



Australian Government
Digital Transformation Agency

Data Loss Prevention - Standard Operating Procedure

March 2020

Contents

Document Overview 4

 Background 4

 Document Audience..... 4

 Purpose 4

 Prerequisites 4

 Associated Documentation 5

Data Loss Prevention..... 6

 Implement New Policy 6

 Modify Existing Policy 10

Abbreviations and Acronyms.....12

Document Overview

Background

Data loss prevention (DLP) is a security feature within Office 365 that, when configured correctly, will identify and protect Agency data and other sensitive information. DLP will ensure the information is only made available to the intended authorised users of the information.

Document Audience

This Standard Operating Procedure (SOP) is intended to support the ongoing operation of the Data Loss Prevention (DLP) capability of Office 365 which is enabled for the Digital Transformation Agency (DTA) Blueprint. It includes the required steps that a suitably trained administrator should follow to maintain the operational state of the solution.

The services and settings provided by the Blueprint should not be modified without fully understanding the security and operational consequence of the change.

Purpose

The purpose of this document is to provide the necessary steps to administer DLP within the Microsoft 365 Compliance Center.

Prerequisites

Before completing the procedures detailed in this document, the following prerequisites should be met:

- It is recommended that the reader/administrator performing the procedures in the document has certification and/or experience with Office 365 and Microsoft Azure.
- Identified their sensitive info types, classification labels/types, and retention labels.

Associated Documentation

Table 1 identifies the documents that should be referenced and understood before administering this solution

Table 1 Associated Documentation

| Name | Version | Date |
|--|---------|---------|
| DTA – Solution Overview | March | 03/2020 |
| DTA – Platform Design | March | 03/2020 |
| DTA – Workstation Design | March | 03/2020 |
| DTA – Office 365 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 |

Data Loss Prevention

Within the Microsoft 365 Compliance Center DLP policies can be configured to identify and protect Agency data and other sensitive information. DLP can be configured for multiple applications, such as:

- Exchange Online,
- SharePoint Online,
- OneDrive for Business, and
- Microsoft Teams.

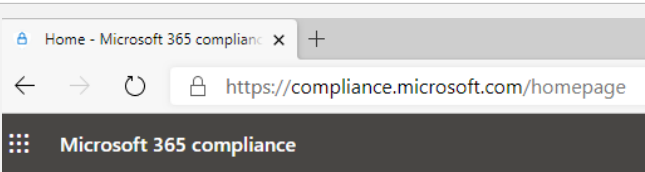
The following sections describe how to maintain and manage DLP and its policies, including the creation of new policies.

Implement New Policy

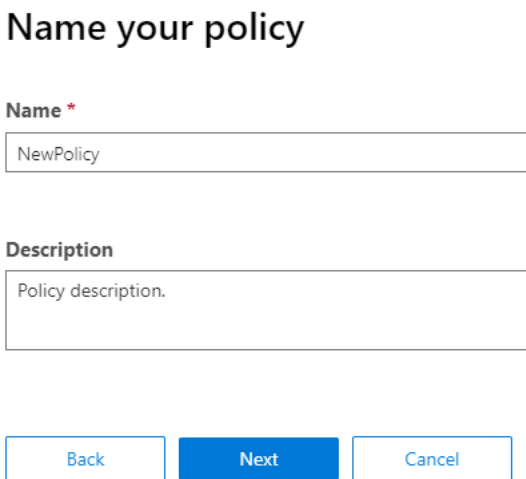
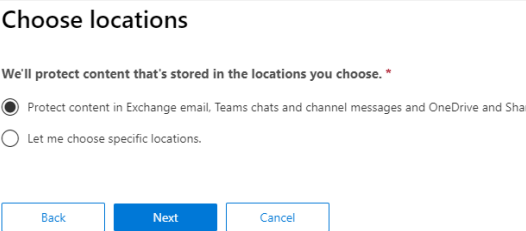
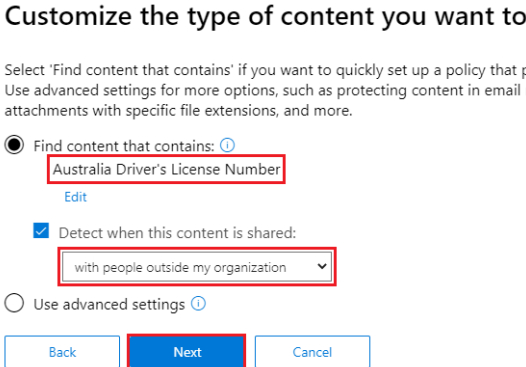
The following table describes how to implement a new DLP policy.

This example describes the scenario where an Agency wants to implement a DLP rule to prevent emails or other information containing Australian driver's license numbers is not shared with unauthorised users.

Table 2 Implement New Policy

| Step | Instruction | Screenshot |
|------|--|--|
| 1. | Open an internet browser and navigate to the Microsoft 365 Compliance Center. https://compliance.microsoft.com/ |  |

| Step | Instruction | Screenshot |
|------|---|--|
| 2. | In the left-hand pane, click Policies | |
| 3. | Within the Policies window, click on Data loss prevention | |
| 4. | Within the Data loss prevention window, click Create policy | <div><h3>Data loss prevention</h3><p>Use data loss prevention (DLP) policies to help identify ar email and docs isn't shared with the wrong people. Learn</p><div><div>+ Create policy</div><div>↓ Export</div><div>↻ Refresh</div></div><div><div>Name</div><div>Australia Privacy Act</div><div>Australia Personallv Identifiable Information (PII) Data</div></div></div> |
| 5. | Click Next | |

| Step | Instruction | Screenshot |
|------|--|--|
| 6. | <p>On the Name your policy page, enter a Name and Description. Enter as detailed a description as possible.</p> <p>When complete press Next</p> |  |
| 7. | <p>On the Choose locations page, select the relevant radio button based on what the policy is protecting.</p> <p>When complete press Next</p> |  |
| 8. | <p>On the Customize the type of content you want to protect page, select the content type you wish to protect and where it is protected from.</p> <p>In this example we are detecting Australian Driver's Licence Numbers when shared outside of the organisation.</p> <p>When complete press Next</p> |  |

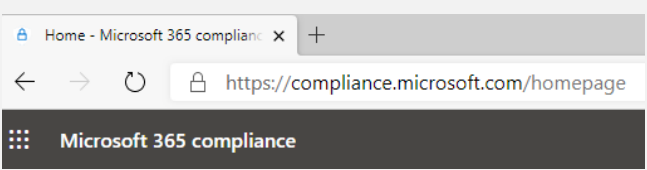
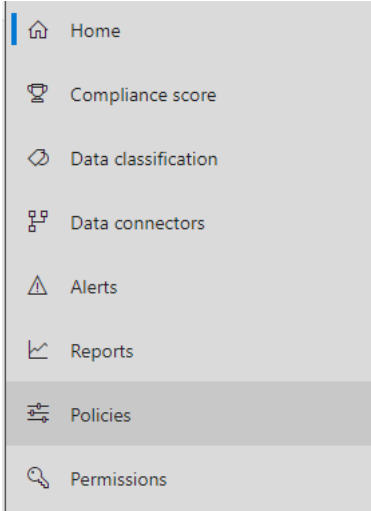
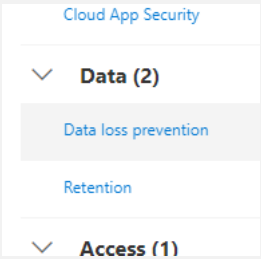
| Step | Instruction | Screenshot |
|------|---|------------------------|
| 9. | Select the appropriate settings on the next page as relevant to your policy. When complete press Next | |
| 10. | If prompted to customise access and override permissions, do so as appropriate | No screenshot required |
| 11. | When prompted to turn the policy on, or test first, it is suggested to always test policies first – as such, select I'd like to test it out first then press Next | |
| 12. | Review your settings, if they all look correct, click Create | |
| 13. | Allow some time for the policy to run. | No screenshot required |



Modify Existing Policy

The following table describes the steps required to modify an existing DLP policy within the Microsoft 365 Compliance Center.

The default DLP settings provided by the Blueprint should not be modified without fully understanding the security and operational consequence of the change.

Table 3 Modify Existing Policy

| Step | Instruction | Screenshot |
|------|--|--|
| 1. | Open an internet browser and navigate to the Microsoft 365 Compliance Center. https://compliance.microsoft.com/ |  |
| 2. | In the left-hand pane, click Policies |  |
| 3. | Within the Policies window, click on Data loss prevention |  |

| Step | Instruction | Screenshot | | | | | | | | | | |
|---|--|---|------|--|-----------------------|---|---|---|---|---|---|---|
| 4. | Within the Data loss prevention screen identify the policy you wish to modify, tick the radio button on its left, then click Edit policy | <div><h2>Data loss prevention</h2><p>Use data loss prevention (DLP) policies to help identify and protect sensitive information in email and other data sources.</p><div><div>+ Create policy</div><div><div><div> Edit policy</div><div> Delete policy</div></div></div></div><table><thead><tr><th>Name</th><th></th></tr></thead><tbody><tr><td>Australia Privacy Act</td><td>:</td></tr><tr><td>Australia Personally Identifiable Information Act</td><td>:</td></tr><tr><td>Australia Health Records Act (HRIP Act)</td><td>:</td></tr><tr><td><input checked="" type="checkbox"/> Detect Australian Drivers licence numbers</td><td>:</td></tr></tbody></table></div> | Name | | Australia Privacy Act | : | Australia Personally Identifiable Information Act | : | Australia Health Records Act (HRIP Act) | : | <input checked="" type="checkbox"/> Detect Australian Drivers licence numbers | : |
| Name | | | | | | | | | | | | |
| Australia Privacy Act | : | | | | | | | | | | | |
| Australia Personally Identifiable Information Act | : | | | | | | | | | | | |
| Australia Health Records Act (HRIP Act) | : | | | | | | | | | | | |
| <input checked="" type="checkbox"/> Detect Australian Drivers licence numbers | : | | | | | | | | | | | |
| 5. | When the editing pane shows up, make the required changes then press Save | <div><div>Save</div><div>Cancel</div></div> | | | | | | | | | | |

Abbreviations and Acronyms

Table 4 details the abbreviations and acronyms used throughout this document.

Table 4 Abbreviations and Acronyms

| Acronym | Meaning |
|---------|-------------------------------|
| DLP | Data Loss Prevention |
| DTA | Digital Transformation Agency |
| SOP | Standard Operating Procedure |