Australian Government
Digital Transformation Agency

Protected Utility Blueprint

Office 365 Design

March 2020

dta

Contents

Background

The DTA developed the Protected Utility Blueprint to enable Australian Government agencies to transition to a secure and collaborative Microsoft Office 365 platform. The solution is underpinned by proven technologies from the Microsoft Modern Workplace solution (Microsoft 365 including Office 365, Enterprise Mobility + Security, and Windows 10). The Blueprint design is delivered as three distinct documents:

- **Platform** – Provides technologies that underpin the delivery of the solution,
- **Workstation** – The client device, which is configured and managed by Microsoft Intune, and
- **Office 365** – Microsoft Office 365 productivity applications.

The Blueprints are accompanied by Configuration Guides and Security Documentation adhering to the Australian Cyber Security Centre (ACSC) PROTECTED requirements for Information and Communication Technology (ICT) systems handling and managing Government information. These artefacts provide a standard and proven Microsoft 365 solution aimed to fast track the adoption of the Microsoft Modern Workplace experience.

The following Blueprint documentation contains considerations for best practice deployment advice from the Australian Government Information Security Manual (ISM), relevant Microsoft hardening advice, the ACSC Essential Eight and the ACSC hardening guidelines for Microsoft Windows 10.

Overview

Purpose

This document provides the design of the technology components that will be implemented to support Office 365. For technologies and services not covered, refer to the respective design document.

Scope

Table 1 describes the components that are in scope for the design.

Table 1 In Scope Components

Component	Inclusions
Office 365 Organisation	Residency Licencing Themes Services & Add-ins Microsoft Search Customer Lockbox
Office 365 Connectivity	Firewall Optimisation
Office 365 Exchange Online	Mail Flow Mail Exchange Records Autodiscover Senders Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) Accepted Domains Remote Domains User Mailbox Configuration Authentication Policies Outlook on the Web Policies Mailbox Auditing Mailbox Auditing Journaling Shared Mailboxes Resource Mailboxes Distribution Lists Dynamic Security Groups Office 365 Groups

	Public Folders Address Book / Address List Mail Contacts
Office 365 Exchange Online Protection	Connection Filtering Anti-malware Policy Filtering Content Filtering
Mail Gateway	Mail Gateway
Office 365 SharePoint Online	SharePoint Online base Configuration
OneDrive for Business	OneDrive for Business Configuration Size Limits Retention Period Backups
Microsoft Teams	Microsoft Teams Configuration Instant Messaging Collaboration Desktop/app sharing Whiteboarding Voicemail Conferencing Broadcasting
Office 365 Advanced Threat Protection	Office 365 ATP Safe Links Office 365 ATP Safe Attachments Office 365 ATP Anti-Phishing
Security and Compliance Center	Alerts Labels Data Loss Prevention Retention Policies Audit Logging Customer Key

Beyond the Blueprint

The Blueprint is designed to provide a baseline cloud only offering for all government agencies. Even if a product is licenced for use under Microsoft, it may not be included in this Blueprint if it is not required for all agencies. An organisation may have additional requirements that will need to be considered outside of this Blueprint including the following:

Component	Exclusion
Office 365 Organisation	Microsoft Search
Security and Compliance Center	Customer Key (requires two azure subscriptions)
PowerApps	PowerApps Configuration
Microsoft Flow	Flow Configuration
Power BI	Power BI

Documentation

Associated Documentation

Table 2 identifies the documents that were referenced during the creation of this design.

Table 2 Associated Documentation

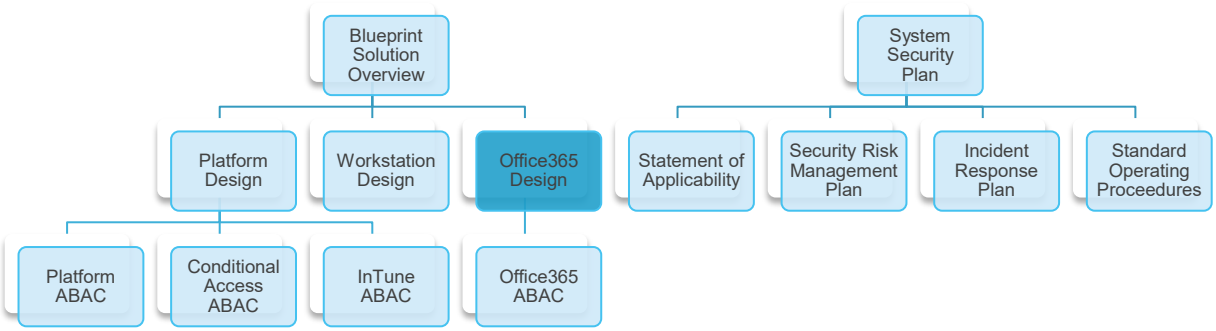
Name	Version	Date
ACSC - Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016[1]	N/A	01/2020
ACSC - Hardening Microsoft Windows 10, version 1709, Workstations[2]	N/A	01/2020
Azure - ACSC Consumer Guide - Protected - 2018	N/A	08/2018
Australian Government Information Security Manual (June 2019)	N/A	10/2019
DTA – Blueprint Solution Overview	March	03/2020
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 – ABAC	March	03/2020
DTA – Platform – ABAC	March	03/2020
DTA – Intune Security Baselines – ABAC	March	03/2020
DTA – Software Updates – ABAC	March	03/2020
DTA – Intune Applications – ABAC	March	03/2020
DTA – Intune Enrolment – ABAC	March	03/2020
DTA – Conditional Access Policies – ABAC	March	03/2020
DTA – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020
Protective Security Policy Framework – Sensitive and classified information[3]	2018.2	02/2018

[1] https://www.cyber.gov.au/publications/hardening-microsoft-office-2016
[2] https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-build-1709
[3] https://www.protectivesecurity.gov.au/sites/default/files/pspf-infosec-08-sensitive-classified-information.pdf

Document Structure

This document is part of the blueprint set of documents as shown in Figure 1 and is technical in nature with the audience expected to be familiar with Office 365 installation and configuration.

Figure 1 - Blueprint Documentation Set



This document covers the information as described in Table 3

Table 3 Document Structure

Section	Description
Design Considerations	This section details items that should be taken into consideration during and after the deployment of this solution.
Office 365 Organisation	Office 365 allows for the configuration of organisation wide settings through the use of a centralised management portal.
Office 365 Connectivity	Office 365 is a globally distributed service. The user experience with Office 365 involves connectivity through highly distributed service connection points that are scaled over many Microsoft locations worldwide.
Exchange Online	Exchange Online is a cloud hosted email solution that has the capabilities of on-premises Exchange Services.
Exchange Online Protection	Exchange Online protection is a cloud hosted email security service (Mail Gateway) that acts to filter spam and scan for viruses on email entering and leaving Exchange Online.
Mail Gateway	The Mail Gateway acts as the central egress and ingress point for mail traffic into an organisation.

SharePoint Online	SharePoint online is an online collaboration and file storage solution. SharePoint integrates heavily with Teams and OneDrive.
OneDrive for Business	OneDrive is a file hosting and file synchronisation solution.
Microsoft Teams	Teams is a cloud hosted unified communications platform. It provides chat, meetings, file storage, and application integrations.
Office 365 Advanced Threat Protection (ATP)	Office 365 ATP is a cloud-based mail threat protection service. The service provides protection against unknown malware and viruses through the use of robust zero-day protection and inclusion of features to safeguard an organisation from harmful links in real time.
Security and Compliance	Office 365 provides Security and Compliance tools which can be utilised to implement an organisation's Information Management Policy and to assist with information governance.

For each component within the document there is a brief description of the contents of the section, a commentary on the things that have been considered in determining the decisions and the design decisions themselves.

Design Considerations

This section details items that should be taken into consideration during and after the deployment of this solution.

Centralised Logging Facility

This design recommends Microsoft 365 E5 licensing to ensure that the advanced security features available in the E5 suite are leveraged by the Commonwealth. Office 365 E3 is included as standard in the Microsoft VSA4 agreement with the Commonwealth. Office 365 E5 provides several advantages and is recommended by this design to enable the Commonwealth to leverage Microsoft's enhanced security features.

Office 365 audit records will be retained for 90 days with the Office 365 E3 licensing tier. Audit logs can be retained for one year with an Office 365 E5 licence or by purchasing Advanced Compliance add-on license with Office 365 E3 licences[4].

It is recommended the Department consider a centralised logging solution to retain Office 365 logs for greater than one year to comply with Commonwealth auditing requirements. Log Analytics (a Microsoft Azure capability) can be configured to centralise the logs for Office 365, Office 365 Advanced Threat Protection (ATP), Microsoft Defender ATP and Intune clients, but has a maximum retention period of two years. A third-party centralised logging solution would provide a longer retention period for Office 365 audit records.

Basic Authentication

Basic authentication provides the ability for Office 365 to communicate with Exchange 2010. This is deprecated and basic authentication will be blocked by default in favour of Modern Authentication. Any required tools/solutions requiring basic authentication should be reviewed and remediated as a prerequisite activity to implementing this solution.

Data Migration

The current design is for a 'greenfield' solution. Auditing, analysis, and migration (if required) of existing data into the solution should be considered. During the auditing and analysis phase particular emphasis should be placed on:

[4] https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance

- Migration Tool Selection
- Bandwidth Available for Migration
- Archive or Migrate data
- User Migration approach

Possible migration tools which could be leveraged for the different information types include:

- Exchange Personal Storage Table (.pst) file migration
- SharePoint Migration Tool for network shares and SharePoint migration
- ShareGate for SharePoint migration

All of the above should be considered as part of a migration strategy.

GovLink

Where GovLink is not required, Exchange Online can be used for mail directly. Where GovLink is required by the Department, please refer to the Solution Overview document for more information.

Telstra Calling and collaboration

Enables agencies to make calls to landlines or mobiles within Microsoft Teams. Telstra calling avoids the complexity of separate collaboration systems. This is discussed in detail in the Microsoft Teams section.

Office 365 Organisation

Office 365 allows for the configuration of organisation wide settings through the use of a centralised management portal. Theses settings drive the user experience organisation wide. Licencing is configured at an organisation wide level.

The settings which are configurable at this level include:

- Residency
- Licencing
- Themes
- Microsoft Search
- Customer lockbox configurations

Residency

Description

Office 365 is a global service which is offered in many different physical regions. Choosing a region to store data is required to ensure that the data of the Department does not get transferred or stored offshore.

Design Considerations

Office 365 tenant residency is critical when setting up of the Department's Office 365 tenant. The region where Office 365 tenant is set up will determine where the data is store. Details of Office 365 data residency can be found from Microsoft's site[5].

Office 365 tenant data residency consideration is required to ensure the agency Office 365 tenant is created and data is stored in Australia.

Design Decisions

Table 4 describes the Office 365 region design decisions.

[5] https://products.office.com/en-au/where-is-your-data-located

Table 4 Office 365 Region

Decision Point	Design Decision	Justification
Office 365 Region	Australia	Ensures data remains onshore, either Sydney or Melbourne.

Licencing

Description

This section will provide licence and licencing configuration consideration to ensure that the agency Office 365 tenant can be assessed up to the PROTECTED level.

Design Considerations

Microsoft offers a number of enterprise licencing options for Office 365, Enterprise Mobility and Security (EMS), and Windows.

These licencing options are summarised below:

- **Microsoft 365 E5 (recommended for this Blueprint)** – Top level Enterprise Plan. Microsoft 365 E5 includes everything inside Microsoft 365 E3 plus additional features and services (largely security and compliance related). In the case of Office 365 E5, the capabilities in Office 365 Advanced Threat Protection (ATP) suite as well as other services such as Office 365 Advanced Compliance are increased.
- **Microsoft 365 E3** - Mid range Enterprise Plan. Microsoft 365 E3 provides access to core products with enhanced features and security features. In the case of Office 365 E3, the Office client suite is included, and the service limits are increased.

To grant access to the services a license is assigned to an individual user account. A license can be assigned by an administrator at the time of the user account is created or through Azure AD group-based licensing. Azure AD group-based licensing allows an Administrator to associate a license to a group. Any members within the group will be assigned that license automatically. When a user is removed from the group the license is removed.

Design Decisions

Table 5 describes the Licencing design decisions.

Table 5 Licencing Design Decisions

Decision Point	Design Decision	Justification
Products Licenced	Office 365 E5	Office 365 E5 licences in combination with EMS E5 are required to obtain all required features for the solution.
Licence Allocation Method	Automated	All user account names that do not contain the text '_priv' will be assigned a Microsoft 365 E5 licence automatically assign licences and applications to users. Ensures privileged accounts do not get licences.

Table 6 describes the Licencing configuration.

Table 6 Licencing Configuration

Configuration	Value	Description
Admin Licence Group	rol-AgencyName-Administrator	This is the group that the agency administrators belong to.
User Licence Groups	rol-AgencyName-Users	This is the group that the agency non-administrator users belong to.

Themes

Description

Office 365 Themes provide a method to customise the portal's look and feel for users.

Design Considerations

The logo of the organisation can be added to the top navigation panel. Themes assist users with familiarisation and adoption of the new system.

Design Decisions

Table 7 describes the Theme design decisions.

Table 7 Theme Design Decisions

Decision Point	Design Decision	Justification
Custom Portal Theme	Configured	Customising the Theme setting assists user to identify that they are in the correct portal.

Note: Themes will be the responsibility of the Agency branding section and this table contains recommendations and restrictions for the themes.

Table 8 describes the Theme configuration.

Table 8 Theme Configuration

Configuration	Value	Description
Logo Image	Agency logo is recommended	Under 10 KB, 200 x 30 pixels in JPG, PNG, GIF, or SVG format. SVG is the preferred format.
Background Image	Agency logo is recommended	15 KB or less, 1366 x 50 pixels in JPG, PNG, or GIF format. This is in line with Microsoft best practice.
Prevent users from overriding their theme	Yes	Flip this toggle to prevent users from choosing their own theme from the Microsoft theme gallery. This is enabled to maintain cadence between potential personal tenancies and the 'corporate' environment.
Navigation bar colour	Default	Based on agency branding standards. To maintain cadence with corporate standards.
Text and icon colour	Default	Based on agency branding standards.
Accent Colour	Default	Based on agency branding standards.
Show the users name on the top navigation bar when the user is signed in	Yes	The users name will be shown to identify who is signed in.

Office 365 Services and Add-Ins

Description

Office 365 centrally manages Office services and add-ins. Office services and add-ins can enhance both the way information is accessed and the way business is conducted. Enabling Services and Add-ins also comes with risks (such as the risk of data loss). Out of the box several services and add-ins are configured within the portal.

Design Considerations

The design will take into consideration the services and add-in that are part of Office 365. The design decision is based on the requirement provided by the department and location of the application that is hosted on.

Design Decisions

Table 9 describes the Services and Add-ins design decisions.

Table 9 Services and Add-ins Design Decisions

Decision Point	Design Decision	Justification
Azure Speech Services	Disabled	Default setting
Bookings	Disabled	Required to meet security recommendations
Calendar	Disabled	ACSC recommendation is to not share calendar information for PROTECTED systems.
Cortana	Disabled	To align with ACSC Windows 10 1709 hardening, Page 55.
Integrated Apps	Disabled	Required to meet security recommendations
External Form sharing	Disabled	Microsoft Forms is hosted outside of Australia.
Microsoft Graph Data Connect	Enabled	API connectivity required for solution management.
Microsoft Planner -iCalendar publishing	Enabled	Internet calendars will be enabled, it is up to the agency which calendars they wish to publish.

Microsoft Search in Bing	Disabled	Microsoft Search integrates with bing.com for Search. Office 365 data is indexed to provide bing.com search functionality and is therefore not desirable for this design.
Microsoft communication to users	Disabled	System admins will be responsible for communication to users
Modern Authentication	Enabled	Modern authentication is an group of technologies that combines authentication, authorisation and conditional access policies to secure an Office 365 tenant. Enabling of Modern Authentication provides ability to use Multi Factor Authentication.
MyAnalytics	Enabled	Provides users with details about their usage of Office 365
External Office 365 group content sharing	Enabled	External collaboration will be conducted in Microsoft Teams which relies on Office 365 groups
Office software download settings	Disabled	Only one instance of the Office Suite is to be installed per user on their Government issued device. Office applications will be deployed to users via the Business Store.
Office on the web	Disabled	Do not allow users to open files in third party storage
Reports	Disabled	Disable data reporting to Microsoft on Office 365 usage.
SharePoint	Enabled	New and Existing guests must sign in or provide a verification code when accessing SharePoint data.
External Sway sharing	Disabled	External collaboration will be conducted in teams.
User owned apps and services	Disabled	Applications will be delivered via the Business Store, there is no need to have the Official Store enabled.
Whiteboard	Disabled	Microsoft Whiteboard is not hosted in Australia.

Self Service Purchase

Description

Self-Service purchase add-ins for Office 365 allows users of Office 365 to purchase 3rd party add-ins to be added into Office 365 tenancy.

Design Considerations

Self-service purchase of applications from the Microsoft Power Platform products was introduced in January 2020. By default, this is enabled for all users within the tenant and paid by credit card.

These processing of data for these add-ins does not sit within Office 365 tenancy. This might cause the data to flow outside and/or stored outside of Australia.

Design Decisions

Table 10 describes the Self-Service design decisions.

Table 10 Self-Service Design Decisions

Decision Points	Design decision	Justification
Global self-service purchase	Disabled	Only administrators are permitted to purchase applications
Power BI self Service purchase	Disabled	Only administrators are permitted to purchase applications
Power Apps self-service purchase	Disabled	Only administrators are permitted to purchase applications
Power Automate (Flow) self-service purchase	Disabled	Only administrators are permitted to purchase applications

Customer Lockbox

Description

Customer lockbox provides a time-boxed, secure mechanism for Microsoft Support Engineers to assist in customers support query in Office 365. Microsoft Support engineers will have to request authorisation from the department to access the underlying data in Office 365 tenant.

Design Considerations

Customer Lockbox address situations where Office 365 Administrators need explicit control, in rare instances, when a Microsoft engineer is needed to access said data to resolve an issue. This ensures all interaction are recorded for auditing purpose.

Design Decisions

Table 11 describes the Customer Lockbox design decisions.

Table 11 Customer Lockbox Design Decisions

Decision Points	Design decision	Justification
Customer Lockbox	Enable	This is to ensure the agency approves any log interaction with Microsoft Support Engineers.

Office 365 Connectivity

Description

Office 365 is a globally distributed service. The user experience with Office 365 involves connectivity through highly distributed service connection points that are scaled over many Microsoft locations worldwide.

Design Considerations

To minimise latency, a customer network should route user requests to the closest Office 365 service entry point, rather than connecting to Office 365 through an egress point in a central location or region.

The following is recommended to achieve optimal Office 365 connectivity and performance:

- **Local DNS resolution and Internet egress -** Provision local DNS servers in each location and ensure that Office 365 connections egress to the internet as close as possible to the user's location. This configuration minimises latency and improves connectivity to the closest Office 365 entry point
- **Add regional egress points -** If an organisations network has multiple locations but only one egress point, add regional egress points to enable users to connect to the closest Office 365 entry point. This configuration minimises latency and improves connectivity to the closest Office 365 entry point
- **Bypass proxies and inspection devices -** Configure browsers to send Office 365 traffic directly to egress points and bypass proxies. Configure edge routers and firewalls to permit Office 365 traffic without inspection. This configuration minimises latency and reduces the load on network devices
- **Enable direct connection for VPN users -** For VPN users, enable Office 365 connections to connect directly from the user's network rather than over the VPN tunnel by implementing split tunnelling. This configuration minimises latency and improves connectivity to the closest Office 365 entry point

Office 365 is a publicly facing SaaS offering. As such, several firewall ports are required to be opened to allow communication between infrastructure and desktops and Office 365.

The detail of these configuration elements is available online from Microsoft[6] and are updated as required to accommodate for product updates and routine change.

It is important to note the traffic between the clients and the Office 365 offering is TLS1.2 encrypted. It is possible that will not be compliant with the ISM requiring Transport Layer Security (TLS) 1.3 as of the August 2018 update. As at 17 Sep 2019 Microsoft is still in the process of preparing for TLS 1.3 in Office 365.[7]

Design Decisions

Table 12 describes the Office 365 Connectivity Optimisation design decisions.

Table 12 Office 365 Connectivity Optimisation Design Decisions

Decision Point	Design Decision	Justification
Local DNS resolution and Internet egress	Configured	DNS will be resolved to the gateway of their internet device.
Add regional egress points	Not Configured	Regional Egress Points are not configured in this solution due to the workstations being directly connected to the internet.
Bypass proxies and inspection devices	Not Configured	Proxys are not configured in this solution due to the workstations being directly connected to the internet.
Enable direct connection for VPN users	Not Configured	VPN's are not configured in this solution due to the workstations being directly connected to the internet.
ExpressRoute Connectivity	Not Configured	Express Routes are not required or configured in this blueprint.

[6] https://docs.microsoft.com/en-au/office365/enterprise/urls-and-ip-address-ranges
[7] https://docs.microsoft.com/en-us/office365/troubleshoot/security/prepare-tls-1.2-in-office-365

Mail Flow

Description

Mail flow is the path taken by an email from the sender to a receiver. A mail gateway can act as the central ingress and egress point for mail traffic into and out of an organisation.

Design Considerations

A mail gateway provides various functionalities, including:

- SPAM filtering
- Phishing protection
- Antivirus
- Encryption
- Message rules
- Header modification

Once mail enters the mail gateway it is processed and sent through to mail servers through the use of listeners and Host Access Tables.

Where organisations are not running a PROTECTED environment, GovLink is not required and Exchange Online can be used for mail directly.

GovLink[8] is a cost-effective solution to enable secure communication between Commonwealth entities across public infrastructure, and is required for PROTECTED mail to be securely transferred between government organisations. When a GovLink mail gateway is required this can be either an existing gateway or a new gateway. More information is provided in the Solution Overview document.

It is not possible to configure Exchange Online to directly send email via GovLink. Exchange Online must resolve to a public facing IP address, which is not possible across the GovLink solution.

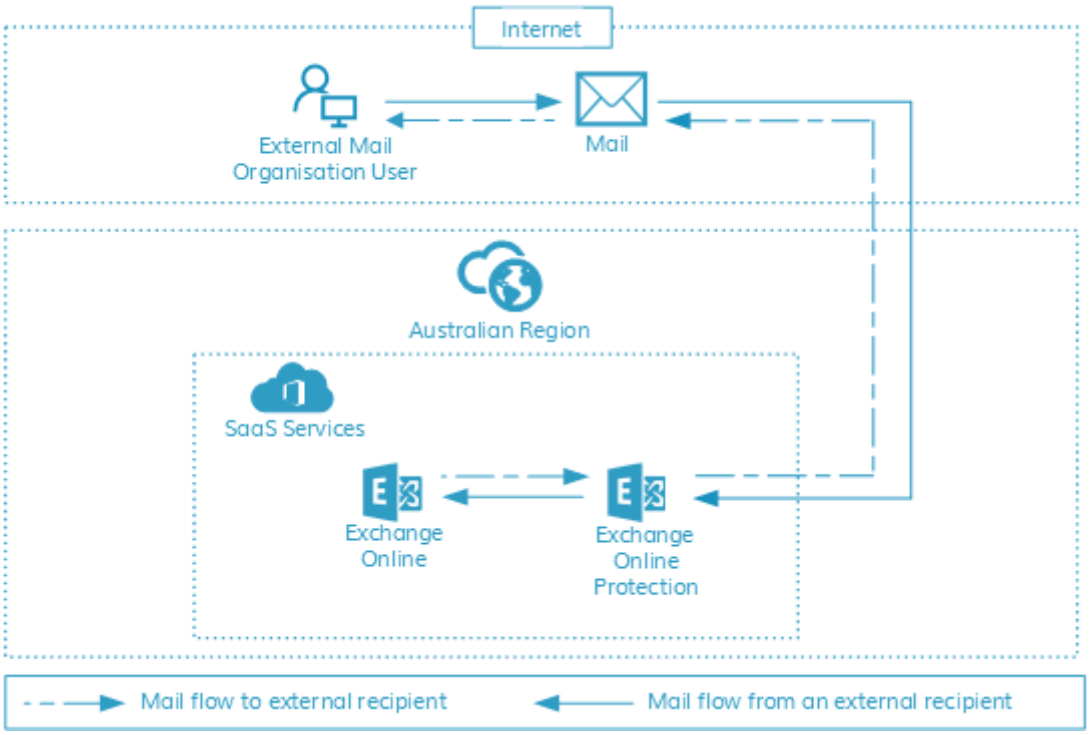
DTA is currently working with Microsoft and the Department of Finance to simplify an agency's ability to achieve this, however at the time of writing there is no native solution to allow a direct interface between the Office365/Exchange Online environment and the GovLink solution.

[8] https://www.finance.gov.au/government/whole-government-information-communications-technology-services/govlink

DTA is able to provide further advice to agencies and reference sites of how other Commonwealth entities have achieved this functionality. Future iterations of this Blueprint will provide more detail on the subject.

Figure 2 shows the mail flow for an organisation that is assessed at below PROTECTED where there is no requirement for a GovLink connection.

Figure 2 Mail Flow for an UNCLASS system



Design Decisions

Table 13 describes the UNCLASS Mail Flow design decisions.

Table 13 UNCLASS Mail Flow Design Decisions

Decision Point	Design Decision	Justification
Agency is running at less than PROTECTED level	Mail gateway is not required, agency can use Exchange online only	Reduced complexity and cost
Mail ingress location	Exchange Online	An on-premises mail gateway does not need to be used, all mail is delivered by Exchange Online

Mail egress location	Exchange Online	An on-premises mail gateway does not need to be used, all mail is delivered by Exchange Online
Mail Connectors	Not configured	Mail connectors are not required for cloud-native (non-hybrid) deployments

Table 14 describes the PROTECTED Mail Flow design decisions.

Table 14 PROTECTED Mail Flow Decisions

Decision Point	Design Decision	Justification
Agency running at PROTECTED level	Mail gateway with connection to GovLink is required	Mandatory
Mail ingress location	GovLink mail gateway	A mail gateway is required.
Mail egress location	GovLink mail gateway	A mail gateway is required.
Centralised Mail Transport	Not Configured	A centralised mail transport is not required in a cloud-native (non-hybrid) deployment
Connector Configuration	Refer to Table 16	Connector configuration will be required between Exchange Online and a mail gateway

Mail Connectors

Description

Mail connectors use TLS to secure communication and can customise the way mail flows into and out of the organisation.

Design Considerations

Mail connectors are required when the organisation is assessed at the PROTECTED level.

It is common for the path to vary per scenario, with the scenarios being:

- Mail inbound from an external mail organisation to a cloud mailbox; and
- Mail outbound from a cloud mailbox to an external mail organisation.

Within the above scenarios, the key decisions that need to be made are:

- Where will the mail be entering from the internet?
- Where will the mail be leaving to go to another mail organisation?

These decisions are generally made based on one or more of the following factors:

- Where are the majority of mailboxes located?
- Is Office 365 Exchange Online Protection to be used for all mail protection within the organisation?
- Are there compliance reasons preventing the use of Exchange Online Protection?

Design Decisions

Table 15 describes the Mail Connector design decisions.

Table 15 Mail Connector Design Decisions

Decision Point	Design Decision	Justification
Mail Connectors	Configured	Mail connectors are required when the organisation is assessed at PROTECTED.

Table 16 describes the Mail Connector configuration when assessed at PROTECTED.

Table 16 Mail Connector Configuration

Configuration	Value	Description
Certificate details	Configured	Certificate to be issued from the GovLink connection agencies gateway.
Virtual IP address (VIP)	Configured	Virtual IP Address details will be provided by the gateway provider.
Exchange Online Receive Connector		
Name	Inbound-connector-from-<GATEWAY>	Describes the source and directionality of mail.
Retain internal mail headers	Unchecked	Internal Mail headers are stripped off messages.

On-premise server identification method and value	Identify by Senders Domain. Reject email messages if they aren't sent over TLS. Require subject name matching <DOMAIN>	Ensures mail is being sent over an encrypted connection to a known domain.
Exchange Online Send Connector		
Name	outbound-connector-to-<GATEWAY>	Describes the source and directionality of mail.
Retain internal mail headers	Checked	When reporting spam that slips past the filters, it is essential that we receive the full message headers from a message
When to use the connector	* (All Mail)	All mail should use the connector
Message routing	Route through these smart hosts.	This should be used route mail to the gateway.
Connector Authentication settings	Always use TLS issued by a trusted Certificate Authority with a SAN matching <DOMAIN>	Ensures mail is being sent over an encrypted connection to a known domain.

Mail Exchange Records

Description

Mail Exchange (MX) records specify the mail server responsible for accepting mail on behalf of the domain.

Design Considerations

The record is a resource in the Domain Name System (DNS) and it is possible for a single domain to have multiple MX records. Multiple records are largely done for availability, redundancy, and load balancing reasons.

Design Decisions

Table 17 describes the Mail Exchange Records design decisions.

Table 17 Mail Exchange Records Design Decisions

Decision Point	Design Decision	Justification
Authoritative DNS MX Record	Mail Gateway	This is the ingress point for the mail for the agency, their mx records will point to the agency gateway that they are consuming their GovLink services
Mail Exchanger/s	Mail Gateway	This is the ingress point for the mail for the agency, their mx records will point to the agency gateway that they are consuming their GovLink services

Autodiscover

Description

Autodiscover is a mechanism for the configuration of a user's email client with minimal user input. The required input from the user is their email address and password.

Design Considerations

Autodiscover for a cloud environment varies from the process utilised when on-premises Exchange is leveraged. With a cloud environment, an Autodiscover Endpoint representing the domain is not available. Instead, DNS redirection and Hypertext Transfer Protocol Secure (HTTPS) redirection is leveraged to direct the Autodiscover client to a trusted Autodiscover Endpoint. The high-level process is:

- The Autodiscover endpoint looks for a host named autodiscover.<DomainName>.com
- DNS provides the Internet Protocol (IP) address of the host autodiscover.outlook.com
- The Autodiscover client attempts communication utilising HTTPS (This fails)
- The Autodiscover client requests redirection over Hypertext Transfer Protocol (HTTP) (This directs the client to autodiscover-s.outlook.com)
- The Autodiscover client attempts communication utilising HTTPS. The communication is successful. However, the new Autodiscover endpoint does not have a server certificate for the

requested hostname. This communication is then redirected using HTTPS redirection to an additional Autodiscover endpoint which can provide the required Autodiscover information.

- The Autodiscover client completes the Autodiscover process with the new Autodiscover endpoint.

To ensure this process functions as described above, appropriate DNS records are required.

Design Decisions

Table 18 describes the Autodiscover design decisions.

Table 18 Autodiscover Design Decisions

Decision Point	Design Decision	Justification
Autodiscover	CNAME autodiscover autodiscover.outlook.com	Autodiscover will improve the user experience and is required to configure a user's Outlook profile and inbox.

Table 19 describes the Autodiscover configuration.

Table 19 Autodiscover Configuration

Configuration	Value	Description
DNS Records (CNAME)	e.g., Autodiscover: autodiscover.outlook.com	A DNS record that points clients to the Autodiscover service.

SPF, DMARC, DKIM

Description

Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) are tools for email authentication.

Design Considerations

These tools can coexist to provide enhanced capabilities.

- **SPF** - SPF is a DNS entry which lists the servers which are allowed to send emails from a specific domain. It allows recipients to verify the identity of incoming mail

- **DKIM** - DKIM, unlike SPF is a tool to verify whether the content of the message is trustworthy. This is completed using a public/private key signing process
- **DMARC** - DMARC enables both SPF and DKIM using policy. A DMARC policy sets out how to handle messages which do not align to what the receiver knows about the sender. This can include rejecting the message; suggesting the message is quarantined; or allowing the message

Design Decisions

Table 20 describes the SPF, DKIM, and DMARC design decisions.

Table 20 SPF, DKIM, & DMARC Design Decisions

Decision Point	Design Decision	Justification
SPF	Configured	Configuration of SPF record(s) are required as a baseline for the deployment.
DKIM	Configured	DKIM is a public/private key signing process used to verify the content of an email. DKIM signing is enabled on emails originating from an organisation's domains.
DMARC	Configured	One DMARC policy is to be configured per Agency domain. This is to be configured at the gateway that the agency consumes. DMARC records are configured for all domains such that emails are rejected if they fail SPF or DKIM checks.

Accepted Domains

Description

Accepted Domains are SMTP namespaces configured within Exchange Online in order to receive emails addressed to users within the accepted domain.

Design Considerations

Accepted Domains consist of the following types:

- **Authoritative Domains** - Authoritative Domains are domains where the Exchange Organisation accepts messages addressed to recipients and is responsible for generating non-delivery reports. On creation of an Exchange Online organisation the tenant domain Fully Qualified Domain Name (FQDN) and the <tenantname>.onmail.onmicrosoft.com FQDN are automatically populated as an Authoritative Domains; and
- **Relay Domains** - Relay Domains are often called Non-Authoritative Domains. The Exchange Organisation will accept the messages addressed to the recipients; however it is not responsible for generating non-delivery reports. Hybrid Exchange leverages Relay Domains and mail connectors to relay messages between both on-premises infrastructure and Exchange Online.

Design Decisions

Table 21 describes the Accepted Domains design decisions.

Table 21 Accepted Domains Design Decisions

Decision Point	Design Decision	Justification
Configure Additional Accepted Domains	Configured	Any additional Agencies that require access to the system are to be included.
Authoritative Domains	Configured	The <agency-tenant>. onmicrosoft.com authoritative domain is created during the enablement of Office 365 and represents the Exchange Online Organisations SMTP address space. The additional authoritative domains are required as each agency will have a corresponding authoritative domain.
Relay Domains	Not configured	This setting is only required to be configured in a Hybrid Exchange scenario.

Remote Domains

Description

Remote Domains allow administrators to control the type of replies and format of messages users send to the destination domain.

Design Considerations

Administrators have the ability to configure Exchange to allow (or block) the following:

- Out of Office messages
- Automatic replies and forwards
- Read or delivery receipts
- Non-delivery report to a specified domain

The default remote domain will apply the same settings to all messages, however administrators can configure specific settings for specific domains.

Design Decisions

Table 22 describes the Remote Domain design decisions.

Table 22 Remote Domains Design Decisions

Decision Point	Design Decision	Justification
Configure Remote Domains	Default configuration applied	The default configuration within Exchange Online will be leveraged.

Table 23 describes the Remote Domain configuration.

Table 23 Remote Domain Configuration

Policy Setting	Configuration	Description
*Name: **		

Domain Name	* Note - * means all external agencies	Name of the remote domain.
Out of Office Automatic Replies	Allow Only External Out of Office replies - Selected	Allows the limiting of the type of client automatic replies.
Automatic Replies	Allow Automatic Replies – Unchecked Allow automatic forwarding - Unchecked	Allows the limiting of automatic replies and automatic forwards.
Message Reporting	Allow Delivery Reports - Ticked Allow Non-delivery Reports – Ticked Allow Meeting Forward Notifications - Unchecked	Allows the limiting of delivery reports, no-delivery reports, and meeting forward notifications.
Use rich text format	Follow User Settings - Selected	Allows the control over message format.
Supported Character Set	None	Allows the control over the character set.

Exchange Online

Description

Microsoft Exchange Online is a cloud-hosted messaging solution that has the capabilities of on-premises Exchange services. Exchange Online gives users access to email, calendar, contacts, and tasks from various devices.

Design Considerations

Exchange Online supports mailbox delegation, where a delegate can have send-on-behalf and management rights over other mailboxes. Shared mailboxes can be assigned to and administered by many users. Application mail sending is supported where the application can authenticate against the Exchange Online system (Simple Mail Transport Protocol (SMTP) message submission to users inside the managed environment or authenticated SMTP message relay to addresses outside the managed environment).

Exchange Online requires a new or existing Azure AD Tenant with appropriate licencing configured. Different licencing levels provide different features and functionality. An Azure AD tenant provides identity which can be fully cloud based or synchronised from an on-premises AD domain.

The implementation of Exchange Online can be coupled with a migration from the existing on-premises Exchange infrastructure. This migration can take the form of one of the following:

- **Hybrid Migration –** Often referred to as a staged migration, is where the on-premises Exchange environment is extended to Office 365 through organisational relationships or federation. During migration user mailboxes will be spread between the online and on-premises environments, this necessitates planning to ensure free/busy, calendar and mailbox sharing all continue to work.;
- **Cutover Migration –** A cutover migration is only recommended for organisations with less than 150 mailboxes and occurs over one or a few days. During this period email access may be unavailable. Prior to the migration event, a connection between the on-premises Exchange Organisation and Exchange Online needs to be established; and
- **PST Migration –** A PST migration is where PST files with a mapping file are either shipped to or uploaded into Office 365. The Exchange Online instance is a greenfield deployment with no configuration required on the on-premises Exchange Organisation.

Design Decisions

Table 24 describes the Exchange Online design decisions.

Table 24 Exchange Online Design Decisions

Decision Point	Design Decision	Justification
Deployment Type	Exchange Online only	The blueprint is designed for agencies that do not have any on-premise equipment.
Office 365 Tenant	Single tenant	Exchange Online services will be hosted within the Agency's secure Office 365 tenant.
User Identity Source	Azure Active Directory	Azure Active Directory will be utilised. No directory synchronisation is required.

User Mailbox Configuration

Description

Remote Domains allow administrators to control the type and format of messages users send to external domains.

Design Considerations

Administrators can configure Exchange to allow (or block):

- Out of Office messages
- Automatic replies and forwards
- Read or delivery receipts
- non-delivery report to a specified domain

Configurations set on the remote domain will override any Exchange Online user implemented settings.

Design Decisions

User Mailboxes are Exchange Mailboxes that are associated with a user account. Usually one mailbox is associated to one user account. These mailboxes can be configured to:

- Allow or disallow Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) connections to them
- Prevent mail from deletion
- Control ActiveSync connections to them
- Control mail size limits
- Control the use of mail archives

The above configuration can be completed on all new mailboxes through the use of a Client Access Services (CAS) Mailbox Plan. A CAS Mailbox Plan is used to configure settings when a licence is assigned to a new user. If the licence is changed, the CAS Mailbox plan linked to that new licence is applied.

Table 25 describes the User Mailbox design decisions.

Table 25 User Mailbox Design Decisions

Decision Point	Design Decision	Justification
Disable IMAP	Configured	IMAP will be disabled to meet Microsoft best practice security advice.
Disable POP	Configured	POP will be disabled to meet Microsoft best practice security advice.
Enable Litigation hold	Configured	Litigation hold will be enabled to meet Microsoft best practice security advice.
Exchange Mailbox Size	100GB per user	Included with Office 365 E3 / E5 licencing.
Language	English	The default language is English, users will have the ability to adjust this if required.
Default time zone	GMT +10	The default time zone is GMT +10 however this can be adjusted based on user location.
Exchange Message Size Limits	Up to 90MB	This is more than sufficient for a user to receive.

Custom Primary SMTP Addressing	firstname.lastname@agency.gov.au	Usernames are to be suffixed with numbers if another user of that name exists (firstname.lastname1@agency.gov.au).

Authentication Policies

Description

Authentication policies control the authentication methods which can be used to access Exchange Mailboxes.

Design Considerations

Authentication polices can be leveraged to protect the organisation from brute force and spray attacks. To protect against this, Basic Authentication can be blocked. Basic authentication is where a username and a password are leveraged for client access requests.

Blocking Basic Authentication forces clients to use Modern Authentication. Blocking Basic Authentication can cause issues when clients within the environment do not support Modern Authentication. If this occurs, it is recommended to investigate whether the client can be upgraded to support Modern Authentication. If it can, then it is recommended that the client be upgraded. If it cannot then a separate authentication policy can be leveraged enabling Basic Authentication for that client only.

Design Decisions

Table 26 describes the Authentication Policy design decisions.

Table 26 Authentication Policy Design Decisions

Decision Point	Design Decision	Justification
Basic Authentication	Disabled	Basic Authentication has known exploits, recommend Modern Authentication.
Authentication Policy Configuration	Configured as per details in the DTA-Office 365 – ABAC document.	

Outlook on the Web Policies

Description

Outlook on the Web (OWA) Policies, are used to control the availability of features and settings in Outlook on the Web.

Design Considerations

A mailbox can only be assigned one OWA Policy and every mailbox must have a policy assigned.

Features and settings which can be controlled by an OWA policy include:

- Third party file provider integration
- Office 365 group creation
- Microsoft Satisfaction survey prompts

Design Decisions

Table 27 describes the Outlook on the Web Policy design decisions.

Table 27 Outlook on the Web Policy Design Decisions

Decision Point	Design Decision	Justification
Third party file provider integration	Disabled	Only Microsoft file providers are approved for integration, no third-party file providers will be configured.
Office 365 group creation by users	Disabled	Groups can only be created by administrators, not users. This will ensure that the GAL is the most up to date and that there is a consistent naming convention utilised.

Mailbox Archive

Description

Office 365 Mailbox Archives provide an unlimited email storage space for users. A mailbox archive is an additional mailbox storage space.

Design Considerations

This archive can be accessed through the web portal or the Outlook client. Users can move or copy mail between their primary and archive mailboxes. Administrators can enable archive and deletion policies. These policies automatically move mail to the archive and, if required, delete mail from the archive when the set criteria are met. Mailbox archives are also subject to retention policies.

Design Decisions

Table 28 describes the Mailbox Archive design decisions.

Table 28 Mailbox Archive Design Decision

Decision Point	Design Decision	Justification
Mailbox Archive	Enabled	The archive mailbox is required to control primary mailbox cache sizes.
Mailbox Archive Policy	Enabled	The use of automated archive mailbox policies improves the user experience and ensures that primary mailbox sizes are controlled.
Archive configuration	Configured as per details in the DTA-Office 365 – ABAC document.	

Mailbox Auditing

Description

Mailbox Auditing provides visibility into the access and modification of user mailboxes by owners, delegates, and administrators.

Design Considerations

Once enabled on a user's mailbox, the activities subject to audit appear within the Office 365 audit log. This information is then available for Security review and analysis. The audit log can and should be exported to a SIEM.

Design Decisions

Table 29 describes the Mailbox Auditing design decisions.

Table 29 Mailbox Auditing Design Decisions

Decision Point	Design Decision	Justification
Mailbox Auditing	Configured	An event log auditing process, and supporting event log auditing procedures, is developed and implemented covering the scope and schedule of audits, what constitutes a violation of security policy, and actions to be taken when violations are detected, including reporting requirements.
Centralised Logging Facility	Not Configured	A Centralised Logging Facility will not be configured but Office ATP and Defender ATP to be implemented with email alerts sent to Global Administrators.

Table 30 describes the Mailbox Auditing design decisions.

Table 30 Audit Configuration

Configuration	Value	Description
User Mailbox and Shared Mailbox Audit Configuration		

Admin Audited Actions	ApplyRecord Copy Create FolderBind HardDelete MessageBind Move MoveToDeletedItems RecordDelete SendAs SendOnBehalf SoftDelete Update UpdateCalendarDelegation UpdateFolderPermissions UpdateInboxRules	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.
Delegate Audited Actions	ApplyRecord Create FolderBind HardDelete Move MoveToDeletedItems RecordDelete SendAs SendOnBehalf SoftDelete Update UpdateFolderPermissions UpdateInboxRules	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.
Owner Audited Actions	ApplyRecord Create HardDelete MailboxLogin Move MoveToDeletedItems RecordDelete SoftDelete Update UpdateCalendarDelegation UpdateFolderPermissions UpdateInboxRules	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.
Office 365 Group Mailbox Audit Configuration		

Admin Audited Actions	Create HardDelete MoveToDeletedItems SendAs SendOnBehalf SoftDelete Update	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.
Delegate Audited Actions	Create HardDelete MoveToDeletedItems SendAs SendOnBehalf SoftDelete Update	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.
Owner Audited Actions	HardDelete MoveToDeletedItems SoftDelete Update	All available audit actions will be selected in order to provide the required visibility of changes made to a mailbox.

Journaling

Description

Journaling within Exchange is the recording of email communications as port of an organisation's retention strategy.

Design Considerations

Journaling can assist with achieving compliance with particular regulations. A Journal rule can be scoped to:

- Internal messages only
- External messages only
- All messages
- Specific recipients

Office 365 supports the use of Journaling with the caveat that an Exchange Online mailbox cannot be used as a journaling mailbox. Journal reports can be delivered to a separate system.

Within Office 365, additional options are available to be leveraged in an organisation's retention strategy. These include:

- Retention Policies
- Litigation hold

The benefit of these options is it reduces the complexity and management overhead involved with recording email communications in a separate system and backing up these separate systems. Retention Policies can also be leveraged across the Office 365 organisation. This provides additional coverage.

Design Decisions

Table 31 describes the Journaling design decisions.

Table 31 Journaling Design Decisions

Decision Point	Value	Description
Configure Journaling	Not Configured	Litigation hold, and Retention policies will be leveraged to replace the functionality provided by journaling.

Shared Mailboxes

Description

A Shared Mailbox is a mailbox which allows one or more users read and send messages. Shared Mailboxes also allow the sharing of a calendar between multiple people.

Design Considerations

Within Office 365 shared mailboxes do not require a licence to be assigned to them unless the mailbox has over 50GBs of data.

Unlike user mailboxes, within AD, these mailboxes are represented by a disabled user account. These accounts can be enabled however this poses a security risk as the mailbox account is not related to a single user.

User access to the mailbox is provided using mailbox delegation rights (Full Access, Send As, Send on Behalf). These rights can be assigned either directly or using a mail enabled security group.

Design Decisions

Table 32 describes the Shared Mailbox design decisions.

Table 32 Shared Mailbox Design Decisions

Decision Point	Design Decision	Justification
Shared mailbox delegation (Full Access, Send As, Send on Behalf)	Configured via Mail enabled Security groups	Mail enabled security groups limit the management overhead associated with mailbox delegation when compared to direct delegations. A security group is required to be mail enabled to appear within Office 365.

Resource Mailboxes

Description

A Resource Mailbox is a mailbox which is assigned to a resource as opposed to a user.

Design Considerations

Resource Mailboxes have two types:

- **Room mailboxes** – Used for meeting rooms
- **Equipment mailboxes** – Used for non-location specific resources such as computers, projectors, microphones, or cars

Users book these resources using meeting requests. Resource Mailboxes can be configured to accept or decline the request based on their availability.

Room Mailboxes can be sorted into lists using Room Lists. Room Lists are leveraged to simplify the booking process by grouping all rooms that meet a certain requirement together (Room lists are usually configured by location). When a user books a meeting, they can select the appropriate room list and then see the available rooms for that time.

Design Decisions

Table 33 describes the Resource Mailboxes design decisions.

Table 33 Resource Mailbox Design Decisions

Decision Point	Design Decision	Justification
Room Mailboxes	Configured	There is a requirement for booking rooms within the solution. Rooms will be configured with a mailbox so that users can book them through their calendars.
Equipment Mailboxes	Configured	There is a requirement for booking equipment within the solution. Equipment will be configured with a mailbox so that users can book them through their calendars.
Room Lists	Configured	There is a requirement for booking rooms within the solution. Room Assets will be configured with a list so that users can book them through their calendars.

Distribution Lists

Description

Distribution lists are groups which when sent an email actually send an email to all members of the list.

Design Considerations

This saves the sender from needing to enter each individual email address when emailing a group. These groups/lists are generally leveraged for emailing an entire team or project. Only internal agency employees can send emails to the “agency-all” distribution list.

Distribution lists are created in different ways depending on the Exchange architecture:

- **Cloud Deployments** - For cloud only deployments, distribution lists are created within Office 365
- **Hybrid Deployments -** For hybrid deployments, distribution lists can be created both within Office 365 and on-premises. upon-premises lists are then synchronised to Office 365. The on-premises method has the benefit of living with the user identity source of truth however it does create complexity when it is not managed in the same location as Exchange

Management of Distribution lists can be streamlined through the enforcement of a Naming Policy. A Distribution list Naming Policy allows the enforcement of a consistent naming strategy across Office 365 Groups. It consists of two parts:

- **Prefix-Suffix Naming Policy** – Setting of prefixes or suffixes for groups names. The prefixes/suffixes can be either fixed strings or user attributes
- **Custom Blocked Words** – Blocking of words in the name based on a custom list

Design Decisions

Table 34 describes the Distribution Lists/Groups design decisions.

Table 34 Distribution Lists/Groups Design Decisions

Decision Point	Design Decision	Justification
Distribution Groups creation	Cloud Created	Management activities for Exchange Online will occur within the portal. The use of cloud created distribution groups also allows for the groups to be upgraded to Office 365 groups at a later stage.
Distribution Naming Policy	Configured The naming convention will be AgencyName-PolicyName	Naming policies streamline the management of Distribution lists and allow for groups to be easily sorted.

Dynamic Security Groups

Description

Dynamic Security groups are Azure AD security groups that are populated based on device and/or user attributes.

Design Considerations

These groups can be leveraged to control access to locations, services, and features.

The membership of a Dynamic Security group is updated whenever an attribute of a device or user is modified. If the user/device no longer matches the group rule, then that user/device is removed. Conversely if a user/device now matches the group rule they are added. When a user is added the group can be configured so that the added user receives an email notifying them of the addition.

Naming of Dynamic Security groups can be streamlined through the use of a Naming policy. The Naming policy ensures that the groups within the environment conform to a standard and their purpose can be easily identified.

Design Decisions

Table 35 describes the Dynamic Security Group design decisions.

Table 35 Dynamic Security Group Design Decisions

Decision Point	Design Decision	Justification
Naming Policy	grp-AgencyName-SecurityGroup-Role	This is in line with other blueprint naming conventions across the solution.
Welcome Email	Disabled	The welcome email will be disabled to reduce the amount of generic correspondence being sent to users.

Office 365 Groups

Description

Office 365 Groups are an extension on the traditional mail Distribution Lists, Mail-enabled Security groups and Shared Mailboxes.

Design Considerations

Office 365 Groups allow members to collaborate with a group email, shared a workspace for conversations, files, calendar events, and a Planner. Unlike Shared Mailboxes, Office 365 groups can be accessed via mobile applications. Office 365 groups are also integrated with Microsoft Teams and are created when a Team is created.

Membership of an Office 365 Group can be dynamically updated using user attributes available in Azure AD. This removes some of the management overhead involved with managing the traditional group structures.

Management of Office 365 Groups can be streamlined through the enforcement of a Naming Policy, Office 365 group expiry, and creation restrictions. An Office 365 Group Naming Policy allows the enforcement of a consistent naming strategy across Office 365 Groups. It consists of two parts:

- **Prefix-Suffix Naming Policy** – Setting of prefixes or suffixes for groups names. The prefixes/suffixes can be either fixed strings or user attributes; and
- **Custom Blocked Words** – Blocking of words in the name based on a custom list.

In conjunction with the Naming Policy, Office 365 groups can also be given expiration dates. This assists with unused group clean-up activities. The expiration period commences on group creation and can be renewed at the end of the period (The owner or contact for groups with no owners has 30 days to renew the group). When a group expires, it is soft deleted for 30 days. Retention policies will however hold the data for the period of the retention policy. An expiration policy can be applied globally to all groups or to specific groups.

Office 365 Groups, by default can be created by any user. This can be restricted to Administrators and members of a security group. This restriction prevents the needless creation of groups. It is advisable to develop a workflow to control the provisioning process.

Design Decisions

Table 36 describes the Office 365 Group design decisions.

Table 36 Office 365 Group Design Decisions

Decision Point	Design Decision	Justification
Office 365 Group creation restrictions	Configured Only administrators can create/configure Office 365 groups.	This will ensure that groups are approved before being created, ensuring all groups have a purpose. This setting also affects Exchange, SharePoint and Teams.
Naming Policy	grp-AgencyName-SecurityGroup-Role	Exchange groups will be named like the following AgencyName-Department e.g. grp-DTA-ExchangeMailbox-ITHelpdesk
Group Expiration	All groups - annually	Group Expiration is required to simplify the management overhead associated with groups and to limit Azure AD clutter.

Address Book / Address List

Description

The Outlook Address Lists, Global Address List (GAL), and Offline Address Book (OAB) are collections of mail-enabled objects.

Design Considerations

They are leveraged for recipient lookup operations (i.e. When a user leverages either the Address book or Check names tools in Outlook). The types of mail-enabled object collections are as follows:

- **GAL** – The GAL is automatically created by Exchange and lists all mail-enabled objects. (The GAL is available by default to all users)
- **OAB** – The OAB is an offline version of the GAL leveraged by clients in Cached Mode
- **Outlook Address List** - An Outlook Address List is a subset of the mail-enabled objects. By default, a number of Address Lists are created, however, additional Address Lists can be created as required

Design Decisions

Table 37 describes the Address Lists design decisions.

Table 37 Address Book / Address List Design Decisions

Decision Point	Design Decision	Justification
Custom Address Lists	Configured – one per agency	Custom address lists can be configured by agency administrators. One will be created as AgencyName-All
GAL and OAB	Generated	These will be generated so that users can send emails within the organisation in accordance with Microsoft best practice.

Exchange Online Protection

Connection Filtering

Description

Connection filtering within Exchange Online Protection refers to the verification of the sender using SPF, DKIM, DMARC and Microsoft intelligence.

Design Considerations

Exchange Online Protection Connection Filtering is always enabled however it can, to a degree, be configured. A connection filter can be implemented to always allow or always block traffic based upon an IP list.

Design Decisions

Table 38 describes the Connection Filter design decisions.

Table 38 Connection Filters Design Decisions

Decision Point	Design Decision	Justification
Configure Connection Filter	Configured	Agencies are to provide IP addresses considered as safe.

Table 39 describes the Connection Filter configuration.

Table 39 Connection Filter Configuration

Configuration	Value	Description
Connection filter policy name	Default	This policy is the default policy configured when Exchange Online is enabled and is consistent with best practice.
Scoped to	All Domains	This is the default setting configured when Exchange Online is enabled.

IP Allow list	Not Configured	This is the default setting configured when Exchange Online is enabled.
IP Block list	Not Configured	This is the default setting configured when Exchange Online is enabled.
Safe list	Disabled	This is the default setting configured when Exchange Online is enabled.

Anti-malware

Description

Anti-malware within Exchange Online Protection refers to the default anti-malware scanning which is completed on all emails routing through the service.

Design Considerations

In addition to the default scanning, anti-malware policies can be configured. These polices allow for the customisation of a response if malware is detected and the restriction of attachment file types.

Design Decisions

Table 40 describes the Anti-malware design decisions.

Table 40 Anti-malware Design Decisions

Decision Point	Design Decision	Justification
Configure Anti-malware Policy	Configured	Configuring the anti-malware policy to allow for the customisation of a response if malware is detected and the restriction of attachment file types.

Table 41 describes the Anti-malware Policy configuration.

Table 41 Anti-malware Policy Configuration

Configuration	Value	Description
Anti-malware policy name	Default	Editing the default policy ensures it applies to all incoming and outgoing mail and is consistent with best practice.
Malware detection response	Notify recipients that the message has been quarantined with the default notification text	This will send a notification to recipients when a message is quarantined.
Sender notifications	Notify internal senders	This will send notification to senders when their message is quarantined.
Administrator notifications	Notify administrators about undelivered messages from internal senders Notify administrators about undelivered messages from external senders	Administrators will be notified when messages are undelivered.
Allowed File type filtering	Disabled	This is the default setting configured when Exchange Online is enabled and is Microsoft best practice. This ensures that all file types are inspected for malware with no exceptions.

Policy Filtering

Description

Policy filtering within Office 365 Exchange Online Protection refers to the enforcement of Transport Rules.

Design Considerations

Transport Rules are a set of rules enforced on mail transiting through the Exchange Organisation. Transport rules can be leveraged by Administrators to complete a number of items on all mail or a subsection of the mail transiting through the Exchange Organisation. These items include:

- Block mail with certain headers

- Apply disclaimers to emails
- Apply Office 365 message encryption

Transport Rules follow the following basic structure:

- **Conditions** – Conditions identify which mail the transport rule applies to. These conditions largely target either information gained from message headers (e.g. the 'to', 'from' or 'CC' fields) or message properties (e.g., size, attachments, subject, body, message classification). A single rule can have multiple conditions apply
- **Exceptions** – Exceptions are an optional component of a Transport Rule and define the mail exempt from the rule
- **Actions** – Actions are used to define what actions to undertake on the messages matching the conditions and which do not match any exemption. These actions include rejecting, deleting, redirecting the emails, and adding recipients, prefixes, and disclaimers. A single rule can have multiple actions applied however some actions are incompatible with others
- **Properties** – Properties are used to define anything which do not fall into another category. This includes enforcing or testing the rule

Design Decisions

Table 42 describes the Exchange Online Policy Filtering design decisions.

Table 42 Exchange Online Policy Filtering Design Decisions

Decision Point	Design Decision	Justification
Transport Rules	Configured	Transport rules within the environment are required to enforce business rules and process.

Table 43 describes the Transport Rules Configuration.

Table 43 Transport Rules Configuration

Configuration	Value	Description
Apply this rule if	The recipient is located outside the organisation	Conditions used to identify the mail subject to the rule.
Do the following	Append the disclaimer and fall back to reject if the disclaimer can't be inserted.	The action to take on the identified mail.
Except if	N/A	Identified mail which should not be subject to the rule.

Choose a mode for this rule	Enforce	The mode which the rule applies. The options are Enforce; Test; Test with Policy tips.
Stop processing more rules	Disabled	Stop processing more rules stops additional rules from being processed on the identified mail.
Defer the message if rule processing does not complete	Enabled	Defer the message if rule processing does not complete prevents the mail from progressing until the rule is completed.
Match sender address in message	Header	Specifies where to look within the message for the sender's address.
Comments	This rule inserts a disclaimer for all traffic leaving the organisation. *e.g., the content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.*	Comments that appear in the portal when the rule is reviewed.

Content Filtering

Description

Content Filtering within Exchange Online Protection refers to SPAM management and SPAM policy.

Design Considerations

Content Filtering polices allow for:

- The customisation of response on SPAM detection
- Marking emails as SPAM based on language detected
- Marking emails as SPAM based on the sender or sender's domain

- Increasing the SPAM score if certain content is present in the email
- Marking emails as SPAM if certain content is present in the email

The use of these policies allows greater management control over SPAM emails.

Design Decisions

Table 44 describes the Content Filtering design decisions.

Table 44 Content Filtering Design Decisions

Decision Point	Design Decision	Justification
Configure SPAM policy	Default configuration	Exchange Online Protection will complete SPAM evaluation.

Table 45 describes the Content Filtering configuration.

Table 45 Content Filtering Configuration

Configuration	Value	Description
SPAM policy name	Default	Editing the default policy ensures it applies to all incoming and outgoing mail and is consistent with best practice.
Enabled/Disabled	Enabled	This policy is the default within Exchange Online and is consistent with best practice.
Detection response for spam	Move message to Junk Email folder	This policy is the default within Exchange Online and is consistent with best practice.
Detection response for high confidence spam:	Move message to Junk Email folder	This policy is the default within Exchange Online and is consistent with best practice.
Mark bulk email as spam:	Enabled	This policy is the default within Exchange Online and is consistent with best practice.
Threshold:	7 (Default)	This policy is the default within Exchange Online and is consistent with best practice.
Sender block list:	Not configured	This policy is the default within Exchange Online and is consistent with best practice.

Domain block list:	Not configured	This policy is the default within Exchange Online and is consistent with best practice.
Sender allow list:	Not configured	This policy is the default within Exchange Online and is consistent with best practice.
Domain allow list:	Not configured	This policy is the default within Exchange Online and is consistent with best practice.
International spam – languages:	Disabled	This policy is the default within Exchange Online and is consistent with best practice.
International spam – regions:	Disabled	This policy is the default within Exchange Online and is consistent with best practice.
End-user spam notifications:	Disabled	This policy is the default within Exchange Online and is consistent with best practice. Administrators will be responsible for SPAM administration and notifications will be hidden from users.

SharePoint Online

SharePoint Online is a document management and collaboration platform within Office 365. The sharing of documents can be controlled to allow or disallow sharing with external parties.

SharePoint Sites

Description

SharePoint Online provides the ability to create Intranet sites and Team Sites for groups or agencies to collaborate and manage their documents.

Design Considerations

The creation and storage sizing of SharePoint online sites can be controlled. Out of the box, users can create SharePoint sites and these sites have no storage limits applied. Without restriction there is potentially a large management overhead.

Design Decisions

Table 46 describes the SharePoint Sites design decisions.

Table 46 SharePoint Sites Design Decisions

Decision Point	Design Decision	Justification
SharePoint site naming convention	Avoid spaces and special characters in site collection naming	Spaces and special characters can cause problems with indexing and extend the length of the path. Short names are easier to remember
Configure Site Storage limits	Configured	Larger storage can increase management. This can be manually set by SharePoint Administrator. Suggest 200GB
Block access from unmanaged devices	Configured	Allow limited web only access. Default settings.
Enable Idle Session sign outs	Sign out users after 1 hr Give users this much notice before signing out: 5 minutes	Default settings
Only allow access from specific IP address locations	Not configured	Access to be controlled via Conditional Access policies.

Only allow access from apps that use modern authentication	Enabled	Default settings

Application Management

Description

Application management enables the organisation to control custom add-ins and webparts, purchased 3rd party applications and the associated licences.

Design Considerations

SharePoint default methods of displaying and sharing of sharing data are available. Third party applications may circumvent controls or auditing and provide other methods of displaying or sharing of SharePoint data. Any third-party applications will need to be validated for compliance.

Design Decisions

Table 47 describes the Application Management design decisions.

Table 47 Application Management Design Decisions

Decision Points	Design Decision	Justification
App Purchase Should end users be able to get apps from marketplace?	No	Only administrators are approved to assign or purchase application.
Apps for Office from the Store Should Apps for Office from the store be able to start when documents are opened in the browser?	No	This setting increases the security of the solution by ensuring documents in the browser cannot start third party apps for Office

Web Parts

Description

SharePoint Online provides spaces for users to customise their SharePoint page to include web parts into the page. Web Parts are additional functional parts that can be added into SharePoint Pages to enhance productivity and usability for the site.

Design Considerations

Web Parts are client-side applications that can be added into SharePoint Online. The document considers these two out of the box sets of webparts that needs to be considered as a part of the design decisions:

- Microsoft published webpart
- Third party published webpart

Design Decisions

Table 48 describes the Webpart design decisions.

Table 48: Webparts Design Decisions

Decision Points	Decision	Justification
Microsoft published webpart	Enabled	Microsoft published webparts cannot be disabled in SharePoint.
Third Party published webpart	Disabled	Third party web parts will be disabled due to potential unsecure data flow outside of Office 365. If a third party published webpart is identified for use in future, the organisation will undertake a risk assessment before implementation.

Sharing and Access Controls

Description

Sharing and Access controls provide granular control over external sharing and access to SharePoint Online. Sharing and Access control is essential for securing SharePoint Online document and information sharing.

Design Considerations

Access to SharePoint Sites can be controlled through a variety of means to ensure that the data of the sites is protected. This includes the configuration of:

- Only allowing access from specific IP address locations
- Only allowing access from apps that use modern authentication
- Blocking access from devices which are not managed by the organisation through Intune
- Sites can be further secured through the implementation of Idle session timeouts. Idle session timeouts essentially act to log a user out of SharePoint after a period of inactivity

Access Controls provides administrative tool to restrict access contents in SharePoint.

Design Decisions

Table 49 describes the SharePoint Online Sharing design decisions.

Table 49 SharePoint Online Sharing Design Decisions

Decision Points	Design Decision	Justification
Sharing Controls	Configured	Sharing to external users will be disabled. Documents within SharePoint Online can only be shared with internal users. Collaboration and sharing will be achieved using Teams.
Access Controls	Configured	Access to SharePoint Online will be controlled on a device level to ensure data is being accessed from approved devices.

Table 50 describes the Sharing configuration.

Table 50 Sharing Configuration

Configuration	Value	Description
External Sharing		
SharePoint	New and existing guests	Guest access is available in accordance with Collaboration in the DTA – Platform Design document
More external sharing settings	Limit external sharing by domain Guests must sign in using the same account to which the sharing invitations are sent	Checked. <Add domains that are allowed> Checked.
OneDrive	Only people in your organisation	No external sharing allowed.
File and folder links		
Choose the type of link that is created by default when users get links	Specific people	Internal link which can only be sent to people in your organisation.
Other settings		
Show owners the names of people who viewed their files in OneDrive	Checked	This is to ensure owners are aware of external users who have access to the document.
Let site owners choose to display the names of people who viewed files or pages in SharePoint	Checked	Permits display of activity on SharePoint sites to foster collaboration.
Use shorter links when sharing files and folders	Checked	Ensure URL are short and concise.
Default link permission	Edit	Users will have edit permissions by default to increase usability. If view permissions are required, this is also available.

Table 51 describes the Access Control configuration.

Table 51 Access Control Configuration

Configuration	Value	Description
Unmanaged Devices		
Unmanaged Devices	Allow limited, web only access	Provide restricted access to devices that aren't Intune compliant.
Idle session time-out		
Sign out inactive users automatically	On	Controls idle time on users logged onto a device.
Sign out users after:	1 hour	Ensure users are logged out after a particular idle time.
Give users this much notice:	5 minutes	Ensure users are notified before they are signed out.
Network Location		
Allow access only from a specific IP address range	Off	Define a trusted network boundary by specifying one or more authorized IP address ranges.
App that don't use modern Authentication		
App that don't use modern Authentication	Block access	Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

Legacy Features

Description

Legacy features allow for backwards compatibility for legacy capabilities from SharePoint on-premises to SharePoint Online. Legacy features are enabled only when there is a reason to do so, as they restrict the features available in SharePoint Online.

Design Considerations

Legacy features are provided by default by SharePoint Online to ensure backwards compatibility with legacy SharePoint on Premise solution.

Design Decisions

Table 52 describes the Legacy Features design decisions.

Table 52: Legacy Features Design Decisions

Decision Point	Decision	Justification
InfoPath	Not configured	InfoPath is going to be deprecated and it is recommended that InfoPath forms to be redeveloped into PowerApps in Office 365
Records Management	Not configured	Not required for this solution. Records Management administrative screen provides configuration settings to route files from a SharePoint Document Library to a centralised SharePoint Records Management site. This is to support the traditional Centralised records management system in SharePoint.
Secure Store Settings	Not Configured	Not required for this solution. Secure Store in SharePoint Online provides a key vault to store all sensitive information in SharePoint. This is primarily used by InfoPath to store sensitive keys and passwords. It is recommended to use Azure Key Vault to store sensitive information.
Business Connectivity Settings	Not configured	Not required for this solution. Business Connectivity Settings provides SharePoint on-premises ability to consume information from third party OData Information store. It is recommended to use PowerBI to consume third party data and publish it to SharePoint Online.

Search	Not configured	Not required for this solution. Search provides legacy support on crawled properties, managed properties and custom configuration required.
Term Store	Not configured	Not required for this solution. Term store provides a consistent taxonomy and ontology for the agency. This enables ease of search for information within SharePoint.
User Profile	Not configured	Not required for this solution. User Profiles provide legacy support of custom properties for users and complied audience.
Hybrid Picker	Not configured	Not required for this solution. This is to ensure hybrid term stores are synchronised between SharePoint Online and on-premises.

OneDrive for Business

Description

OneDrive for Business is a cloud-based, secure, personal document store. It allows storage and access of files from any approved device, allows offline editing, simple organisational collaboration, search tools, and advanced encryption and security features. The sharing of these documents can be controlled to allow or disallow sharing with external parties.

OneDrive data can be configured to automatically synchronise data so the user does not need to download files every time they wish to access them.

On deletion of a user's account content can be deleted or retained for a specified period of time.

Sharing

Description

The OneDrive sharing administration screen provides granular configuration. Controlling OneDrive sharing ensures that data is shared internally and externally in a secure manner.

Design Considerations

OneDrive provides end users the ability to securely store their personal data in Office 365. The design considers that OneDrive is used for personal storage and sharing within the department.

Design Decisions

Table 53 describes the OneDrive for Business Sharing design decisions.

Table 53 OneDrive for Business Sharing Design Decisions

Decision Point	Design Decision	Justification
External Sharing	Disabled	Sharing to external users will be disabled. Collaboration and sharing will be achieved using Teams.

Table 54 contains the OneDrive sharing configuration.

Table 54 OneDrive Configuration

Configuration	Value	Description
Links		
Default Link Type	Internal: Only people in your organisation	No sharing is permitted outside the Department.
External Sharing		
SharePoint	Only people in your organisation	No external sharing allowed.
OneDrive	Only people in your organisation	No external sharing allowed.
Advanced settings for external sharing		
Allow or block sharing with people on specific domains	Unchecked	Specific domains are not defined, meaning that content is permitted to be shared with all users within the directory (internal).
External users must accept sharing invitation using the same account that the invitations were sent to	Checked	Required to ensure users are authenticated before accepting sharing invitation
Let external users share items they don't own	Unchecked	Restricts external users (guests) from re-sharing content.
Other settings		
Display to owner the names of people who viewed their files	Checked	Ensure owner is are aware of who it has been shared with

Synchronisation

Description

OneDrive and SharePoint can synchronise content locally through the OneDrive for Business client. Content can be "pinned" for offline use, ensuring that specific content is available offline, and changes are merged at a later date. The Sync Administration screen provides control Synchronising of File in OneDrive and SharePoint.

Design Considerations

This is required to provide the ability for end users to work offline from Office 365. This section describes the design decisions to enable end users to sync files from OneDrive to their managed device.

Design Decisions

Table 55 describes the OneDrive for Business Sync design decisions.

Table 55 OneDrive for Business Sync Design Decisions

Decision Point	Design Decision	Justification
Sync client	Configured	The OneDrive sync client is used to synchronise Desktop, Documents and pictures folders with the users OneDrive as well as allowing the synchronisation of SharePoint and Teams files.

Table 56 describes the storage and synchronisation configuration.

Table 56 Storage and Synchronisation Configuration

Configuration	Value	Description
Show the Sync button on the OneDrive Website	Checked	The sync button allows OneDrive files to be synced locally through the OneDrive for Business client.
Allow syncing only on PC joined to specific domains	Unchecked	Access to OneDrive content and synchronisation is controlled via Conditional Access, so this setting is not configured.
Block syncing of specific file type	Unchecked	File type synchronisation is not restricted. Office ATP and Defender ATP provides additional protection against malicious files.
Days to retain files after user account is marked for deletion	365 days	Default setting. Must align with the agency internal record keeping policies.
Limit OneDrive user Capacity	1024GB	Default setting. The largest home drive identified by the Department is less than 1TB.

Notifications

Description

Notifications provide OneDrive users with information about how OneDrive is operating. The notification administration screen provides notification control to OneDrive owners.

Design Considerations

The design considers notification and alerting of users for all shared documents in the organisation to ensure users are aware of the status of shared documents.

Design Decisions

Table 57 describes the OneDrive Notification design decisions.

Table 57 OneDrive Notification Design Decisions

Decision Point	Design Decision	Justification
User notifications	Configured	Notifications will be configured to provide users with relevant information.

Table 58 describes the OneDrive notification configuration.

Table 58 OneDrive Notification Configuration

Configuration	Value	Description
Display device notification to users when OneDrive files are shared with them	Checked	OneDrive will notify users when new files are shared with them
E-mail OneDrive owners when		
Other users invite additional external users to shared files	Checked	OneDrive will notify users when a user re-shares a document to an external user (guest)
External users accept invitations to access files	Checked	OneDrive will notify users when external users accept an invitation to access files.

An anonymous access link is created	Checked	OneDrive will notify users when an anonymous access link is created

Microsoft Teams

A Team in Microsoft Teams is a grouping of users who are working together to achieve an outcome. Within the Team, Channels can be used to breakdown the work into smaller more specific items. These channels can be extended using Bots, Tabs, and connectors.

Microsoft Teams leverages most of the functionality of the Office 365 components. When a Team is created the following artefacts are created out of the box:

- **SharePoint Site** - A new SharePoint site with the URL format of /sites/<SiteTitle>, with the <SiteTitle>'s spaces are stripped out.
- **Office 365 Group** - A new Office 365 Group, which is added into the Azure AD tenant. This is created with the site title as the Group Name.
- **Teams email –** A new email address per channel can be created. The email inbox is managed centrally by the Microsoft Team services. At the time of writing this document, the email address will have a domain of <custom email inbox>@apac.teams.ms.
  Note: This email is not part of Microsoft Exchange Online.

Access

Description

Access to a team in Microsoft Teams is controlled through the use of Office 365 groups located in Azure AD.

Design Considerations

On team creation, an Office 365 group will be created. Owners of the group can perform administrative actions across the team. Office 365 group creation can be restricted to a security group and Administrators.

Design Decisions

Table 59 describes the Teams Access design decisions.

Table 59 Teams Access Design Decisions

Decision Point	Design Decision	Justification
Team creation permission	Selected administrators	Teams will be created by select administrators to ensure that Teams are created using a documented approval workflow, avoiding Team proliferation. This setting is required as Azure AD group creation is restricted which only allows administrators to create 365 groups, and hence Teams.
Administrative action over Teams after creation	Team Owners	Team Owners will either be selected administrators (for Teams such as branches with many users) or managers and their delegates (such as in a section with relatively small user counts). Team owners will be assigned logically at creation time and updated as required
Team membership allocation	Manual by administrators or Team Owners	Team membership will be allocated manually initially with dynamic group allocation investigated in a future project phase when the logic for group membership is developed.

Dynamic Security groups

Description

Dynamic Security Groups are Azure AD security groups that are populated based on device and/or user attributes.

Design Considerations

Dynamic Security groups can be leveraged to control access to locations, services, and features.

The membership of a Dynamic Security group is updated whenever an attribute of a device or user is modified. If the user/device no longer matches the group rule, then that user/device is removed. Conversely if a user/device now matches the group rule they are added. When a user is added the group can be configured so that the added user receives an email notifying them of the addition.

When dynamic security groups are used more widely, naming of Dynamic Security groups can be streamlined using a Naming Policy. The Naming Policy ensures that the groups within the environment conform to a standard and their purpose can be easily identified.

Design Decisions

Table 60 describes the Dynamic Security Group design decisions.

Table 60 Dynamic Security Group Design Decisions

Decision Point	Design Decision	Justification
Naming Policy	grp-<Agency>-<GroupName>	Assists in MOGs and standardisation of agency configuration.

Organisation Wide Configuration

Description

Microsoft Teams is a collaboration platform that enables the agency to work collaboratively with external agencies. This allows users to collaborate internally and with trusted guest users and set up meetings with external users.

Design Considerations

The design will consider the following configurations

- **External Access** - configures allowable domains to connect to the agency instance of Microsoft Teams. This also configures Skype for Business integration.
- **Guest Access** – is when an external user is invited to be a member of the team. Once a team owner has granted someone guest access, they can access that team's resources, share files, and join a group chat with other team members.
- **Teams Settings** – configures the default behaviour of all users in the Teams application.

Design Decisions

Table 61 describes the Teams Organisation Wide design decisions.

Table 61: Teams Organisation Wide configuration

Decision Point	Design Decision	Justification
External Access	**Configured:** (Example) Allow dta.gov.au	Allow only dta.gov.au and deny sharing to external users. This will prevent users from setting up meetings with users that are not setup as a Guest of the department.
Guest Access	**Configured**: Guest Access: Enabled Disable Giphy, Memes and stickers	Disable Giphy Meme and stickers.
Teams Setting	**Configured** Disable all third-party file storage	This is to ensure departmental users do not save file outside of the Office 365 tenant.

Policies & Settings

Description

Microsoft Teams provides ability to create policies around messaging, meetings, calling, video, and guest access. These settings can be configured in policies and assigned to individual users within the organisation.

Design Considerations

The list below highlights the policies that can be configured with in teams:

- **Teams Policies** – Teams policies defines the policy for users to discover private teams and create private channels.
- **Meeting Policies** – Meeting policies define creations of meetings, audio and video, content sharing, and participant and guest permissions to meetings in Teams
- **Live events Policies** – Live events policies is used to globally broadcast departmental meeting via teams.
- **Messaging Policies** – Messaging policies defines behaviour of messages in Teams. The policy defines user capability in sending, editing, deleting, voice messages, and using giphy, stickers, URL preview and translator.

- **Teams App** – Teams apps policy defines the list of apps that can be used in Teams. Microsoft Teams provides Microsoft published apps and third-party apps that can be used in Microsoft Teams. Departments can control on creation of custom apps in Teams.

Design Decisions

Table 60 describes the Dynamic Security Group design decisions.

Table 60 Teams Policy design decision

Decision Point	Design Decision	Justification
Team Policy	**Configured**: Disable private channels	Team policy will be left as default settings. Discovered private teams Create private channels
Meeting Policies	**Configured** Global policy: Disable Whiteboard Automatically admit people – Everyone in your organisation	Meeting policy dictates how audio, videos and applications that are used in a team meeting. Whiteboard will be disable as the application does not meet application residency requirements.
Live events Policies	**Configured**: Who can join live events: Everyone in Organisation	Live events is configured to prevent users outside of the organisation (guest and external users) cannot attend these meeting.
Messaging Policy	**Configured**: Disable Giphy, Memes and stickers	Messaging policy dictate how messaging is used in Teams. These includes usage of Giphy, Memes and stickers in messages.
Teams app	**Configured** Global Policy: Block specific app from Microsoft Apps • Forms • Yammer Block all Third-Party Apps Block all Tenant Apps	Microsoft Forms and Yammer are hosted in United States. This will cause data sovereignty issue for the agency All Third-Party Apps are blocked. These Third-Party apps needs to be evaluated individually. Tenant Apps are custom developed applications created by the agency. This should be enabled if it is required.

Voice Calling

Description

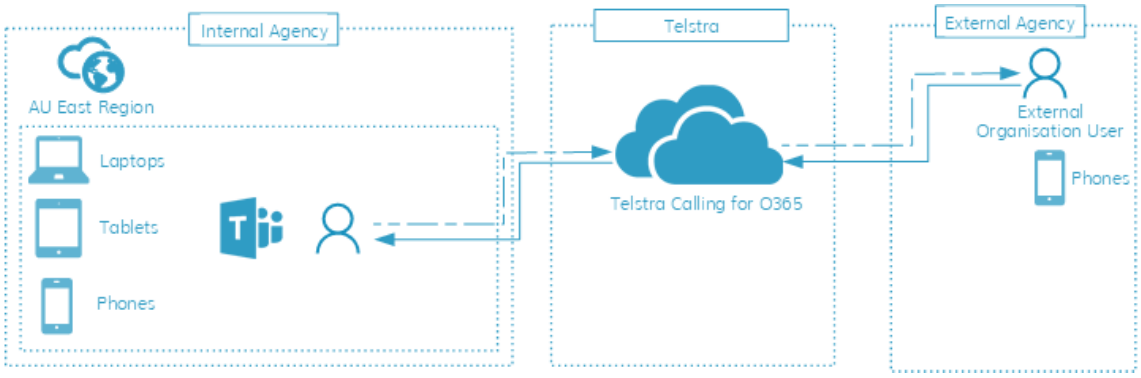
Enables agencies to make calls to landlines or mobiles within Microsoft Teams.

Design Considerations

Telstra Calling for Office 365 avoids the complexity of separate collaboration systems.

Figure 3 describes how connectivity is achieved between Microsoft Teams and Telstra.

Figure 3 - Telstra Calling for Office 365



Design Decisions

Table 62 describes the Voice Calling design decisions.

Table 62 Voice Calling Design Decisions

Decision Point	Design Decision	Justification
Telstra calling for Office 365	Configured	Agencies will require dial in and dial out functionality. This arrangement will need to be organised, paid for and configured by agencies that require this functionality. The configuration will not be covered in this blueprint.

Security and Compliance

Office 365 provides Security and Compliance tools which can be utilised to implement an organisation's Information Management Policy and to assist with information governance. The Office 365 Security and Compliance tools provides the ability to govern and monitor the following components:

- SharePoint Online
- OneDrive for Business
- Teams
- Exchange Online

Alerts

Description

Office 365 contains various out-of-the-box Alert Policies, some of which are dependent on the available Office 365 licence. Alert Policies can be configured to track administrative activities, malware threats, user actions and/or data loss incidents.

Design Considerations

Each alert can be configured with the following settings:

- **Tracked Activity** - The activity that will cause the alert to be generated. For example, sharing a file with an external user, assigning access permissions, or creating an anonymous link
- **Activity Conditions** - When a tracked activity triggers, additional conditions can be applied to filter out unnecessary alerts. For example, an alert can be triggered only if a certain user performs a task
- **When to Trigger** - When the above conditions are met, further filtering can be applied to only alert when a certain threshold is met. For example, an alert is only raised if the activity has been performed more than five times
- **Alert Category** - An alert category is assigned to assist with tracking and managing the alerts generated

- **Alert Severity** - An alert severity is assigned to assist with tracking and managing the alerts generated. The severity is displayed in the subject line of the alert email
- **Alert Notification** - An alert can be configured with a list of email addresses that should receive the alert notifications. Daily notification limits can also be configured to ensure an alert receiver is not bombarded with alert emails for the same event. Triggered alerts can also be viewed in the Security & Compliance Center

Design Decisions

Table 63 describes the Alert Policies design decisions.

Table 63 Alert Policies Design Decisions

Decision Point	Design Decision	Justification
Alert Policies Status	Default Alert Policies enabled	Custom alert policies are not required for the initial phase. Custom alert policies will be considered in a future project phase.

Office 365 provides Security and Compliance tools which can be utilised to implement an organisation's Information Management Policy and to assist with information governance. The Office 365 Security and Compliance tools provides the ability to govern and monitor the following components:

- SharePoint Sites
- OneDrive for Business
- Exchange Online
- SharePoint Groups
- Alerts

Office 365 contains various out of the box Alert Policies, some of which are dependent on the available Office 365 licence. Alert Policies can be configured to track administrative activities, malware threats, user actions and/or data loss incidents.

Each alert can be configured with the following settings:

- **Tracked Activity** - The activity that will cause the alert to be generated. For example, sharing a file with an external user, assigning access permissions, or creating an anonymous link
- **Activity Conditions** - When a tracked activity triggers, additional conditions can be applied to filter out unnecessary alerts. For example, an alert can be triggered only if a certain user performs a task

- **When to Trigger** - When the above conditions are met, further filtering can be applied to only alert when a certain threshold is met. For example, an alert is only raised if the activity has been performed more than 5 times
- **Alert Category** - An alert category is assigned to assist with tracking and managing the alerts generated
- **Alert Severity** - An alert severity is assigned to assist with tracking and managing the alerts generated. The severity is displayed in the subject line of the alert email
- **Alert Notification** - An alert can be configured with a list of email addresses that should receive the alert notifications. Daily notification limits can also be configured to ensure an alert receiver is not bombarded with alert emails for the same event. Triggered alerts can also be viewed in the Security & Compliance Center

Table 64 describes the Alert Policies design decisions.

Table 64 Alert Policies Design Decisions

Decision Point	Design Decision	Justification
Alert Policies Status	Default Alert Policies enabled	Custom alert policies are not required for the initial phase. Custom alert policies may be considered in the future based on ongoing requirements.

Classification Labels

Description

Classification labels which is located under the Office 365 Security & Compliance Center offers the ability to both control the data flow of sensitive information and control the retention of data. Classifications labels consists of the following:

- **Sensitivity Labels** – Allow label specific protection policy settings to be enforced
- **Retention Labels** – Allow label specific retention policy settings to be enforced

Sensitivity labels can be applied in the supported Office applications either in Office 365 ProPlus, Office Online or using the Azure Information Protection (AIP) unified labelling client. The AIP unified labelling client is not capable of the advanced functions listed above however it is supported across

multiple platforms including MacOS. These functions will be added at a future stage as the older AIP client will be retired in favour of the AIP Unified Labelling Client.

Design Considerations

Classification labels are published to users using Label Policies. Label Policies define the users who can utilise the label and the locations within Office 365 where it can be used. Classification labels can be applied in the following ways:

- **Manually** - The label is applied manually by the end-user
- **Automatically applied based on the location of the document** - Labels can be configured to automatically apply based on the location of the document. For example, SharePoint
- **Automatically applied based on detected Sensitive Information Type** - Labels can be configured to automatically apply based on the type of sensitive information found. For example, documents containing Australia driver's license numbers

At the time of writing, Sensitivity labels cannot be configured to satisfy some specific requirements listed in the Protective Security Policy Framework (PSPF). The PSPF requires the protective marking to be applied to email messages via either:

- Appending the protective marking to the Subject field using a specified syntax (Subject Field Marking)
- Including the protective marking in an Internet Message Header Extension using a specified syntax (Internet Message Header Extension)

Sensitivity labels create a protective marking within the message header however they do not meet the format outlined in the PSPF. The subject field marking can also not be implemented as Exchange Online does not allow the appending of the subject line using transport rules.

At time of writing, a solution is being developed to integrate Sensitivity labels with a mail relay solution to meet the format outlined in the PSPF.

Design Decisions

Table 65 describes the Classification design decisions.

Table 65 Classifications Design Decisions

Decision Point	Design Decision	Justification
Sensitivity Labels	Enabled	Labels will be applied in accordance with the latest guidance from the Protective Security Policy Framework
Retention Labels	Enabled	Labels are recommended to be applied to automate retention configuration and compliance, but the development of specific retention labels is out of scope for this project
Labelling Policy	Enabled	Users will apply labels manually initially. Automatic labelling will be developed in a future project stage after considering potential impacts on backups and productivity changes

Retention Policies

Description

Business information is required to be managed in order to comply with industry and government regulations and internal policies that require data to be retained for a certain period.

Design Considerations

Office 365 retention policies assist with meeting these requirements by providing the following features:

- Configure policies to proactively decide whether to retain content, delete content, or both retain and then delete the content
- Apply a single policy to the entire organisation or just to specific locations or users
- Apply a policy to all content or just content meeting certain conditions, such as content containing specific keywords or specific types of sensitive information

When information is subject to a retention policy, end-users can continue to edit and work with the content as if nothing's changed because the content is retained in place, in its original location. But if

someone edits or deletes content that's subject to the policy, a copy is saved to a secure location where it's retained while the policy is in effect.

Design Decisions

Table 66 describes the Retention Policies design decisions.

Table 66 Retention Policies

Decision Point	Design Decision	Justification
Retention Policies	Configured	To ensure that legislative data retention requirements are met. This is to ensure that the agency holds the data for fraud detection.

Table 67 describes the Retention Policies configuration.

Table 67 Retention Policy Configuration

Decision Point	Design Decision	Justification
Name: Exchange Indefinite Hold		
Retention configuration	Retain the data "Forever"	How long the data is to be held by the policy.
Location	Exchange email – All users included	The Office 365 location where the policy applies.
Name: SharePoint Indefinite Hold		
Retention configuration	Retain the data "Forever"	How long the data is to be held by the policy.
Location	SharePoint Sites – All Sites	The Office 365 location where the policy applies.
Name: OneDrive Indefinite Hold		
Retention configuration	Retain the data "Forever"	How long the data is to be held by the policy.
Location	OneDrive Accounts – All Accounts	The Office 365 location where the policy applies.
Name: Office 365 Groups Indefinite Hold		
Retention configuration	Retain the data "Forever"	How long the data is to be held by the policy.
Location	Office 365 Groups – All Groups	The Office 365 location where the policy applies.

Name: Teams Channel Messages Indefinite Hold		
Retention configuration	Retain the data “Forever”	How long the data is to be held by the policy.
Location	Teams channel messages – All teams included	The Office 365 location where the policy applies.
Name: Teams chats Indefinite Hold		
Retention configuration	Retain the data “Forever”	How long the data is to be held by the policy.
Location	Teams chats messages – All users included	The Office 365 location where the policy applies.

Data Loss Prevention

Description

Data Loss Prevention (DLP) policies enable an organisation to identify, monitor, and automatically protect sensitive information across Office 365. DLP policies can be targeted to one or multiple products within the Office 365 suite.

Design Considerations

A DLP policy can be configured to:

- Identify sensitive information, documents in a specific site (for SharePoint only) or specific labels contained in Exchange Online, SharePoint Online, and OneDrive for Business.
- Prevent end-users from accidental sharing sensitive information
- Prevent end-users from accidentally deleting a document
- Educate end-users by presenting messages them on how to stay compliant when relevant. This is done without interrupting their workflow

At the time of writing Office 365 has 100 prebuilt sensitive information types (Australian Passport Numbers etc.). In addition to the prebuilt sensitive information types custom types can be created. These custom types look for strings, patterns, or key words.

Design Decisions

Table 68 describes the Data Loss Prevention design decisions.

Table 68 Data Loss Prevention Design Decisions

Decision Point	Design Decision	Justification
Data Lost Prevention Policies	Configured	To provide insights into the movement of potentially sensitive information.

Table 69 describes the Data Loss Prevention design decisions.

Table 69 Data Loss Prevention Configuration

Policy Setting	Configuration	Description
Name: Australian Privacy Act		
Locations	Protect content in Exchange email, Teams chats, channel messages, OneDrive and SharePoint documents.	The locations where the policy will apply.
Content type	Australian Driver's Licence number Australian Passport number	The types of sensitive information being detected.
Sharing detection	With people outside my organisation	When the policy is applied.
Notify users	Enabled	Users are notified when the policy is triggered. They are also provided policy tips for managing sensitive information.
Amount of instances	5	The amount of sensitive information required to trigger the policy (10 is the default).
Send incident reports	Enabled	User and nominated administrator are notified when the policy is triggered.
Restrict access or encrypt the content	Disabled	Access to the content that triggers the policy can be encrypted or and access limited.
Name: Australian Personally Identifiable Information (PII) data		
Locations	Protect content in Exchange email, Teams chats, channel messages, OneDrive and SharePoint documents.	The locations where the policy will apply.

Content type	Australia Tax File Number Australia Driver's Licence Number	The types of sensitive information being detected.
Sharing detection	With people outside my organisation	When the policy is applied.
Notify users	Enabled	Users are notified when the policy is triggered. They are also provided policy tips for managing sensitive information.
Amount of instances	5	The amount of sensitive information required to trigger the policy (10 is the default).
Send incident reports	Enabled	User and nominated administrator are notified when the policy is triggered.
Restrict access or encrypt the content	Disabled	Access to the content that triggers the policy can be encrypted or and access limited.
Name: Australian Health Records Act (HRIP Act)		
Locations	Protect content in Exchange email, Teams chats, channel messages, OneDrive and SharePoint documents.	The locations where the policy will apply.
Content type	Australia Tax File Number Australia Medical Account Number	The types of sensitive information being detected.
Sharing detection	With people outside my organisation	When the policy is applied.
Notify users	Enabled	Users are notified when the policy is triggered. They are also provided policy tips for managing sensitive information.
Amount of instances	5	The amount of sensitive information required to trigger the policy (10 is the default).
Send incident reports	Enabled	User and nominated administrator are notified when the policy is triggered.
Restrict access or encrypt the content	Disabled	Access to the content that triggers the policy can be encrypted or and access limited.

Name: Australian Financial Data		
Locations	Protect content in Exchange email, Teams chats, channel messages, OneDrive and SharePoint documents.	The locations where the policy will apply.
Content type	SWIFT Code Australia Tax File Number Australia Bank Account Number Credit Card Number	The types of sensitive information being detected.
Sharing detection	With people outside my organisation	When the policy is applied.
Notify users	Enabled	Users are notified when the policy is triggered. They are also provided policy tips for managing sensitive information.
Number of instances	10	The amount of sensitive information required to trigger the policy (10 is the default).
Send incident reports	Enabled	User and nominated administrator are notified when the policy is triggered.
Restrict access or encrypt the content	Disabled	Access to the content that triggers the policy can be encrypted or and access limited.

Audit and Logging

Description

The Office 365 Security & Compliance Center provides the ability to monitor and review user and administrator activities across the Office 365 applications from the past 90 days. Audit logs are kept by default for 90 days but are configurable up to one year by default for E5 licensing.

When an event occurs for the respective application it will take anywhere from 30 minutes up to 24 hours before it can be viewed in the audit log search.

The Office 365 Management Activity API enables third-party applications to consume audit logs from Office 365. If audit logging is disabled, third-party applications can still consume audit logs from the Office 365 Management Activity API.

Table 70 shows the list of Office 365 applications, their auditing capabilities and duration wait time once an event occurs.

Table 70 Office 365 applications and auditing

Application	User Activity	Admin Activity	Duration wait time
Exchange Online	Yes	Yes	30 minutes
OneDrive for Business	Yes		30 minutes
SharePoint Online	Yes	Yes	30 minutes
Sway	Yes	Yes	24 hours
Power Bi	Yes	Yes	30 minutes
Workplace Analytics		Yes	30 minutes
Dynamics 365	Yes	Yes	24 hours
Yammer	Yes	Yes	24 hours
Microsoft Power Apps	Yes	Yes	24 hours
Microsoft Power Automate	Yes	Yes	24 hours
Microsoft Steam	Yes	Yes	30 minutes
Microsoft Teams	Yes	Yes	30 minutes
Microsoft Forms	Yes	Yes	30 minutes
Azure Active Directory		Yes	24 hours
eDiscovery activities in Office 365 Security & Compliance Center[9]	Yes	Yes	30 minutes

Design Considerations

At the time of writing, audit logging is not enabled by default and must be turned on first in the Office 365 Security & Compliance Center before user or administrator activities can be audited.

[9] https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log

Design Decisions

Table 71 describes the Audit Logging design decisions.

Table 71 Audit Logging

Decision Point	Design Decision	Justification
Unified Audit Logging	Enabled One-year retention	To provide visibility into the actions being undertaken within the Office 365 environment.

Office 365 Advanced Threat Protection

Description

Office 365 Advanced Threat Protection (ATP) extends the native security features in Office 365.

Design Considerations

The protections provided by Office 365 ATP are designed to defend against attacks from multiple threat vectors including email, websites and documents stored in online libraries, such as SharePoint Online. Each of the Office 365 ATP capabilities is enabled and managed via policies configured from the Office 365 Security and Compliance Center.

Office 365 ATP provides the following capabilities:

- **Office 365 ATP Safe Links** - Office 365 ATP Safe Links provides inspection of links included in emails and Office 365 documents to determine if it is malicious
- **Office 365 ATP Safe Attachments** - Office 365 ATP Safe Attachments provides sandbox execution of attachments to detect and delete malicious content
- **Office 365 ATP Anti-Phishing** - Office 365 ATP Anti-Phishing provides machine learning capabilities to detect advanced phishing campaigns

Design Decisions

Table 72 describes the Office 365 ATP design decisions.

Table 72 ATP Design Decisions

Decision Point	Design Decision	Justification
Office 365 ATP Safe Links	Configured	Configured in accordance with advice in PROTECT - Malicious Email Mitigation Strategies (Nov 2019)
Office 365 ATP Safe Attachments	Configured	Configured in accordance with advice in PROTECT - Malicious Email Mitigation Strategies (Nov 2019)

Office 365 ATP Anti-Phishing	Configured	Configured in accordance with advice in PROTECT - Malicious Email Mitigation Strategies (Nov 2019)

Safe Links

Description

ATP Safe Links can help protect an organisation by providing time-of-click verification of web addresses (URLs) in email messages and Office documents. Protection is defined through ATP Safe Links policies that are configured by an organisation.

Design Considerations

ATP Safe Links protection works as outlined below for URLs in emails that are hosted in Office 365:

- All incoming email goes through Exchange Online Protection, where IP and envelope filters, signature-based malware protection, anti-spam and anti-malware filters are applied
- An end-user signs into Office 365 and accesses their Exchange Online mailbox
- An end-user opens an email message containing a URL, and then clicks on the URL in the email message
- The ATP Safe Links feature immediately checks the URL before opening the website. The URL is identified as blocked, malicious, or safe
- If the URL sends an end-user to a website that is included in a custom "Do not rewrite" URLs list for a policy that applies to the user, the website opens
- If the URL sends an end-user to a website that is included in the organisation's custom blocked URLs list, a warning page opens
- If the URL sends an end-user to a website that has been determined to be malicious, a warning page opens
- If the URL goes to a downloadable file and the ATP Safe Links policies are configured to scan such content, the downloadable file is checked
- If the URL is considered safe, the end-user is taken to the website

ATP Safe Links protection works as outlined below for URLs in Office 365 ProPlus applications:

- A user opens a Word, Excel, PowerPoint, or Visio, and is signed in using their Office 365 security credentials. The document contains URLs

- When a user clicks on a URL in the document, the link is checked by the ATP Safe Links service
- If the URL sends an end-user to a website that is included in a custom "Do not rewrite" URLs list for a policy that applies to the user, that user is taken to the website
- If the URL sends an end-user to a website that is included in the organisation's custom blocked URLs list, the user is taken to a warning page
- If the URL sends an end-user to a website that has been determined to be malicious, the user is taken to a warning page
- If the URL goes to a downloadable file and the ATP Safe Links policies are configured to scan such downloads, the downloadable file is checked
- If the URL is considered safe, the end-user is taken to the website

Design Decisions

Table 73 describes the Safe Links design decisions.

Table 73 ATP Safe Links Design Decisions

Decision Point	Design Decision	Justification
Office 365 ATP Safe Links	Configured	Configured in accordance with advice in PROTECT - Malicious Email Mitigation Strategies (November 2019)

Table 74 describes the Safe Links configuration.

Table 74 ATP Safe Links Configuration

Decision Point	Design Decision	Justification
Settings that apply to content across Office 365		
Block the following URL's	No URL's defined.	Managing the Blocked URL list is an ongoing administrative task. Suggest and administrator be employed to conduct these activities.
Settings that apply to content except mail		
Use safe links in Office 365 ProPlus, Office for iOS and Android	Enabled	Safe links will be checked by default within these Office 365 applications

Office Online of the above applications	Enabled	To protect URL's in the Office Online viewer, enable this setting.
For the locations selected above: Do not track when users click safe links	Enabled	Information about when end-users click safe links in the Office 365 documents will not be stored due to the amount of logging it will consume.
For the locations selected above: Do not let users click through safe links to original URL	Enabled	If end-users click on safe links in Office 365 documents, then they will be directed to a warning page and will not be presented with an option to continue to the original link.

Safe Attachments

Description

The ATP Safe Attachments feature checks email attachments at the email is received but before it is delivered to the user mailbox.

Design Considerations

When an ATP Safe Attachments policy is in place and an end-user who is covered by that policy views their email in Office 365, their email attachments are checked, and appropriate actions are taken, based on the configured policies.

Design Decisions

Table 75 describes the Safe Attachments design decisions.

Table 75 ATP Safe Attachments Design Decisions

Decision Point	Design Decision	Justification
Office 365 ATP Safe Attachments	Configured	Configured in accordance with PROTECT - Malicious Email Mitigation Strategies (November 2019)

Table 76 describes the Safe Attachments configuration.

Table 76 ATP Safe Attachments Configuration

Decision Point	Design Decision	Justification
Protect files in SharePoint, OneDrive, and Microsoft Teams	Checked	If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent users from opening and downloading the file.
Warning	Dynamic Delivery	Dynamic Delivery ensures attachments are scanned and detected malware is quarantined. It also includes attachment previewing capabilities for most PDFs and Office files during scanning.
Redirect attachment on detection. Send the blocked, monitored or replaced attachment to an email address	Enable Redirect - Ticked	This will send blocked or replaced email messages with an attachment that is identified as malicious to a selected email address.
Apply the above selection of malware scanning for attachments times out or error occurs	Ticked	Will redirect an end-user's email messages to a selected email address even if a time out or error occurs when malware scanning an attachment. This allows legitimate emails to be recovered and malware to be investigated.
Applied to	Configured	All agency domains (e.g., dta.gov.au).

Anti-Phishing

Description

ATP anti-phishing protects users by checking incoming messages for indicators that the message may be spoofed by impersonator or part of a phishing campaign. Most phishing emails involves a malicious actor disguising oneself (spoofing) as an individual who is known to the recipient. The messaged is crafted in a such a way which can trick the user into clicking a link, downloading malware, or stealing user credentials.

Design Considerations

Anti-phishing uses mailbox intelligence to build a profile of communication habits between each user and maps out these relationship patterns. In an event of a phishing campaign ATP will analyse the message behaviour against the user profiles to determine if the sender is legitimate or an impersonator.

Anti-spoof specifically analyses the senders address to determine if it is legitimate or forged. Administrators can allow our block specific users from spoofing an internal domain. i.e. An external organisation to send out advertising or products on behalf of the agency.

Design Decisions

Table 77 describes the Office 365 ATP Anti-Phishing design decisions.

Table 77 ATP Anti-Phishing Design Decisions

Decision Point	Design Decision	Justification
Office 365 ATP Anti-Phishing	Configured	Configured to meet ACSC - PROTECT - Malicious Email Mitigation Strategies (November 2019)

Table 77 describes the ATP Anti-Phishing configuration.

Table 78 Anti-Phishing Configuration

Configuration	Value	Description
Impersonation Policy		
Add users to protect	Off	Add up to 60 internal and external users you want to protect from being impersonated by attackers.
Add domains to protect	Automatically include the domains I own: On Include custom domains: Off	Specify domains which you want to protect from being impersonated by attackers.
Actions	If email is sent by an impersonated user: Quarantine the message If email is sent by an impersonated domain: Quarantine the message	Specify an action in an event an attacker impersonates the users or domains you have specified.

Mailbox Intelligence	Enable mailbox intelligence: On Enable mailbox intelligence based on impersonated protection: On If an email is sent by an impersonate user: Quarantine the message	This feature uses machine learning to determine a user's email patterns with their contacts. With this information, the artificial intelligence can better distinguish between genuine and phishing emails. Impersonated protection allows Office 365 to customize user impersonation detection and better handle false positives. When user impersonation is detected, based on mailbox intelligence, you can define what action to take on the message.
Add trust senders and domains	Not configured	When users interact with domains or users that trigger impersonation but are considered to be safe. i.e. if a partner has the same/similar display name or domain name as a user defined on the list.
Spoofing Policy		
Spoofing filter settings	Enable antispoofing protection: On	Allows the Department to filter email from senders who are spoofing domains.
Enable Unauthenticated Sender Feature	Enable Unauthenticated Sender: On	Displays a notification to users in Outlook when a sender fails authentication checks.
Actions	If email is sent by someone who's not allowed to spoof your domain: Quarantine the message	Specify an action in an event an unauthorised user spoofs a domain.

Abbreviations and Acronyms

Table 79 details the abbreviations and acronyms used throughout this document.

Table 79 Abbreviations and Acronyms

Acronym	Meaning
ABAC	As Built As Configured
ACSC	Australian Cyber Security Centre
AD	Active Directory
AIP	Azure Information Protection
API	Application Programming Interface
ASD	Australian Signals Directorate
ATP	Advanced Threat Protection
CAS	Client Access Server
CNAME	Canonical Name
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System
DTA	Digital Transformation Agency
EMS	Enterprise Mobility & Security
FQDN	Fully Qualified Domain Name
GAL	Global Address List
GB	Gigabytes
GIF	Graphics Interchange Format
GMT	Greenwich Mean Time
HRIP	Health Records and Information Privacy
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service

ICT	Information and Communication technology
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISM	Information Security Manual
IT	Information Technology
JPG	Joint Photographic Experts Group
KB	KiloByte
MX	Mail Exchange
OAB	Offline Address Book
OWA	Outlook Web Access
PII	Personally Identifiable Information
PNG	Portable Network Graphics
POP	Post Office Protocol
PSPF	Protective Security Policy Framework
PST	Personal Storage Table
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Subject Alternate Name
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SPAM	Unsolicited Commercial Email
SPF	Sender Policy Framework
SVG	Scalable Vector Graphics
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TB	Terabytes
TLS	Transport Layer Security
URL	Uniform Resource Locator (Web address)

VIP	Virtual IP
VPN	Virtual Private Network