

Configuration Guide to Minimise Common Data Breach Issues for Microsoft 365

09 MAY 2022

Supported by

In supported of

Getting Started

This quick-start configuration guide is to help businesses minimise common breach issues through good security practices in Microsoft 365, using these simple configuration steps.

The guide is for organisations using Microsoft 365 (“M365”) Business Standard edition through Windows devices. Some of the settings are to be configured at M365, while others are to be configured at the Windows devices (“@Windows Device”).

Windows 10 Enterprise is used as the reference version for the steps and screenshots shared.

(Note: This guide does not include the initial setup process such as planning and deploying your tenant, apps, and services.)

Contents

WINDOWS DEVICE SETTINGS

1. [Strong Password Settings](#)
2. [How to Turn On Bitlocker Disk Encryption](#)

M365 SETTINGS

1. [Enable Multi-Factor Authentication \(MFA\) for Administrators](#)
2. [Review of User Accounts](#)
3. [Disable Email Auto Forwarding](#)
4. [Configure Folder Permissions for OneDrive](#)
5. [Manual Back-Up of Local Files](#)
 - [Back-up from local device to OneDrive](#)
 - [Restore from OneDrive to local device](#)
6. [Restoring the Entire OneDrive](#)
7. [Restoring a Selected File in OneDrive](#)

APPENDIX

[How to Securely Zip a File](#)

CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

1. Strong password settings (@Windows device)

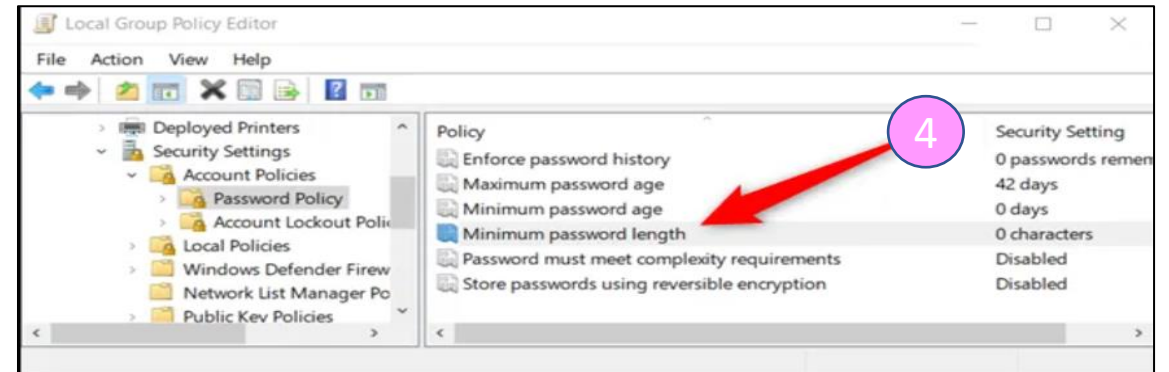
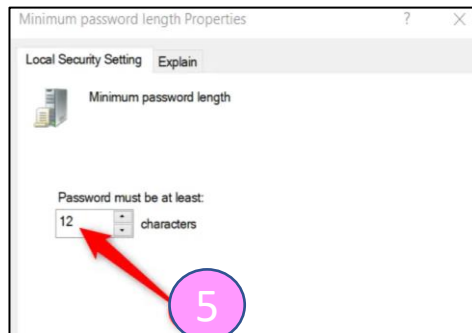
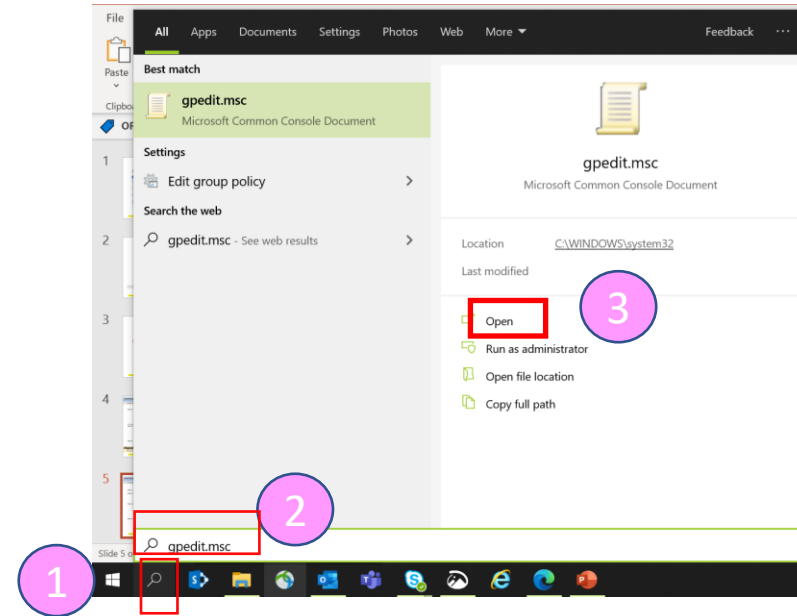
Step 1: Launch the group policy editor by pressing Windows+R

Step 2: Type “gpedit.msc” and press “Enter”

Step 3 Click to “Open”

Step 4: Navigate to Computer configuration > “Windows settings” > “Security settings” > “Account policies” > “Password policy” > “Minimum password length”

Step 5: Set the minimum password length to 12 characters

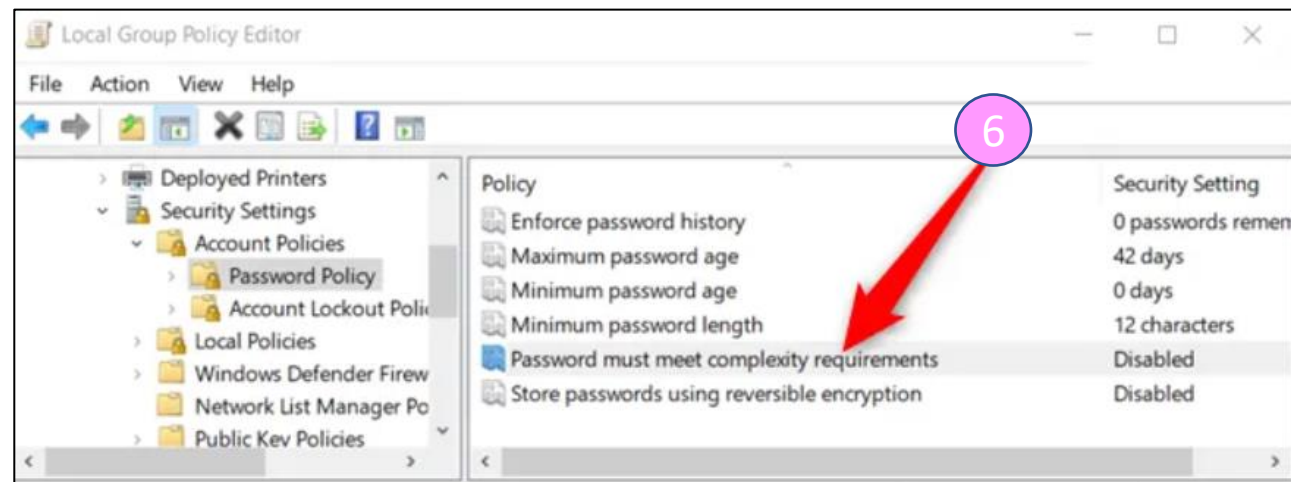


CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

1. Strong password settings (@Windows device) – Cont'd

Step 6: Click to enable password complexity requirements, to facilitate users in creating a secure password

Step 7: Restart your computer after making the policy changes




Enabling the complexity requirements means:

- DO NOT contain the user account name or full name
- Be at least 6 characters in length and contain characters from at least 3 of the following 4 categories:
 - Uppercase English letters (A-Z)
 - Lowercase English letters (a-z)
 - Base 10 digits (0-9)
 - Non-alphabetic characters (such as \$, !, %)

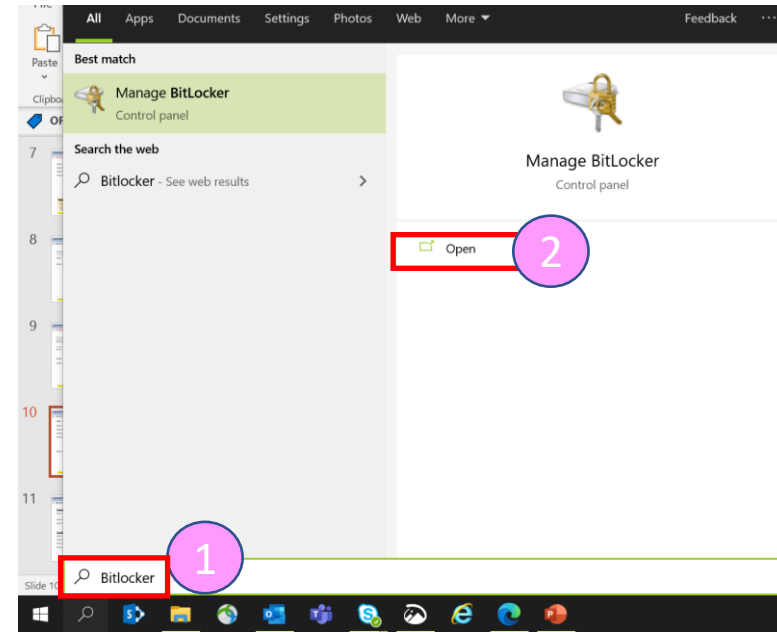
CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

2. How to Turn on BitLocker Disk Encryption (@Windows device)

NOTE: For Windows 10, BitLocker is available on the Pro and Enterprise editions only

Step 1: Click on the magnifying glass and type "Bitlocker" 

Step 2: Click to "Open"



Step 3: Under the "Operating system drive" section, ensure that you see "BitLocker on". If not, click on "Turn on BitLocker"



CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

1. Enable Multi-Factor Authentication (MFA) for Administrators

Step 1: From Microsoft 365 Admin Center, Go to “Home” > “Setup” > Protect your org with security defaults (MFA) > Click on “Manage”

To enable MFA for selected user

Step 2: From the list of users, select the user account to be activated with MFA by putting a tick against the user > Select “Enable”

Step 3: The following screen will be presented. Click on “enable multi-factor auth”, to enable MFA

The first screenshot shows the Microsoft 365 Admin Center navigation path: Home > Setup > Protect your org with security defaults (MFA). A pink circle with the number '1' highlights the 'Manage' button, which is also highlighted with a red box. A green 'Completed' status indicator is visible.

The second screenshot shows the 'multi-factor authentication users' page. A pink circle with the number '2' highlights the 'Enable' button in the user action menu for 'Eddy Tan', which is also highlighted with a red box. The table below shows the user list:

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/> Eddy Tan	Eddy@OrgA128.onmicrosoft.com	Disabled
<input type="checkbox"/> Edwin Leon	LeonEd@OrgA128.onmicrosoft.com	Disabled
<input type="checkbox"/> John Doe Smith	JD@OrgA128.onmicrosoft.com	Disabled

The third screenshot shows a dialog box titled 'About enabling multi-factor auth'. It contains the text: 'Please read the deployment guide if you haven't already.' and 'If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup'. A pink circle with the number '3' highlights the 'enable multi-factor auth' button, which is also highlighted with a red box. A 'cancel' button is also visible.

Additional Information:

- After the administrator has enabled MFA, users will be asked to set up verification details which is required to complete the MFA configuration.
- Users can choose to receive the verification code through a text message, call, or push notification via the Microsoft Authenticator app.

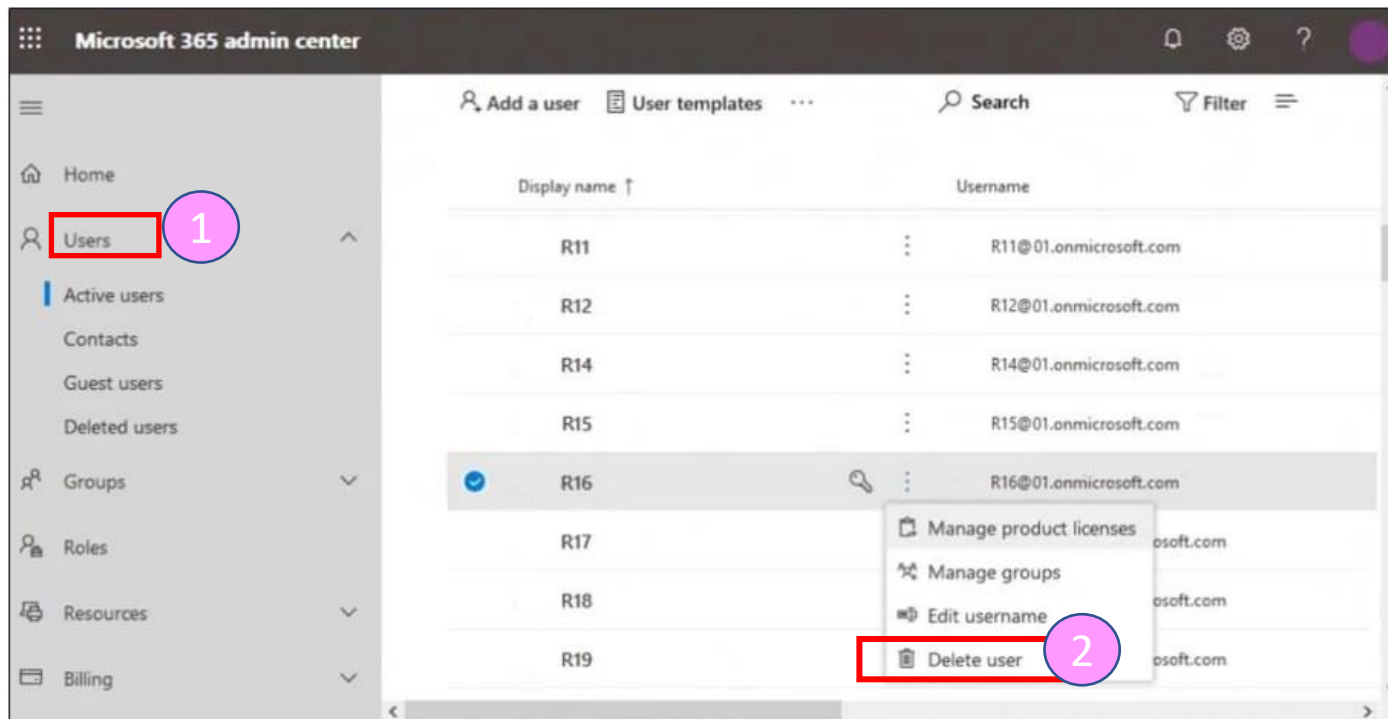
CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

2. Review of User Accounts

Regularly conduct periodic review of user accounts to ensure that unused accounts are removed.

Step 1: From Microsoft 365 Admin Center, Go to “Home” > “Users”

Step 2: Review the list of users, to see if any of them should be removed (e.g. employees who have left the organisation, etc.) If there is a user(s) to be removed, right-click on the user and select “Delete user”



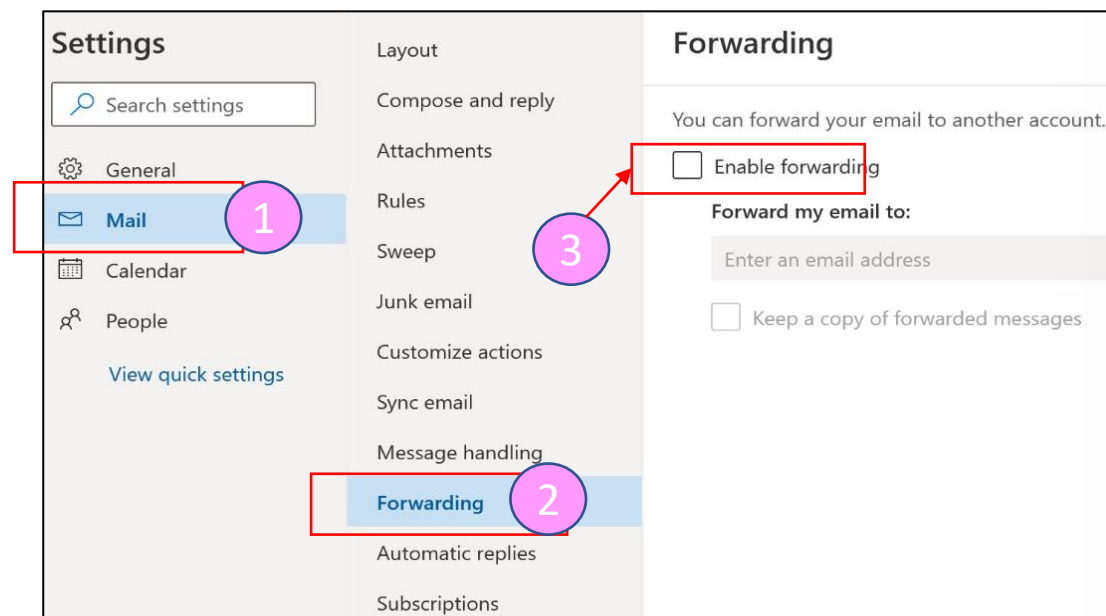
CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

3. Disable Email Auto Forwarding

Step 1: In the Outlook web client, Go to “Settings” and click on “Mail”

Step 2: Select “Forwarding”

Step 3: Ensure that the checkbox “Enable forwarding” is unchecked



Additional Information:

- Default setting for automatic forwarding to external email is turned off in M365, for enhanced security.
- It is recommended to disallow automatic forwarding if the user’s email account is often used for large amounts of personal data or personal data more likely to result in harm to individuals.
- For more information, visit <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide>

CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

4. Configure Folder Permissions for OneDrive

If you want to prevent external file sharing in Microsoft 365 Groups, you can turn off the external file sharing in the Microsoft 365 admin center.

To turn off external file sharing

Step 1: In the Microsoft 365 admin center, click "*Organisational profile*"

Step 2: Click "*SharePoint*"

Step 3: Ensure that the following checkbox is ticked, "*Only people in your organisation – no external sharing allowed*"

The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane shows the 'Organization profile' link highlighted with a red box and a pink circle containing the number '1'. The main content area shows the 'SharePoint' link highlighted with a red box and a pink circle containing the number '2'. Below this, a table lists various services, with the 'SharePoint' row highlighted by a red box. To the right, a 'SharePoint' configuration pane is open, showing the 'Users can share with:' section. The radio button for 'Only people in your organization – no external sharing allowed' is selected and highlighted with a red box and a pink circle containing the number '3'. Other options include 'Existing guests only', 'New and existing guests', and 'Anyone'. A yellow warning banner at the top of the pane states: 'Your Microsoft 365 Groups settings let people outside the organization access group content. These guests will receive an error when they try to access SharePoint content. Change Microsoft 365 Groups settings.'

CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

5. Manual Backup and Restore of Local Files

Note: Please ensure that your M365 OneDrive account is set-up

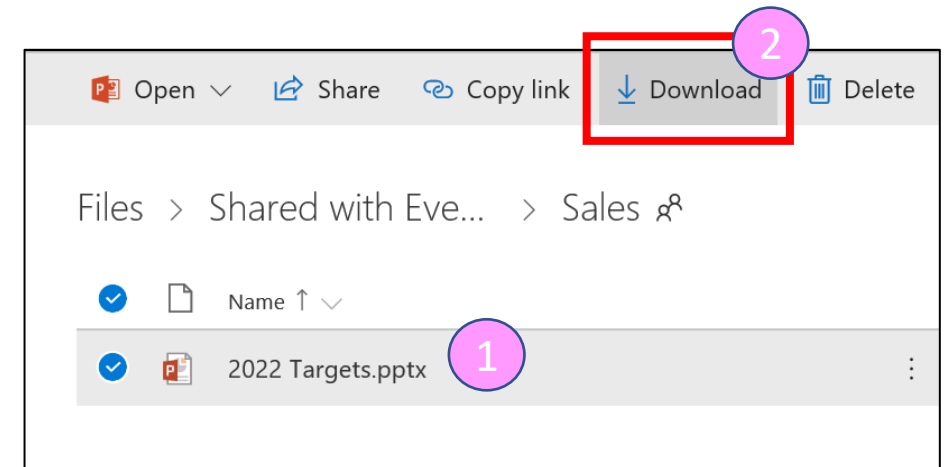
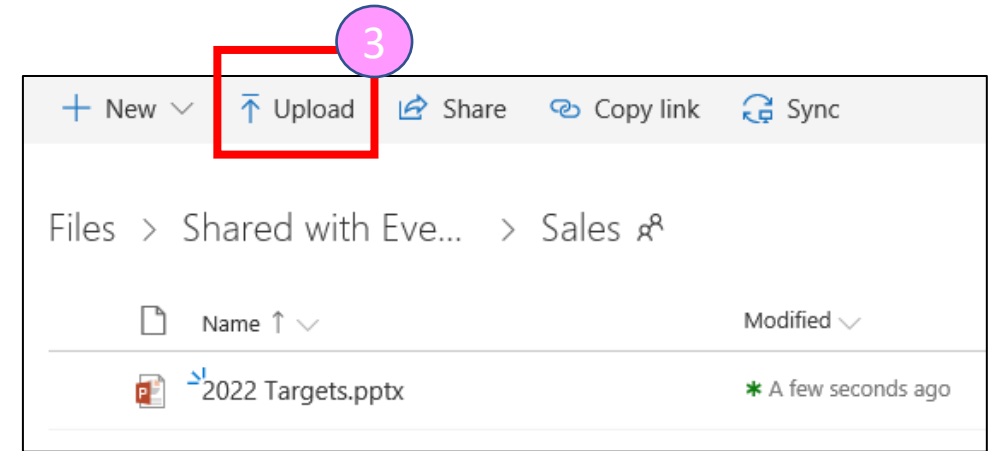
To backup from local device to M365 OneDrive:

- Step 1:** *Zip the folder/file that you wish to backup. Assign a password to the zipped file if necessary
- Step 2:** At OneDrive, navigate to the target folder for the backup file
- Step 3:** Click on “*Upload*” button in OneDrive and select the *zipped file from the previous step

** Step 1 & 2 on how to securely zip a file is covered under the Appendix*

To restore from M365 OneDrive to a local device:

- Step 1:** Select the backed up zipped file/file at M365 OneDrive
- Step 2:** Click on “*Download*”
- Step 3:** Unzip the file if necessary and key in the password if necessary and copy the file/folders to the target destination on your local device



CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

6. Restoring the Entire OneDrive

- All documents stored at OneDrive are automatically synchronised to another cloud location. This works like an automatic backup
- For restoration of data from backup, you can either restore your OneDrive (select from a day within the last 30 days), or restore a previous version of the selected file. This page shows the steps to restore your entire OneDrive

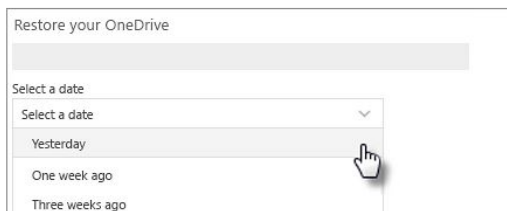
Restore OneDrive to a previous time

To restore your OneDrive, you'll need to have Microsoft 365. Otherwise, you'll be redirected to this article when you try to follow the steps below.

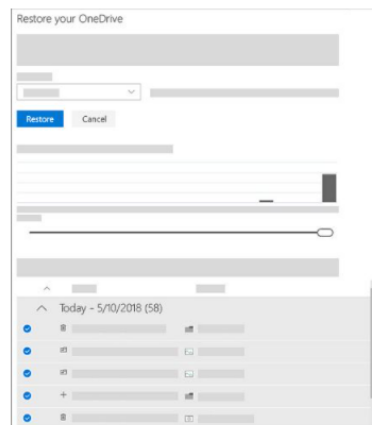
1. Go to the [OneDrive website](#). (Make sure you're signed in with the correct account.)
2. If you're signed in with:
 - A personal account with a Microsoft 365 subscription, at the top of the page, select **Settings** > **Options**, and then select **Restore your OneDrive** from the left navigation.
 - A work or school account, select **Settings** > **Restore your OneDrive**.

Note: The **Restore your OneDrive** option isn't available in the classic experience of OneDrive for work or school or without a Microsoft 365 subscription.

3. On the Restore page, select a date from the dropdown list—such as **Yesterday**—or select **Custom date and time**. If you're restoring your files after automatic ransomware detection, a suggested restore date will be filled in for you.



4. Use the activity chart and activity feed to review the recent activities that you want to undo.



The daily activity chart shows the volume of file activities in each day for the last 30 days. It gives you an overview of what has happened to your OneDrive over time and it can help you identify any unusual activities. For example, if your OneDrive was infected by malware, you can look for when it happened.

The activity feed shows individual file and folder operations in reverse chronological order. You can scroll down to see previous days, or move the slider below the daily activity chart to quickly move to a specific day.

Tip: Use the expand and collapse arrow next to each day in the activity feed to show or hide activities for that day.

5. If you selected **Custom date and time**, select the earliest activity that you want to undo. When you select an activity, all other activities that occurred after that are selected automatically.

Note: Before you select **Restore**, scroll to the top of the activity feed to review all the activities you are about to undo. When you pick a day in the activity chart, the more recent activities are hidden in the feed, but they're still selected when you select an activity.

5. If you selected **Custom date and time**, select the earliest activity that you want to undo. When you select an activity, all other activities that occurred after that are selected automatically.

Note: Before you select **Restore**, scroll to the top of the activity feed to review all the activities you are about to undo. When you pick a day in the activity chart, the more recent activities are hidden in the feed, but they're still selected when you select an activity.

6. When you're ready to restore your OneDrive, select **Restore**. This action will undo all the activities you selected.

Your OneDrive will be restored to the state it was in before the first activity you selected.

Note: If you change your mind about the restore you just did, you can undo the restore by running Files Restore again and selecting the restore action you just did.

Limitations and troubleshooting

- When version history is turned off, Files Restore can't restore files to a previous version. For information about versioning settings, see [Enable and configure versioning for a list or library](#). Files Restore uses version history and the recycle bin to restore OneDrive, so it's subject to the same restrictions as those features.
- You can't restore deleted files after they've been removed from the [site collection recycle bin](#)—either by manual delete or by emptying the recycle bin. A SharePoint site collection administrator may be able to view and restore those deleted items.
- Albums are not restored.
- If you upload a file or folder that you deleted, Files Restore will skip the restore operation for that file or folder.
- If some files or folders cannot be restored, a log file will be generated at the root folder of your OneDrive to capture the errors. The name of the file will begin with "RestoreLog" followed by an ID (for example, RestoreLog-e8b977ee-e059-454d-8117-569b380eed67.log). You can share the log file with our support team to troubleshoot any issues that may occur.

Source: <https://support.microsoft.com/en-us/office/restore-your-onedrive-fa231298-759d-41cf-bcd0-25ac53eb8a15>

CONFIGURATION GUIDE FOR MICROSOFT 365 (M365)

7. Restoring a Selected File

- All documents stored at OneDrive are automatically synchronised to another cloud location. This works like an automatic backup.
- For restoration of data from backup, you can either restore your OneDrive (select from a day within the last 30 days), or restore a previous version of the selected file. This page shows the steps to restore a selected file.

Restore a previous version of a file stored in OneDrive

OneDrive for Business, SharePoint Server Subscription Edition, [More...](#)

With version history, you can see and restore older versions of your files stored in OneDrive or SharePoint. Version history works with all file types, including Microsoft 365 files, PDFs, CAD files, photos, videos, and more. If you need to, you may be able to [restore deleted OneDrive files](#) or [restore deleted SharePoint items](#) from the recycle bin.

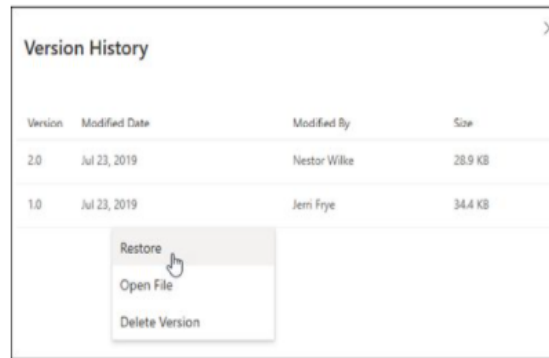
Tip: You can also [View previous versions of Office files](#) in Office apps.

1. Sign in to OneDrive with your personal Microsoft account or your work or school account.
2. Select the file that you want to restore to an earlier version (you can only restore one file at a time), right-click, then select **Version history**.

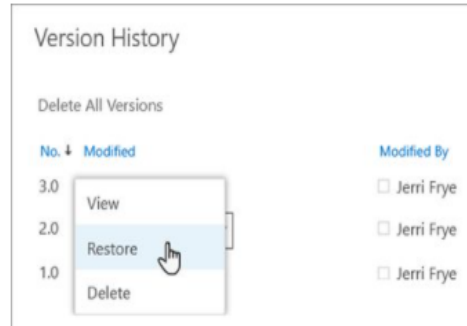
Note: In Classic view, select the document, then at the top, select **More > Version History**.

3. In the **Version History** pane, do one of the following:

If you're signed in to OneDrive or SharePoint with a work or school account (such as a Microsoft 365 account), select the ellipses (...) next to the version of the document that you want to restore, and then click **Restore**.

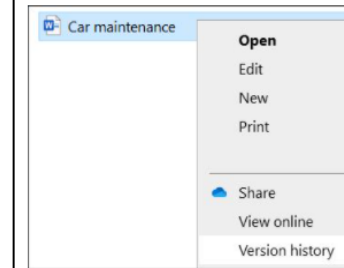


In Classic view or previous versions of SharePoint Server, select the arrow next to the version of the document that you want to restore, and then click **Restore**.



Use Version history in File Explorer

If you have the OneDrive [sync app](#) installed on your PC, right-click the file that you want to restore to an earlier version in File Explorer and select **Version history**. Then select the ellipses (...) next to the version you want and click **Restore**.



The document version you selected becomes the current version. The previous current version becomes the previous version in the list.

Notes:

- If you sign in with a personal Microsoft account, you can retrieve the last 25 versions. If you sign in with a work or school account, the number of versions will depend on your [library configuration](#).
- If you're using OneDrive as part of SharePoint Server, your administrator may have turned off document versioning. For more information about SharePoint versioning settings (which also apply to OneDrive for work or school) see [Enable and configure versioning for a list or library](#) or [How does versioning work in a list or library?](#)
- If you're signed in to OneDrive with a Microsoft account, items in the recycle bin are automatically deleted 30 days after they're put there. If your recycle bin is full, the oldest items will be automatically deleted after three days. If you're signed in with a work or school account, items in the recycle bin are automatically deleted after 93 days, unless the administrator has changed the setting. See more information about [how long deleted items are kept](#) for work or school accounts.

Source: <https://support.microsoft.com/en-us/office/restore-a-previous-version-of-a-file-stored-in-onedrive-159cad6d-d76e-4981-88ef-de6e96c93893>

Configuration Guide to Minimise Common Data Breach Issues for Google Workspace

09 MAY 2022

Supported by

In supported of

Getting Started

This quick-start configuration guide is to help businesses minimise common breach issues through good security practices in Google Workspace, using these simple configuration steps.

The guide is for organisations using Google Workspace (“GWS”) Business Standard edition through Windows devices. Some of the settings are to be configured at GWS, while others are to be configured at the Windows devices (“@Windows Device”).

Windows 10 Enterprise is used as the reference version for the steps and screenshots shared.

(Note: This guide does not include the initial setup process such as planning and deploying your tenant, apps, and services.)

Contents

WINDOWS DEVICE SETTINGS

1. [Strong Password Settings](#)
2. [How to Turn On Bitlocker Disk Encryption](#)

GWS SETTINGS

1. [Enable Multi-Factor Authentication \(MFA\) for Administrators](#)
2. [Strong Password Settings \(for GWS\)](#)
3. [Disable Email Forwarding](#)
4. [Review of User Accounts](#)
5. [Configure Folder Permissions for Google Drive](#)
6. [Manual Back-Up of Local Files from Windows device to GWS](#)
7. [Restoring a Selected File from GWS](#)

APPENDIX

[How to Securely Zip a File](#)

CONFIGURATION GUIDE FOR GOOGLE WORKSPACE

1. Strong password settings (@Windows device)

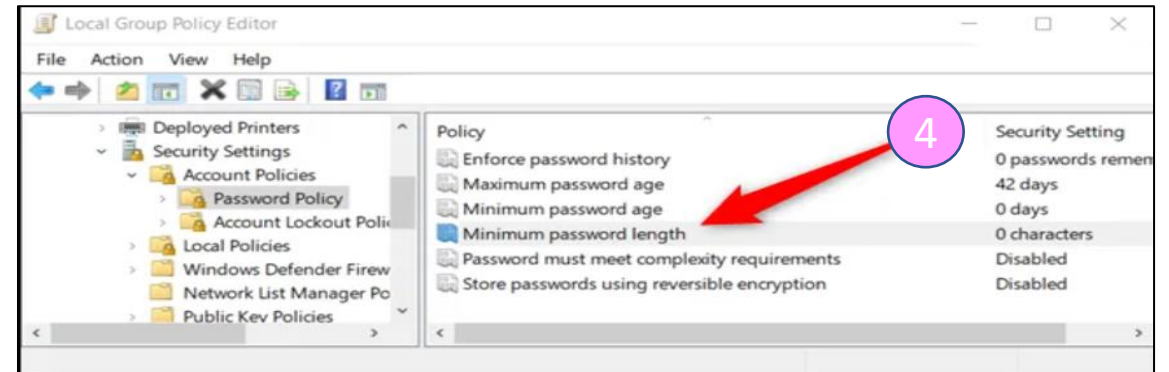
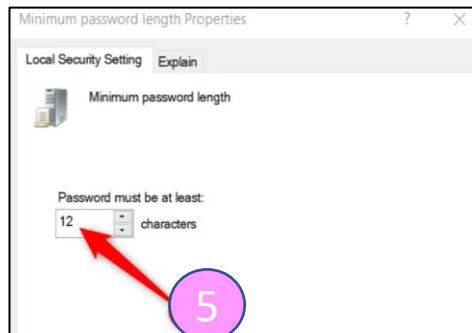
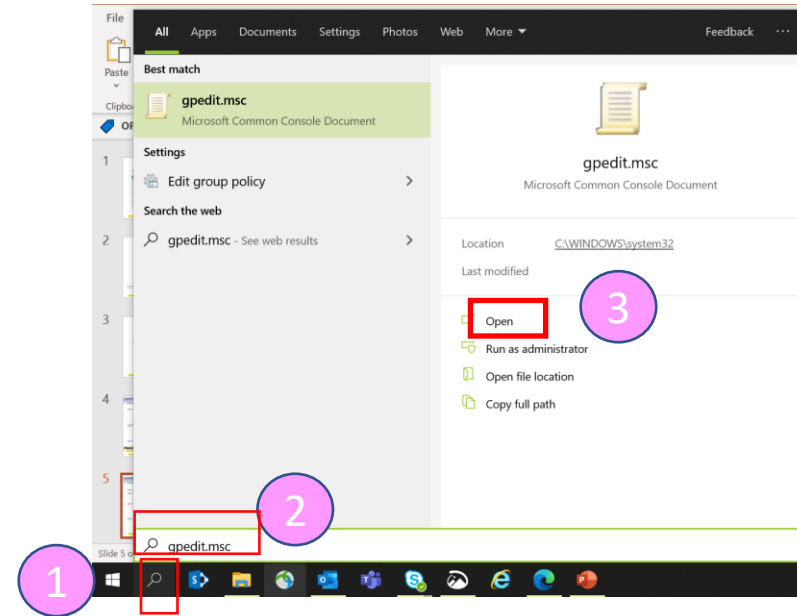
Step 1: Launch the group policy editor by pressing Windows+R

Step 2: Type “gpedit.msc” and press “Enter”

Step 3 Click to “Open”

Step 4: Navigate to Computer configuration > “Windows settings” > “Security settings” > “Account policies” > “Password policy” > “Minimum password length”

Step 5: Set the minimum password length to 12 characters

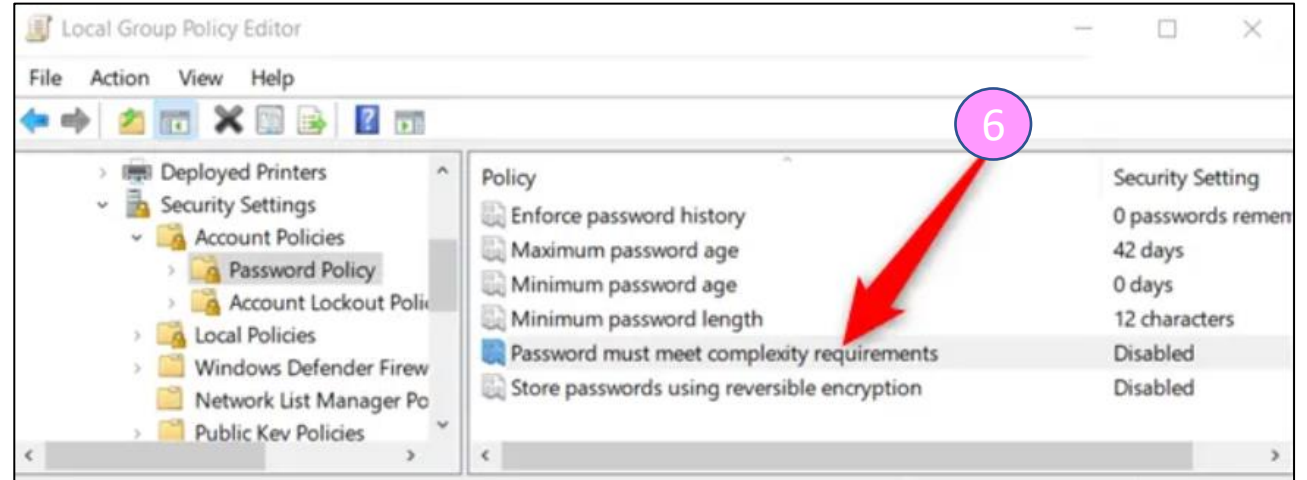


CONFIGURATION GUIDE FOR GOOGLE WORKSPACE

2. Strong password settings – Cont'd (@Windows device)

Step 6: Click to enable password complexity requirements, to facilitate users in creating a secure password

Step 7: Restart your computer after making the policy changes




Enabling the complexity requirements means:

- DO NOT contain the user account name or full name
- Be at least 6 characters in length and contain characters from at least 3 of the following 4 categories:
 - Uppercase English letters (A-Z)
 - Lowercase English letters (a-z)
 - Base 10 digits (0-9)
 - Non-alphabetic characters (such as \$, !, %)

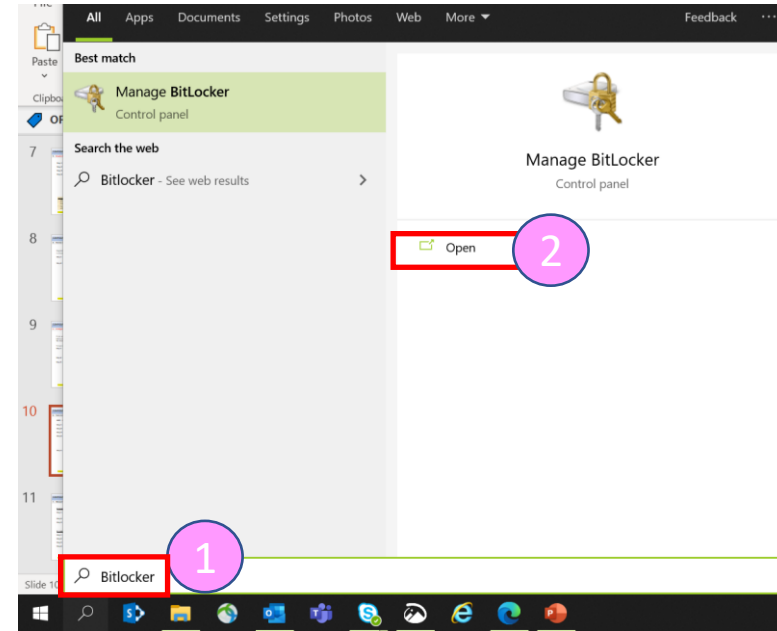
CONFIGURATION GUIDE FOR GOOGLE WORKSPACE

2. How to Turn on BitLocker Disk Encryption (@Windows device)

NOTE: For Windows 10, BitLocker is available on the Pro and Enterprise editions only

Step 1: Click on the magnifying glass and type “Bitlocker” 

Step 2: Click to “Open”



Step 3: Under the "Operating system drive" section, ensure that you see “BitLocker on”. If not, click on “Turn on BitLocker”



CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

1. Enable Multi-Factor Authentication (MFA) for Administrators

Step 1: From the Google Admin console, sign in using an administrator account

Step 2: Go to “Security Settings” > “2-Step Verification”

Step 3: Select an organisational unit or exception group

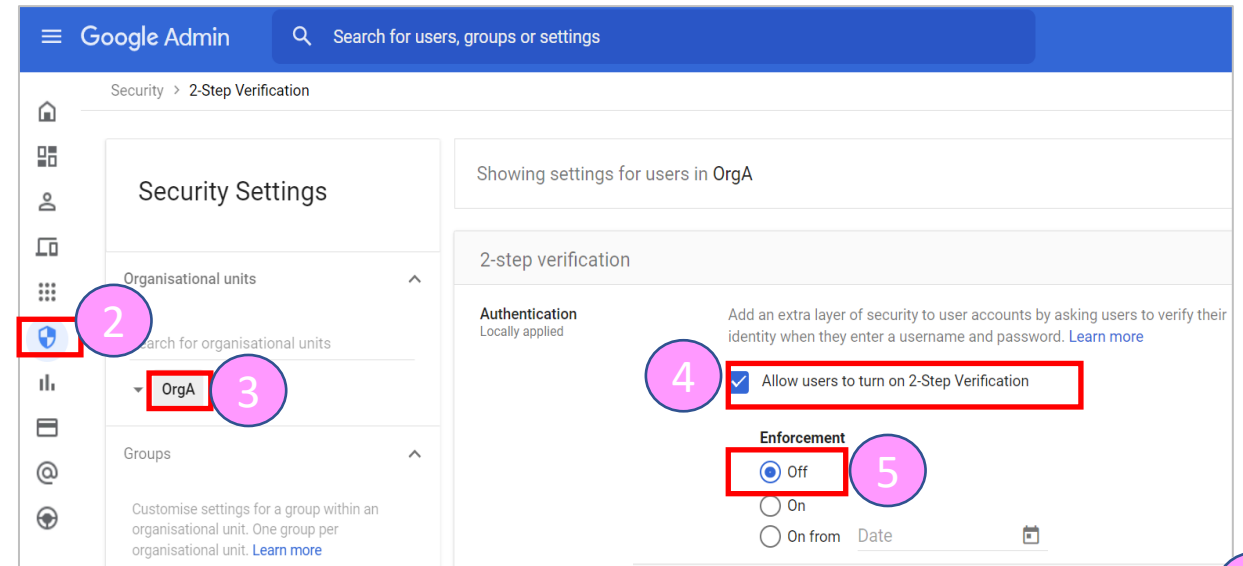
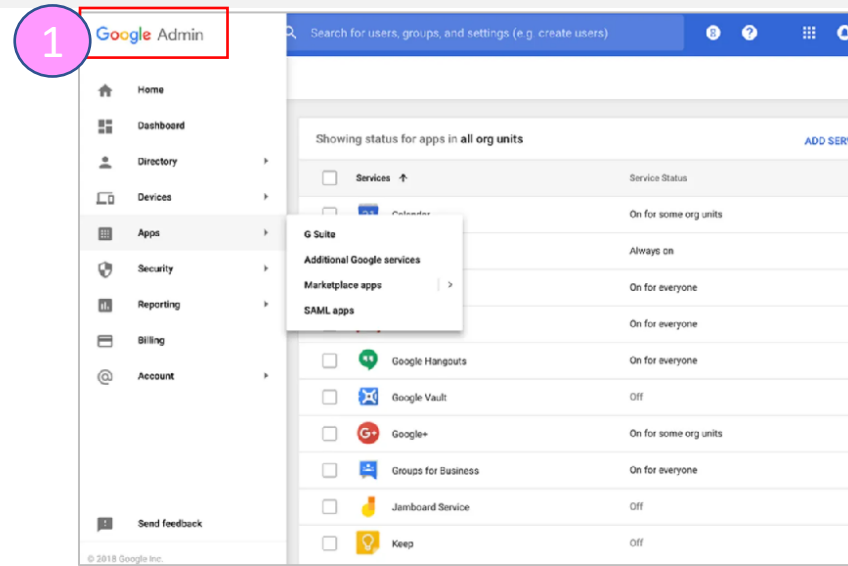
Step 4: Check “Allow users to turn on 2-Step Verification”

Step 5: Select “Enforcement” > “Off”

Step 6: Click ‘Save’

Additional information:

- You can use the following for MFA:
 - Security keys
 - Google prompt
 - Google Authenticator app
 - Backup codes
 - Text message or phone call
- More Information can be found under this [link here](#).
- GWS security checklist can be found here: [link here](#).



CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

2. Strong Password Settings

Step 1: From the Google Admin console, go to “*Security Settings*” > “*Password management*”

Step 2: Under Length, configure minimum length to 12 characters

The screenshot shows the Google Admin console interface. The top navigation bar includes the Google Admin logo and a search bar. The main content area is titled 'Security > Password Management' and shows settings for 'OrgA'. The 'Password management' section is expanded, showing 'Password management' (Locally applied) and 'Configure password policies for your organisation'. A yellow information box states: 'These policies don't apply in some cases, such as when users are authenticated by a third-party identity provider. [Learn more](#)'. Under the 'Length' section, it says 'Must be between 8 and 100 characters'. The 'Minimum length' field is set to 12, and the 'Maximum length' field is set to 100. A red box highlights the '12' in the 'Minimum length' field, and a pink circle with the number '2' is next to it. In the left sidebar, the 'Security Settings' link is highlighted with a red box, and a pink circle with the number '1' is next to it.

Additional information:

- Enforce a password history policy to ensure that employees do not reuse their previous passwords.
- Encourage users to use passphrases such as “Iwant2l@se10kg”, which may be long and complex, yet easy to remember.
- Discourage users from using the same passwords across different systems.


CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

3. Disable Email Automatic Forwarding

It is recommended to disallow automatic forwarding if the user's email account is often used for large amounts of personal data or personal data more likely to result in harm to individuals

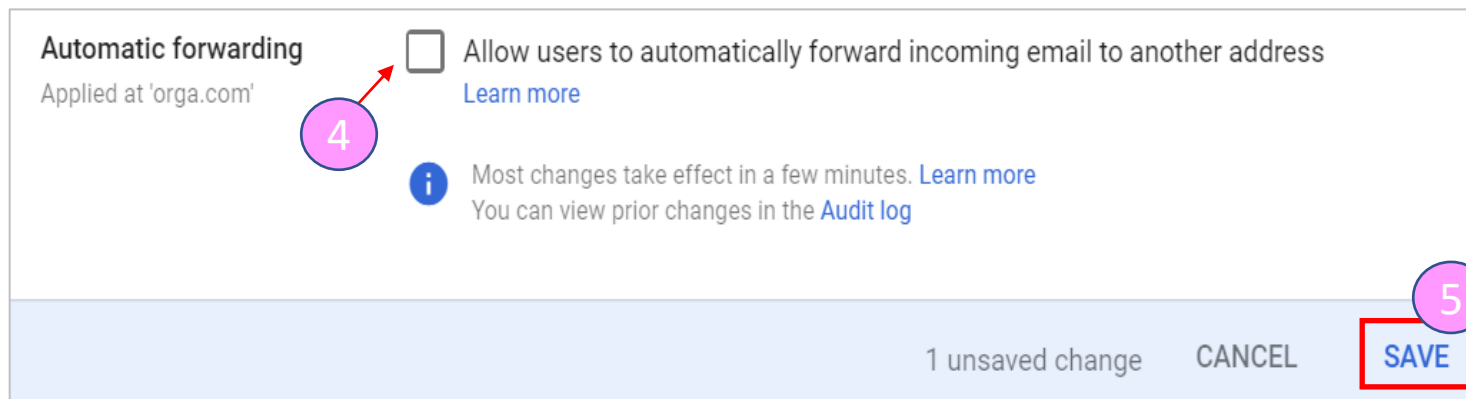
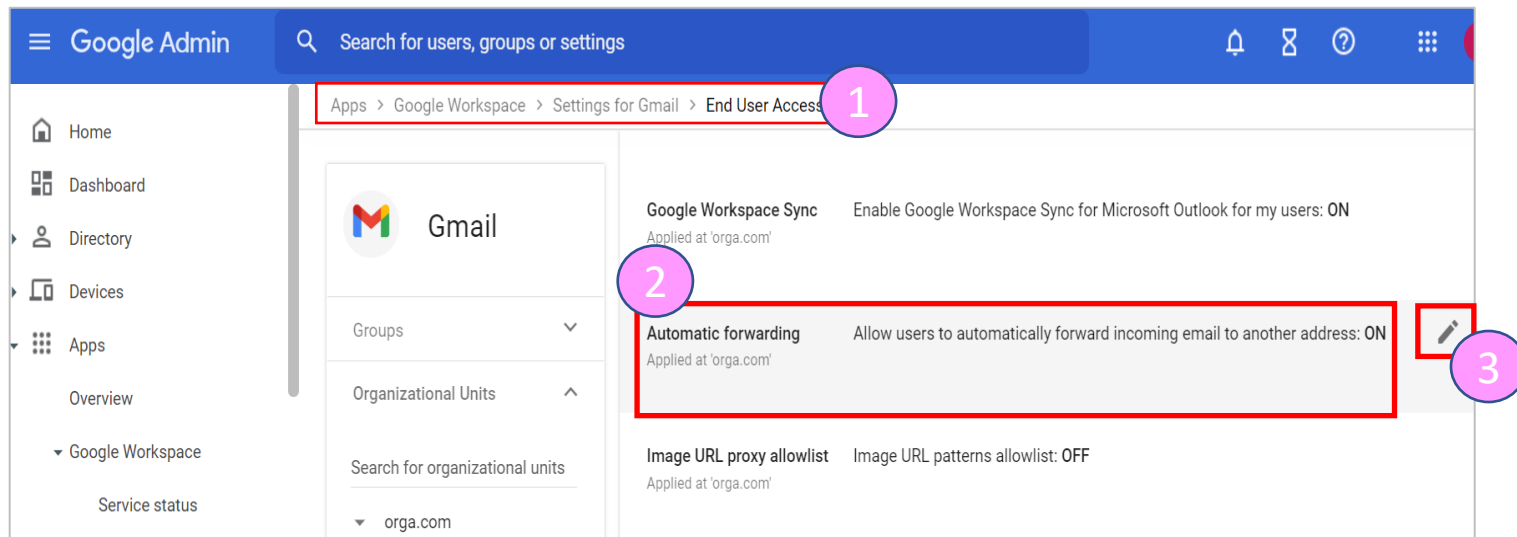
Step 1: Go to Apps > "Google Workspace" > Settings for Gmail > "End User Access"

Step 2: Go to "Automatic forwarding"

Step 3: Click on the pencil icon to edit 

Step 4: Uncheck the checkbox at the "Automatic Forwarding" section to disable mail forwarding feature (i.e. if user is handling sensitive personal data in his/her daily work)

Step 5: Click "Save"



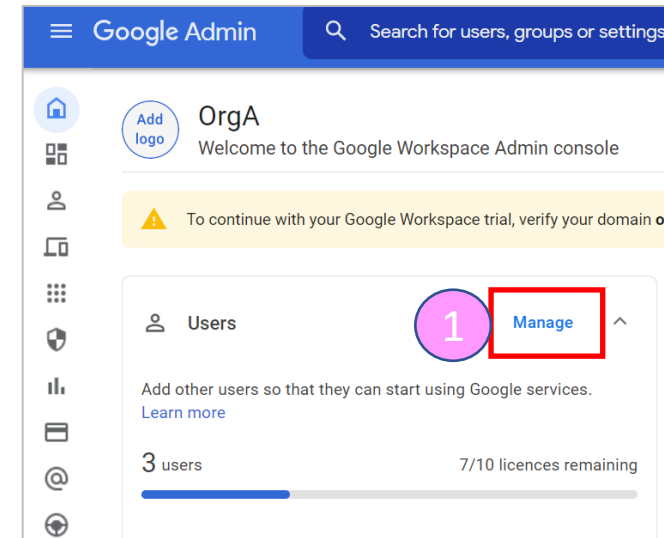
CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

4. Review of User Accounts

Regularly conduct periodic review of user accounts to ensure that unused accounts are removed.

Step 1: From the Google Admin Page, Go to “Users” > “Manage”

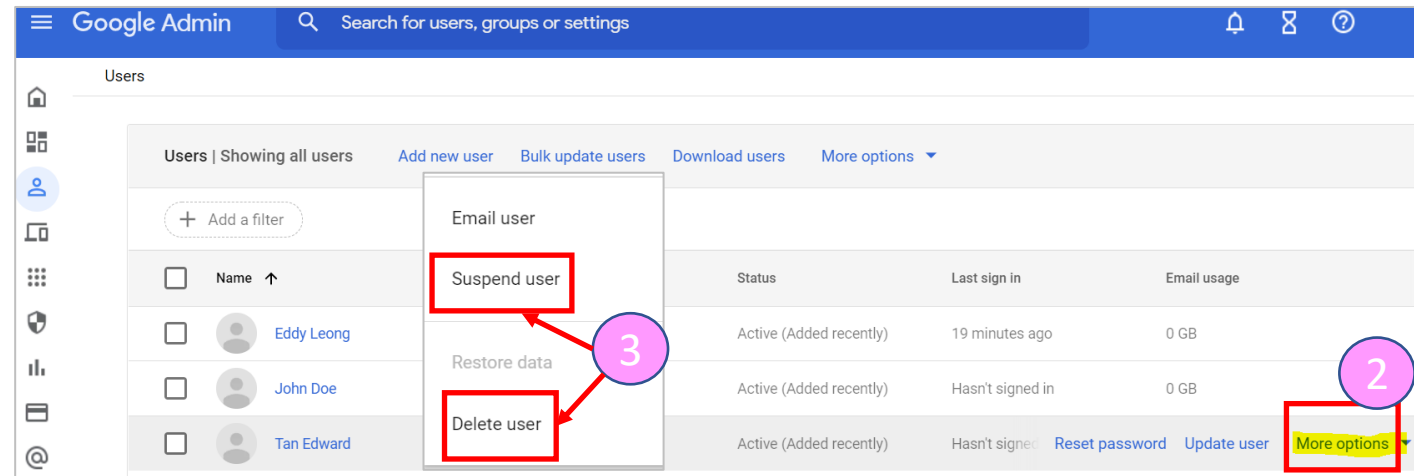
Check through the list of users, to see if any of the users should be removed (e.g. employees who have left the organisation, etc.)



If there is a user(s) to be removed,

Step 2: Select “More options”

Step 3: Select “Delete user”. Alternatively, select “Suspend user” first, for example if there is a need for the administrator to save out user data




CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

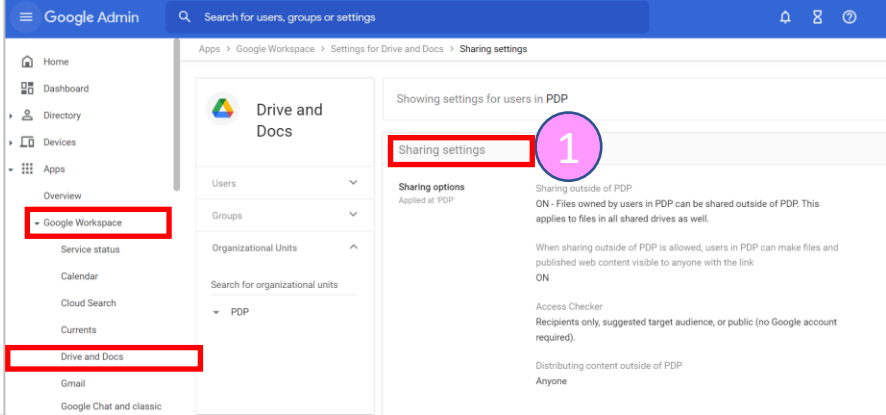
5. Configure Folder Permissions (For Google Drive)

Turn off sharing with external parties to prevent accidental sharing with unintended parties or the general public.

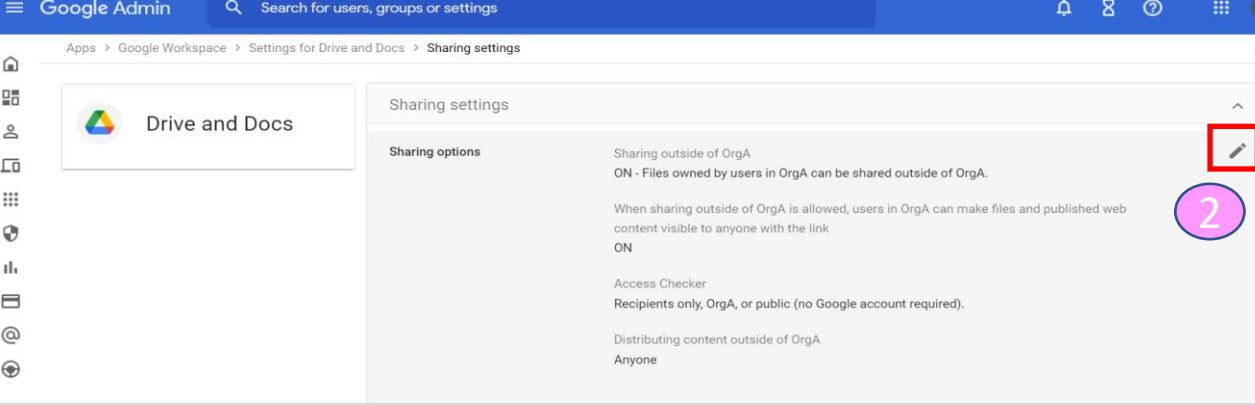
Step 1: Go to Google Admin > “Apps” > “Google Workspace” > “Settings for Drive and Docs” > “Sharing settings”

Step 2: Click on the pencil icon 

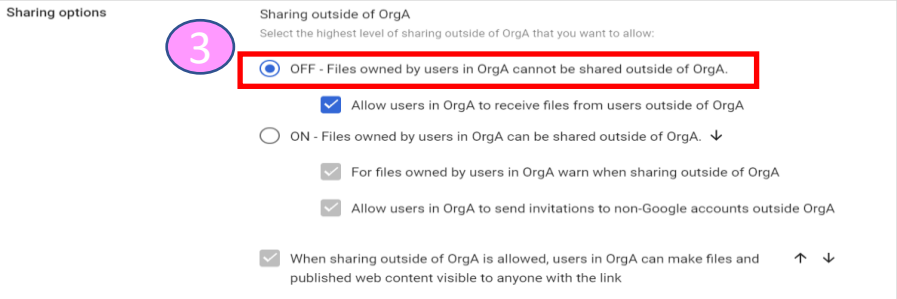
Step 3: Select ‘OFF’ to disallow sharing outside your organisation



The screenshot shows the Google Admin console interface. The left sidebar has 'Google Workspace' and 'Drive and Docs' highlighted with red boxes. The main content area shows 'Sharing settings' for users in PDP, with a red box around the 'Sharing settings' link and a pink circle with the number '1' next to it.



The screenshot shows the 'Sharing settings' page for Drive and Docs. A red box highlights the pencil icon in the top right corner, and a pink circle with the number '2' is next to it.



The close-up screenshot shows the 'Sharing options' section. A red box highlights the 'OFF - Files owned by users in OrgA cannot be shared outside of OrgA.' radio button, and a pink circle with the number '3' is next to it.

CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

6. Manual Backup of Local Files from Windows device to GWS

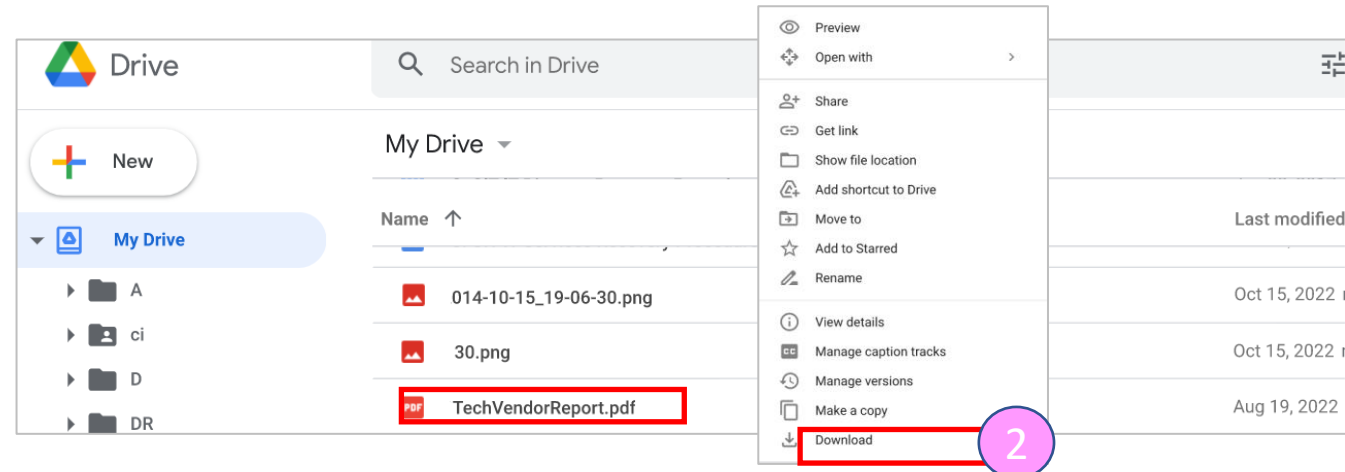
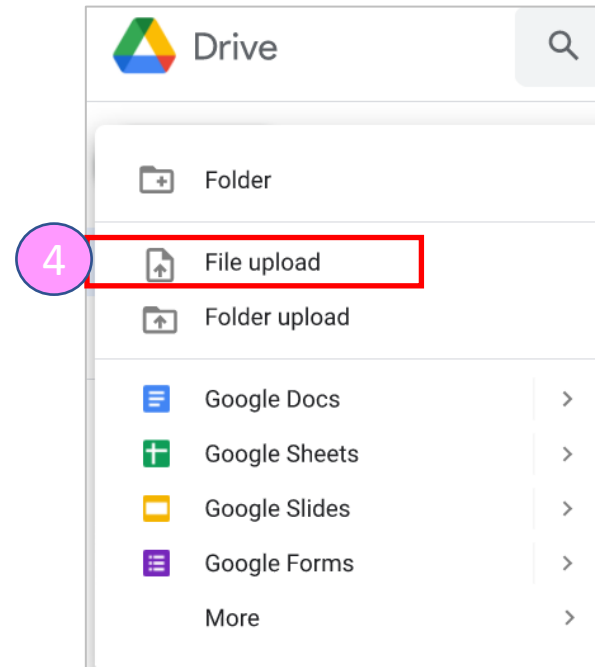
* How to securely zip a file is covered under the Appendix

To **backup** from a local device to Google Drive:

- Step 1:** *Zip the local files/folder that you wish to backup
- Step 2:** Assign a password to the *zipped file if necessary
- Step 3:** At Google Drive, navigate to the target folder for the backup file then click on “File Upload”
- Step 4:** Select the *zipped file from your local drive that you wish to upload

To **restore** from Google Drive to a local device:

- Step 1:** Select the backed up zip file/folder in Google Drive
- Step 2:** Right-click on the file and select “Download”
- Step 3:** Unzip the file, key in the password if necessary and copy the file/folders to the target destination on your local device



CONFIGURATION GUIDE FOR GOOGLE WORKSPACE (GWS)

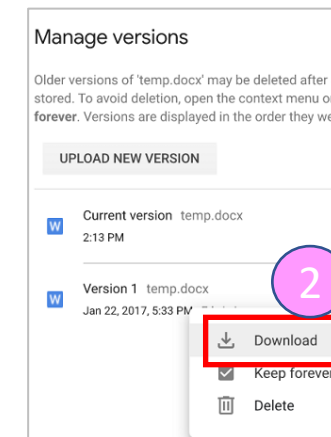
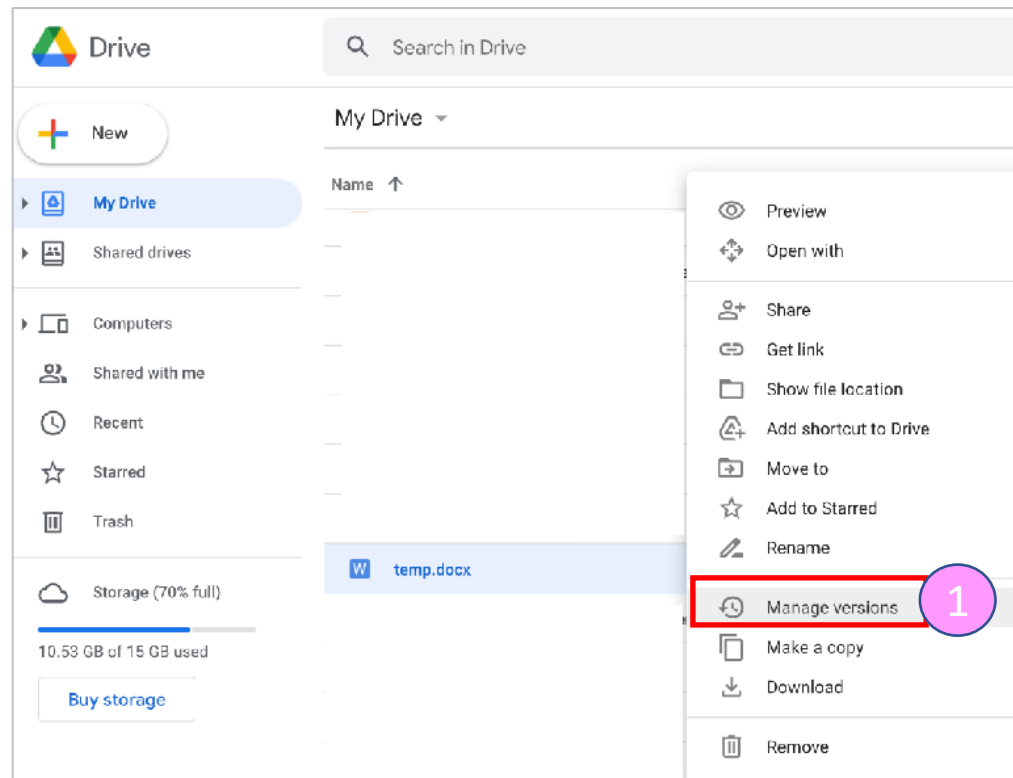
7. Restoring a Selected File from GWS

All documents stored at Google Drive are automatically synchronised to another cloud location. This works like an automatic backup. For restoration of data from backup, you can restore a previous version of the selected file.

To restore a selected file

Step 1: In Google Drive, right-click on selected file > “*Manage versions*”

Step 2: Select the desired version of the file to restore, and click “*Download*”



APPENDIX: HOW TO SECURELY ZIP A FILE

A. USING 7-ZIP

To zip a file

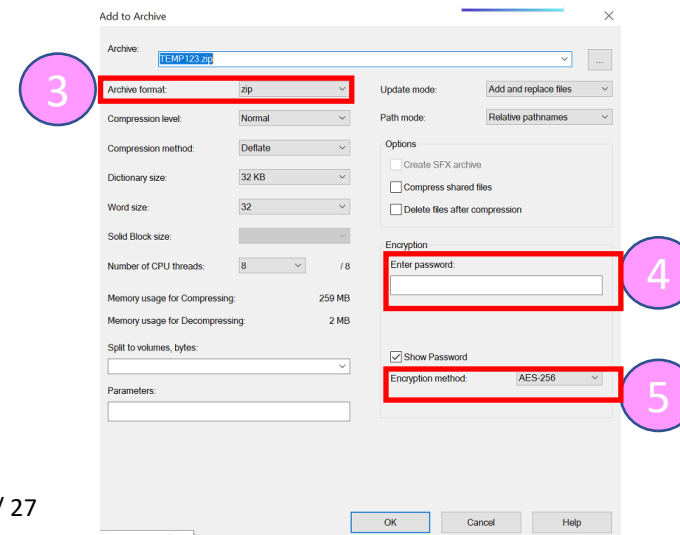
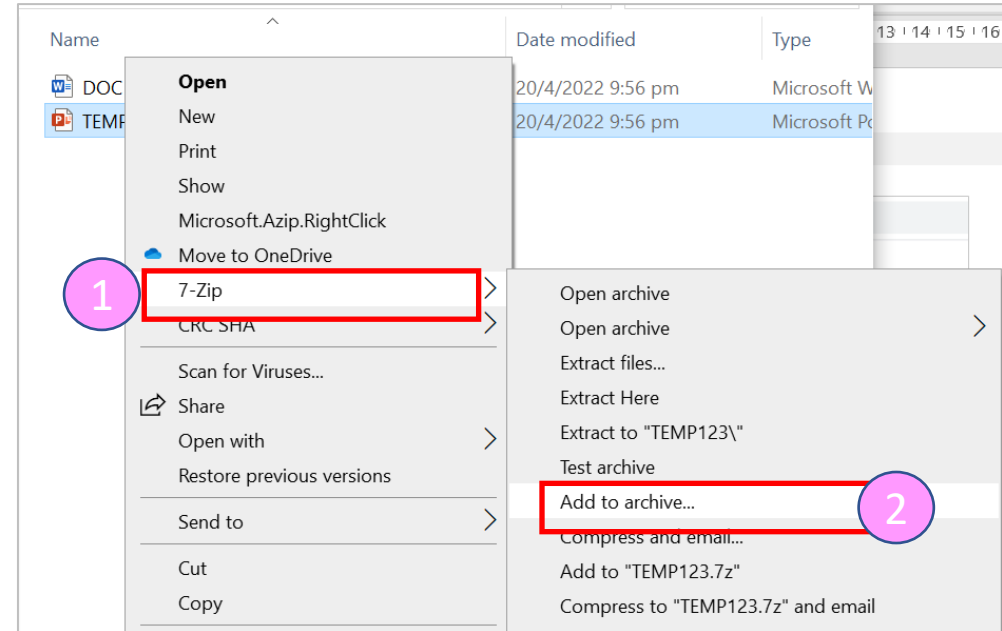
Step 1: Right-click on the selected to be zipped and select “7-Zip”

Step 2: Select “Add to archive”

Step 3: Ensure Archive format is “Zip”

Step 4: Enter password for the zip file

Step 5: Select encryption method as “AES 256”



www.imda.gov.sg/dpe

Copyright 2022 – Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC)

The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The IMDA, PDPC and their members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights and may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.

Supported by



In supported of

