is a business need to process PROTECTED level information through an OFFICIAL rated Office 365 tenancy, the tenancy should be reclassified as PROTECTED. Licences may also need to be upgraded to E5, and/or additional external compensatory controls put in place, due to the additional controls required for a PROTECTED level tenancy.

Secure Scores

The use of Secure Scores is an effective way to ensure that the security of Office 365 is **maintained over time**. It is recommended that the achievement and maintenance of the relevant Secure Scores are written into the **Performance Plans** of Office 365 administration/security staff or included in the **contract** of any outsourced service providers providing Office 365 administration services.

Secure Scores can be obtained through the built-in Office 365 Compliance Centre, and can be used by departments and agencies to quickly understand their tenancy's current level of security. This dramatically reduces audit burden by **automatically calculating** a percentage score across three areas (**Identity**, **Applications** and **Devices)** based on the security controls enabled on the tenancy. Furthermore, the Compliance Centre dashboard provides a **detailed breakdown** of specific areas making suggestions of how and where security of the tenancy can be improved.

In addition to departments and agencies using Secure Scores to better understand their own security posture, the Cyber Security Branch (CSB) of Digital Victoria will collect the Identity and Application Secure Scores of each Victorian Government tenancy to identify tenancies that **require help** in uplifting their security. CSB will also periodically publish an anonymous Victorian Government Secure Score **benchmark** to help agencies understand how they compare across the Victorian Government and within their sector. Individual scores from departments and agencies will not be published, rather only the minimum, maximum and average scores across the Victorian Government and for each sector therein. This benchmark data will be classified OFFICIAL:Sensitive and shared only with relevant parties within the Victorian Public Service.

For tenancies classified as **OFFICIAL**, the minimum Secure Score that should be achieved and maintained is: **75%**

For tenancies classified as **PROTECTED**, the minimum Secure Score that should be achieved and maintained is: **85%**

An Office 365 **E3** licence is required to enable the minimum amount of security controls for any Victorian Government Office 365 tenancy.

The Secure Score considers both the enabled security controls and the behaviour/activity (e.g. how well Office 365 administrators and/or Security Operations Centres respond to security alerts)

As Microsoft releases new functionality, Secure Scores may drop until action is taken by departments and agencies to **enable additional security controls** included with this new Office 365 functionality.

If there are compensatory security controls enabled outside of Office 365, there is the option for the equivalent controls within Office 365 to be excluded from the Secure Score calculation.

Cenitex offers a shared service that is available to administer the Office 365 tenancy (and the security controls) of any Victorian Government department or agency from any sector, even if they are not a Cenitex customer from an infrastructure management perspective.

There are also **Microsoft Partners** in Australia that offer services to manage government tenancies. A Silver or Gold partner is recommended for the management of OFFICIAL tenancies, and a Gold partner for PROTECTED.

Security Certification

Administrators and security analysts looking after Victorian Government Office 365 tenancies should hold relevant Office 365 and security-related certifications (https://docs.microsoft.com/en-us/learn/certifications/)

If your organisation has an Enterprise Skills Initiative (ESI) agreement with Microsoft, free self-paced training is available and exams may also be at no extra cost.

It is highly recommended that Office 365 administrators also certify in non-security related Office 365 topics, to reduce the risk of misconfiguration of the platform.

Office 365 Administrators are Privileged Users and therefore should undergo additional personnel checks as per OVIC's **VPDSS Standard 10 – Personnel Security**.

Recommended Controls for OFFICIAL Tenancies

These controls require an E3 licence at a minimum. Note that additional controls to those listed here may be needed to achieve and maintain the required Secure Score for an OFFICIAL classified tenancy.

Conditional Access Policy/MFA

MFA should be required at least **once a day** for all users when accessing Office 365 when outside of a government network or when using a non-government issued/BYOD device.

Weaker SMS-based or Voice Call MFA can be used, however the preference is to use stronger MFA methods such as a smartphone **authenticator app** or hardware/USB **key**. If some users do not want to use their personal phones for MFA, consider issuing them a work mobile or a hardware/USB key for MFA purposes.

> *Privileged users such as Office 365 administrators should use strong MFA in all situations (including both when on and off a government network/device)*

An **idle timeout** (no activity) of 4 hours is recommended before authentication is re-invoked.

If there is a valid business case for a specific user account to not have MFA, this account can be placed in an “**Exclude group**” and its use closely monitored by your Office 365 administrators or Security Operations Centre.

If MFA has not already been enabled for all users, consider a **staggered implementation** by first enabling MFA for administration roles, then for specific high risk system access, and then for the remaining users.

The following controls are recommended to prevent MFA being breached through MFA (Prompt) Bombing/Fatigue/Spamming:

- Enable Azure MFA number matching / MFA two-digit codes
- Show additional context to end users in MFA push notifications
- Limit the amount of MFA failures that can occur before an account is temporarily locked
- Implement Azure AD Identity Protection
- Monitor and alert on Azure AD / MFA events in your SIEM
- Monitor and alert on new MFA and MDM device enrolments (unusual behaviour)
- Protect against password spray using Azure AD Password Protection
- Disable MFA Push Notification (revert to manual inputting of temporary six-digit code)

Lifecycle Management

All users should automatically lose access to Office 365 within 24 hours of being terminated in a Human Resources system, Active Directory, or Identity Lifecycle Management System.

All non-permanent staff should have expiry dates against their accounts to execute this process automatically as soon as the expiry date has passed.

Legacy Authentication & Encryption

Legacy authentication (e.g. IMAP or POP, as opposed to modern OAuth-based authentication) should be **disabled**. This may require application email relay use cases to be moved onto another cloud-based email server, replacing or upgrading meeting room booking console systems, or replacing legacy in-office video conferencing systems with screens allowing users to use Microsoft Teams meetings through their work devices.

Deprecated encryption such as TLS 1.0 and 1.1 should not be used.

Guest Management

Conceptually there are three trust levels for end users in a Victorian Government context

- **Agency** users (from the same department or agency) = High Trust
- **Government** users (from other Victorian, State or Federal government departments or agencies, or associated bodies with contractual or Memorandum of Understanding (MOU) arrangements with the trusting agency) = Medium Trust
- **External** users (with no official relationship with the trusting agency) = Low Trust

Government and External guest users should be required to use MFA in all circumstances. It is recommended these users use their **own Azure AD account** from their workplaces' Office 365 tenancy (if they have one), rather than recreating an account in your own Azure AD. This way their access to your tenancy is automatically revoked if they are revoked from their own tenancy.

It is recommended to create **Dynamic Groups** to track guest accounts and apply different levels of access, and to allocate a sponsor to these groups. The sponsor should be responsible for performing monthly user access reviews for guest access. This can be set up as a recurring task in Office 365, or in a separate Identity Lifecycle Management system linked to Azure, or in an IT Service Management system as a recurring ticket.

Guest accounts should have **minimal privileges** and should not have any tenancy level administration roles or be SharePoint or Teams site owners. External users should not be allowed to share files they don't own, or further extend access to other external users.

Government and External access to content is best managed through a Teams Site, using Guest Access controls, blocking external sharing from OneDrive, and through the use of Shared Channels.

Labelling

Users should label each email they send or each document they save using the standard government labels (UNOFFICIAL, OFFICIAL, OFFICIAL:Sensitive).

PROTECTED, SECRET or TOP SECRET information **should not** be emailed through or saved to OFFICIAL rated Office 365 tenancies.

Data Loss Prevention

At a minimum, the following Data Loss Protection policies should be put in place and tuned on a quarterly basis:

- blocking PROTECTED documents from being saved or emailed to anyone, and alerting admins to these attempts
- alerting when OFFICIAL:Sensitive documents are emailed to an external non-government email address
- alerting when OFFICIAL:Sensitive documents are being downloaded or printed en masse by anyone
- preventing any content from being downloaded and distributed by External Guest Users
- identifying offensive language
- identifying cleartext passwords
- identifying Personally Identifiable Information
- identifying financial (e.g. credit card) data
- identifying personal health information (if applicable)
- identifying sensitive information relevant to the department/agency that may not yet be labelled

It is recommended that sector-specific policy configurations be **shared** across departments and agencies in each sector (e.g. health, water, LGA, justice) to avoid re-work in each tenancy.

Third Party Applications

End users should not be able to add **Third Party Applications** or **Webparts** (e.g. from the Marketplace). This process should be managed by Office 365 administrators who should seek management/security/IT change management approval before proceeding. Outlook 365 **third-party file view integration** should also be disabled, as should **third-party file storage** and the ability for third party apps from the store to open office documents in the browser. The ability for external users to request permissions to access an internal party’s application should also be disabled.

PowerShell & Service Accounts

To cater for a lack of interactive MFA, PowerShell and Service Accounts should be: restricted to certain locations, be on a government network, have longer and more complex passwords, disallow interactive logon, and have their secrets rotated at least annually.

PowerShell should be **disabled** for all standard users.

Email

Some of these controls may be fulfilled by email filtering systems outside of Office 365.

- Enable all **anti-spam**, **anti-malware** and **anti-phishing** controls
- Block emails with **ransomware** extensions
- Add a **warning banner** into emails if the provenance of the email is outside of the same, or another, Victorian Government email domain
- Add a **warning banner** into emails if the incoming external email fails SPF and/or DKIM checks
- Block incoming emails if they have a **classification above** OFFICIAL:Sensitive
- Warn users before opening Office file attachments that include **macros**
- Alert admins on the creation of **forwarding/redirect** rules to external email addresses
- Alert admins when suspicious email sending **patterns** are detected

Password/MFA Reset Process

To avoid account or MFA takeover (including through social engineering), secure self-service/admin/helpdesk password/MFA reset processes should be implemented e.g.:

- A self-service process requiring MFA before a password is reset or a new MFA is registered
- A manual process requiring service desk involvement with security questions based on an end user’s private HR data, or requiring approval from the end user’s manager to proceed

End users should be **alerted by email** when a new device logon occurs, when their password is changed/reset, or if their MFA is registered/reset.

Logging & Monitoring

It is recommended that **Unified Audit Logging** is enabled and configured with a minimum 1-year (preferred **2-year**) retention period for all end user and admin logging events. The default E3 licence retention is 90 days, a 1-year retention period requires an E5 Compliance or E5 eDiscovery licence with an Audit add-on license.

Other logging options include: sending logs to a logging server, Azure data storage or a SIEM system.

Ensure the storage account containing the container with activity logs is encrypted with a key that is stored securely outside of Office 365 (e.g. in a department or agency key vault).

Alerts should be acted on within **24 hours** by either your Office 365 Administrators or your Security Operations Centre.

Calendars

It is recommended to disable the **external visibility** of meeting names, content and invitees. **Free time visibility** for other Victorian Government tenancies can occur to enable cross-agency meetings to be arranged more easily.

Power Platform

A governance process should be put in place to ensure that each application built on the Power Platform is:

- **Reviewed** by an Office 365 Administrator, Enterprise Architect and/or IT manager in order to ensure that it is not replicating the functionality of an existing or commercially available application (in house, COTS or SaaS based), i.e. apply the "re-use before buy before build" principle
- **Registered** in the organisation's Application Register as well as the organisation's Information Asset Register (as per OVIC)
- **Assessed** using OVIC's Confidentiality, Integrity and Availability ratings, and allocated a label (e.g. OFFICIAL, PROTECTED etc), as well as a business owner

The **Centre of Excellence Starter Kit** (https://docs.microsoft.com/en-us/power-platform/guidance/coe/starter-kit) gives good visibility into how the Power Platform is used within a tenancy, and alerts can be configured to capture new Power Platform deployments that haven't gone through an official governance process.

Least Privilege access should be applied across all layers of the Power Platform e.g.

- **Tenant** (including cross-tenant exfiltration controls)
- **Environments**
- **Resources**
- **Connectors** (including tightening the privileges in the systems being connected to, and Data Loss Prevention policies should be configured to prevent "business" and "non-business" connectors being used in the same application)
- **Dataverse** data
- **On prem data gateway** and data (this can be disabled unless required, and on-prem components should be kept patched and secured in their own right)

It is also important to ensure the Power Apps portal is set to **private** rather than public.

Yammer

The following security controls are recommended for agencies using Yammer:

- Subscribe to **Yammer Enterprise** to get better security and compliance tools (Yammer Basic should not be used for government business)
- Do not post data classified **PROTECTED** onto Yammer
- Use **InTune** or equivalent to manage the Yammer app on staff devices
- Synchronise Yammer users with **Azure AD** to automatically add and remove users from Yammer
- Use multiple levels of admin roles so you can assign the correct permissions to match employee's roles (the concept of **least privilege**)
- Prevent or limit file **uploads**
- Control **external network** access (preferably do not allow external networks, or only allow admins to create them, and preferably do not allow external parties into an internal network)
- Track Yammer Events in the Office 365 **Audit** log and with the Management Activity API
- Set up a **usage policy** to ensure only appropriate content is posted
- Monitor keywords for unacceptable or **inappropriate content** so you can intervene if necessary.
- For large organizations, use **dynamic groups** to update group membership automatically as people join, leave, or move within your organisation
- Set **expiration policies** for Office 365 connected Yammer groups. When set, group owners are prompted to renew the groups if they still need them

Recommended Controls for PROTECTED Tenancies

These controls require an E5 licence at a minimum. Note that these controls are in addition to or override/extend the OFFICIAL controls listed above.

Conditional Access Policy/MFA

MFA should be required for PROTECTED tenancies at least once per day for **all users** in **all situations** (i.e. whether they are on or off a government network, or using a government issued or BYOD device).

Weaker SMS or Voice Call MFA should not be used for PROTECTED tenancies which should use stronger MFA methods such as smartphone **authenticator apps** or hardware/USB **keys**.

End users should be alerted by both **email** and **SMS** when a new device logon occurs, when their password is changed or reset, or if their MFA is registered or reset.

An **idle timeout** (no activity) of 1 hour is recommended before authentication is re-invoked.

Privileged Access Management

Privileged users (e.g. Exchange Administrator, SharePoint Administrator, Teams Service Administrator, Power BI Administrator) should use additional just-in-time **Privileged Identity Management** controls offered by Office 365, or have their credentials and sessions managed by a separate **Privileged Access Management** platform.

Customer Lockbox (for controlling Microsoft technician access to Email, SharePoint and OneDrive data for the purposes of troubleshooting) should be enabled and used.

Labelling

Users should label each email they send or each document they save using the standard government labels (UNOFFICIAL, OFFICIAL, OFFICIAL:Sensitive, PROTECTED).

SECRET or TOP SECRET information **should not** be emailed through or saved to PROTECTED rated Office 365 tenancies.

Security Testing

PROTECTED level tenancies should be subjected to a penetration test or Red Team simulated attack at least once per year. The scope of this should include: end user account take over, privileged user account takeover, and service desk social engineering attacks.

Data Loss Prevention

The following additional Data Loss Protection (DLP) policies can be put in place and tuned on a **monthly** basis:

- preventing PROTECTED documents from being emailed as an attachment to **anyone** (within the organisation or outside of the organisation). A link requiring user authentication (with MFA) to access PROTECTED documents may still be sent to external users as long as they are being managed as per the Guest User guidance above
- blocking en masse downloading or printing of PROTECTED documents by anyone
- identifying national security information (if applicable, refer to the relevant federal agency for a copy of their DLP policy if they are using Office 365 and have one)
- enabling DLP for Teams chat and channels

Email

- Configure alerting administrators on the **Elevation of Exchange admin** privileges
- Configure alerting administrators when a **Malware campaign** is detected
- Configure alerting administrators when **Phish emails delivered** because a user's Junk Mail folder is disabled
- Enable ATP **Safe Attachments** and **Safe Links** for blocking malicious attachments and links in phishing emails including in SharePoint, OneDrive, Microsoft Teams and Office clients
- Enable **Azure Information Protection** and **Azure Rights Management** to encrypt files labelled PROTECTED
- Block **Auto-forwarding** to External Domains (manage any exceptions in a controlled way
- Block incoming emails if they have a **classification above** PROTECTED

Logging & Monitoring

- Enable a minimum **2-year retention** for all end user and admin logging events. This can be achieved by: shipping logs to a logging server, Azure data storage or a SIEM system, or adding the 10-year audit log retention add-on license to your E5 licence.
- Monitor and alert on **suspicious admin/privileged user behaviour**.
- Monitor and alert on **changes to admin accounts/settings**.
- Alerts should be acted on within **one hour** by either your Office 365 administrators or your Security Operations Centre.

References

Reference / Acronym	Description
ACSC	Australian Cyber Security Centre https://www.cyber.gov.au/
CIS	Center for Internet Security https://www.cisecurity.org/benchmark/microsoft_365
DKIM	Domain Keys Identified Mail https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email
DLP	Data Loss Protection
DMARC	Domain-based Message Authentication, Reporting, and Conformance https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email
DTA	Digital Transformation Agency https://desktop.gov.au/blueprint/office-365.html
ISM	Information Security Manual https://www.cyber.gov.au/acsc/view-all-content/ism
IRAP	Infosec Registered Assessors Program https://www.cyber.gov.au/acsc/view-all-content/programs/irap
LGA	Local Government Authority
MFA	Multi Factor Authentication
MS	Microsoft https://www.microsoft.com
O365	Microsoft Office 365 https://docs.microsoft.com/en-us/microsoft-365
OVIC	Office of the Victorian Information Commissioner https://ovic.vic.gov.au/

Reference / Acronym	**Description**
PSPF	Protective Security Policy Framework https://www.protectivesecurity.gov.au/
SOC	Security Operations Centre
SPF	Sender Policy Framework https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing
VPDSS	Victorian Protective Data Security Standards https://ovic.vic.gov.au/data-protection/standards/
WoVG	Whole of Victorian Government