Microsoft Information Protection & Data Loss Prevention Kick-Start Guide

MSFTCOMPLIANCE.COM

Information Protection & DLP Kick-Start Guide

I have been working within Microsoft Compliance for several years now and I enjoy it. I get to work with all types of organisations within most industries some that are working under strict regulations and some that are not but want to protect business data. It provides me with a chance to learn something new every day. As a result, I like to have information to hand when talking to customers or colleagues, subsequently, I created this guide to share as much information as I could in an email or chat without having to stall or even leave the call to go look for what I needed.

As a result, due to me being able to quickly share it, we could continue discussing the topic whilst reviewing the information. Thereafter, once the call had finished those in the meeting had the kick-off guide to support them in building out their understanding for planning MIP & DLP, additionally providing advice on creating designs and configuring requirements. Therefore, the guide is a collection of links that will assist you in navigating the Microsoft Information Protection, Data Loss Prevention Solutions. In addition, providing information on the linking solutions and features in a single place.

Wanting to share as much information with people as I can is great. However, due to the wide scope of the solutions and the complexities they are built with, this means there is a great deal of information for evaluation. Consequently, it is often difficult to find links and information specific to your requirements. Don't get me wrong, Microsoft Docs are brilliant, and they certainly provide us with the information we seek. Nevertheless, at times it can be hard to find within the millions of pages and links to search through so, I often find myself spending lots of time 'searching' rather than 'doing'. And so, therefore, this is the reason I created this Kick-Start Guide for myself which I am now going to share with you.

Having this at hand has been a huge help to them and me! Therefore, I hope this guide will provide you with the same advantages as it has me.

This guide offers you the resources to; learn the solutions, get started with the solutions, compose designs and Labelling Taxonomies. Prepare for and implement configurations to provide the best protection for business-sensitive data. In addition to all this, I will offer a few words on each of the areas providing a brief introduction and where applicable share my experiences.

Where relevant I have included the license type needed for each solution and or feature. This is displayed by the following: E3 meaning an E3 License required or E5 meaning an E5 License required. Yes, Microsoft offers Bolt-On Licenses, however, to make things as easy as possible I have not included them as license options in this document. They are, however, outlined in the M365 Licensing Matrix should you need to check entitlements.

This guide will cover: - Information Protection; Sensitivity Labelling – Auto Labelling and Manual Labelling, Labelling Client Versions, Data Loss Prevention, EndPoint Data Loss Prevention, Data Discovery; Cloud & On-Premises, Data Analysis, Data Reporting, Data Collection & Explorers, Cloud App Security for Information Protection & Customer Lockbox* and Compliance Boundaries*

Enjoy!

Information Protection & DLP Kick-Start Guide

Contents

1. Microsoft's Four Pillars of Data

Microsoft has broken down their Data methodologies into easy-to-follow segments, these allow you as an admin to break down the capabilities of the solution within each area to understand what is required to flow through them to maintain the best possible approach for the organization. Inside this guide, I will be covering off items within; Know Your Data, Protect Your Data & Prevent Data Loss, but not everything. Govern Your Data is not covered at all within this guide, this will be covered within another Kick-Start Guide.

1.1 Know Your Data

The Know Your Data segment is to provide the business with the chance to understand the data landscape and identify sensitive or important data across Cloud and On-Premises. This delivers the chance to migrate data into the required workloads or identify data that requires labelling before migrating to Cloud for regulatory purposes.

1.2 Protect Your Data

The Protect Your Data segment is to provide the business with the chance to protect data with encryption via Information Protection Labelling with Microsoft Keys, Bring Your Own Keys or Double Key Encryption or Office Message Encryption, extend Information Protection to Microsoft Cloud App Security, configure access restrictions, configure visual markings.

1.3 Prevent Data Loss

The Prevent Data Loss segment is to provide the business with a chance to configure Data Loss Prevention Policies for Data-in-Transit, Data-in-Use and Data-at-Rest to prevent intentional or accidental oversharing of sensitive information.

1.4 Govern Your Data

The Govern Your Data segment is to provide the business with a chance to retain data based on policies and labels, create a defensible disposal strategy with data disposition reviews, moreover, provide the ability to store data in M365 for the business to govern. In addition, Microsoft offers the capability to abide by regulatory requirements for marking items as immutable.

2. Microsoft Information Protection – Sensitivity Labelling for Files, Emails, & Container Labelling for Groups & Sites

Sensitivity Labelling is undoubtedly the first and most adopted solution within Compliance. Almost immediately, organizations want to protect their business-sensitive data by assigning a Classification Taxonomy or as Microsoft likes to call it, Labelling Taxonomy. Though, this can be an overwhelming task at times, trying to map out what has been defined within the taxonomy document into configurations and permissions within labels is difficult especially for organisations that share encrypted data externally regularly. Therefore, navigating around the MS Docs for information can be tough, especially, when there are some great blogs out there that are a benefit to the use cases you are wanting to build out. If you weren't looking hard enough, one would simply assume they do not exist.

In some circumstances, I have had conversations with organisations that have yet to compose a Taxonomy. They will, therefore, try to assemble the document as they build out the labelling

configurations. As you can imagine, this takes a huge amount of time and effort to work through, due to building out the core configurations without that important baseline taxonomy to work in conjunction with.

When it comes to Labelling, Microsoft has Three Stages on how to roll out Labelling through the business. This comes in the form of **Crawl, Walk, Run**. Time and again, I will hear the business wants to use Auto-Labelling as it is easier for the user's, this way the business is not relying on individuals selecting the right Label or in some cases choosing a Label at all. However, as you will read below this is not recommended, **Crawl** is the first step into Labelling, and that means manual labelling. If a user cannot determine what data they own or collaborate with, how can they ever know its sensitivity?

Encourage the business to provide time in rolling out Labelling as a manual process, consequently, allowing users to identify the data and the Sensitivity Label that maps back to it. There is more information on the subject under the links below.

The following links will provide a better understanding of Microsoft Information Protection & Labelling for sharing sensitive data as this is a priority for your organisation: -

- Microsoft Information Protection Deployment Acceleration Guide with Crawl, Walk Run:
  - Microsoft Information Protection and Data Loss Prevention - Compliance Customer Experience Engineering (CxE)
- Designing a Classification Framework for M365 Labelling:
  - Create a well-designed data classification framework - Microsoft Service Assurance | Microsoft Docs
- Classification aka Labelling Taxonomy:
  - Data classification & sensitivity label taxonomy - Microsoft Service Assurance | Microsoft Docs
- Learn about Labels:
  - Learn about sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Labels:
  - Get started with sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- MIP: Notes from the field:
  - https://techcommunity.microsoft.com/t5/security-compliance-identity/mip-notes-from-the-field/ba-p/1501297
- External Sharing Scenarios:
  - Secure external collaboration using sensitivity labels - Microsoft Tech Community
- Restrict Access to Content via Labels:
  - Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs
- Considerations for Encrypted Content:
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#considerations-for-encrypted-content
- A small troubleshooting guide for auto-applying sensitivity labels that do not auto-apply:
  - https://answers.microsoft.com/en-us/msoffice/forum/msoffice_o365admin-mso_security-mso_o365b/a-small-troubleshooting-guide-for-auto-applying/ffa60688-f500-4691-8fef-8cb0452c3faf?tm=1631607529198
- Co-Authoring for Encrypted Document:

- Co-authoring on Microsoft Information Protection encrypted documents is now generally available - Microsoft Tech Community

2.1 Container Level Labelling for Groups & Sites

Container Level Labelling provides your organisation with the ability to apply a Sensitivity Label to a SharePoint Site, M365 Groups and Teams Channels. The organization may already have this feature, enabled, however, if it is not, an administrator will need to navigate to the Information Protection Section within the Compliance Portal, there you will be presented with a Banner suggesting Setting up Container Level Labelling for your organisation. Select **Turn On**, this will run in the background and configure, thereafter, follow the link provided to enable the sync of the labels. When the configuration message has disappeared, check the labels to see if you now have the option to apply these labels for Groups & Sites. Although, please bear-in-mind; this configuration can take up to 24 hours to apply.

Note:
If you find that when you have tried to enable this feature and it is not working, I have a blog, which will guide you through the process: - ➢ Enabling Container Level Sensitivity Labelling for Groups & Sites in Microsoft 365

2.2 Auto-Labelling Service-Side & Cloud Data Discovery & Labelling Enforcement (E5)

The Service Side Auto-Labelling Solution provides the business with the ability to automatically apply Sensitivity Labels based on data matched from a Sensitive Information Type. Additionally, it offers a Scanning Mode option, which, can be used as a Cloud Data Discovery Tool. Once the business has created a Custom Sensitive Information Type or chosen a Default Sensitive Information Type, the service will scan for this type of data in the locations you have configured. When completed it provides a data landscape of where your sensitive items are located. Additionally, it delivers recommendations of where matched data can be enforced with the relevant Sensitivity Label for items in the Cloud, this will provide the business with the ability to gather an in-date report of what data is where and what recommendations are offered when it comes to the Labelling. Only after scanning has completed and the business has evaluated the data reported back, of which, confirming matched, or removing unmatched items should you consider turning on the enforcement.

2.2.1 Contributing Links: -

- Service-Side Auto-Labelling:
  - Automatically apply a sensitivity label to content in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs

3. Azure Information Protection Scanner (Discover E3, Enforce E5) On-Premises Data Discovery & Labelling Enforcement

The Azure Information Protection Scanner provides the business with the ability to automatically apply Sensitivity Labels based on data matched from a Sensitive Information Type. Moreover, it offers a Discovery Mode option, which, can be used as an On-Premises Data Discovery Tool for the following locations, On-Premises SharePoint 2019 through to 2013, 2010 is supported, however, in extended support, also giving coverage for UNC Paths that use the SMB & NTFS Protocols. Once the business has created the required labels within the Compliance Centre, this then provides the opportunity to run a Data Discovery for On-Premises files. Once the Discovery Mode to completes, it will provide a report displaying the information types detected in the data sets that have been

scanned. It is not unusual to set up dedicated Labels and a Label Policy to run the Scanner with, maximizing the search for Sensitive Information Types you need to match. Moreover, the Scanner is a great way to enforce labels on items before migrating them to Cloud, this helps when there is a regulatory need to do so.

3.1 Contributing Links: -

- AIP Scanner Prerequisites:
  - Azure Information Protection (AIP) unified labeling scanner prerequisites | Microsoft Docs
- Requirement for AIP Scanner:
  - https://docs.microsoft.com/en-us/azure/information-protection/requirements
- Deployment Guide:
  - https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-configure-install
- AIP Scanner Best Practises:
  - https://techcommunity.microsoft.com/t5/security-compliance-identity/best-practices-for-deploying-and-using-the-aip-ul-scanner/ba-p/1878168#reporting
- PowerShell Library:
  - PowerShell Gallery | AIPScannerConfig 1.1.92

4. Viewing Sensitive Data - Content Explorer & Activity Explorer (E5 feature)

Here is where all the organisational user content and data activity is displayed. This will make possible a view on how Sensitive Information & Sensitivity Labelling is being used throughout the environment. Although, you will need additional permissions to view the sensitive information data sets that have been detected. Be cautious who the Content Explorer permissions are shared with as it provides a data level reveal when reviewing items.

4.1 Contributing Links: -

- Get Started with Content Explorer:
  - Get started with content explorer - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Activity Explorer:
  - Get started with activity explorer - Microsoft 365 Compliance | Microsoft Docs
- Labelling Activity Reference:
  - Labeling actions reported in Activity explorer - Microsoft 365 Compliance | Microsoft Docs

5. Data Loss Prevention (E3)

Data Loss Prevention enables the business to increase or expand their protection of data via Data Loss Prevention Policies. DLP Policies can be configured to identify, monitor, and protect sensitive items, consequently, reducing the risk of accidental or intentional data leakage. DLP offers many preventative patterns across the following: -

- Locations: Exchange, Teams, SharePoint, OneDrive
- Office Applications: Word, Excel, PowerPoint
- Windows 10 Devices
- Third-Party Cloud Applications

- On-Premises File Shares
- On-Premises SharePoint

I repeatedly see DLP configured to prevent Sensitive Information Types and items encrypted with Sensitivity Labels from leaving the environment. For example, if you had a document that contains Highly Confidential financial information and has been labelled with a Sensitivity Label named Highly Confidential Internal, admins can configure a policy to check for that Sensitive Information Type and/or Sensitivity Label to block sharing, thereafter, creating an audit report for traceability. Further controls are the opportunity to display Policy Tips, which enables the business to provide information on why a certain Policy & Rule has been triggered, therefore, educating the user of the sensitive information and why the business does not allow for this type of data to be shared externally. In addition to Blocking data from being shared internally or externally the business can configure Overrides, where a user would have the option to select the Override allowing the sharing of data to be achieved. A more recent feature for data-at-rest would quarantine sensitive items and then lock them.

Selecting the locations where DLP can be configured will provide different options within the rules. For example, having Exchange, SharePoint & OneDrive selected will provide fewer options than just having Exchange selected. As a result, I would always research the use cases for the organisation and then build out the DLP Policies per-location required, maximizing the configurable options available.

It is highly advisable that when creating DLP Policies the business does so in the configuration of **Test It Out First.** This will provide the ability to review the policy matches and assess the results allowing for fine-tuning where required. Moreover, offering the chance to assess the policy's impact before turning it on.

5.1 Alerting for Data Loss Prevention

Data Loss Prevention now has a dedicated Alerting area within the Data Loss Prevention Blade in the Compliance Centre, this will display all the alerts that have occurred in the environment. In addition to this, Data Loss Prevention auditing is available from the Reports Blade, then by navigating to **Organizational Data,** displayed within here is the following information:

- DLP Policy Matches: Displays the matches made when a policy is in test mode
- DLP Incidents: Displays the incidents that have taken occurred at the item level
- DLP False Positives & Overrides: Shows the Overrides or False Positive Feedback

5.2 Contributing Links: -

- Learn About Data Loss Prevention:
  - Learn about data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Plan for Data Loss Prevention:
  - Plan for data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Data Loss Prevention Policy Reference:
  - Data Loss Prevention policy reference - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Data Loss Prevention:
  - Get started with the default DLP policy - Microsoft 365 Compliance | Microsoft Docs
- Policy Tips for Data Loss Prevention:
  - Send email notifications and show policy tips for DLP policies - Microsoft 365 Compliance | Microsoft Docs

- Policy Tips Reference:
  - Data Loss Prevention policy tips reference - Microsoft 365 Compliance | Microsoft Docs
- Alerts for Data Loss Prevention:
  - View the reports for data loss prevention - Microsoft 365 Compliance | Microsoft Docs

6. Data Loss Prevention for Microsoft Teams (E3) & (E5)

Data Loss Prevention for Microsoft Teams can prevent the sharing of sensitive information within a Teams Chat or Channel, including Private Channels. DLP for Teams provides the business with the ability to block items that have been labelled with a Sensitivity Label or includes a Sensitive Information Type. This will block the item(s) from being shared within a Teams conversation where External access has been enabled, or, where a Teams conversation has a Guest is present. Along with blocking the item from being shared within the chat administrators can apply a Policy Tip, this will display a message to the user who has triggered the rule allowing the business to educate their users on why this type of sensitive information cannot be shared.

Here are a couple of examples from Microsoft Docs: -

Example 1: Protecting sensitive information in messages. Suppose that someone attempts to share sensitive information in a Teams chat or channel with guests (external users). If you have a DLP policy defined to prevent this, messages with sensitive information that are sent to external users are deleted. This happens automatically, and within seconds, according to how your DLP policy is configured.

Example 2: Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive for protection to be in place. This is an example of DLP for SharePoint that shows up in Microsoft Teams, and therefore requires that users are licensed for Office 365 DLP (included in Office 365 E3) but does not require users to be licensed for Office 365 Advanced Compliance.)

Microsoft has recently announced four new Conditions in Teams Data Loss Prevention Policies. These introductions provide the business with an improved compliance position for Teams Chats and Channels.

Teams DLP now features:

- Sender is
- Recipient is
- Sender domain is
- Recipient domain is

6.1 Contributing Links: -

- Learn About DLP for Microsoft Teams

    - Learn about the default data loss prevention policy in Microsoft Teams (preview) - Microsoft 365 Compliance | Microsoft Docs
- Data Loss Prevention & Microsoft Teams
    - Data loss prevention and Microsoft Teams - Microsoft 365 Compliance | Microsoft Docs
- Announcing Public Preview of New Conditions in Teams DLP
    - Announcing Public Preview of New Conditions in Teams DLP - Microsoft Tech Community

7. EndPoint DLP (E5)

EndPoint DLP enables protection at the Windows layer when it comes to organisational data users are interacting with, which, could be data-in-use and data-at-rest. EndPoint DLP protects sensitive information by protecting the content from being copy and pasted, uploaded to third-party cloud solutions, copied to USB, uploaded via a non-Microsoft browser, shared with external domains and blocking unallowed apps from accessing sensitive data. Within a DLP Rule, you can set the following controls Audit, Block, and with the new advancements you can offer User Overrides from M365 Services and Devices, furthermore, where required Justifications on the items you have configured for blocked with override. A couple of important notes on EPDLP, devices will need to be onboarded into the Compliance Centre, yet, if you have devices enrolled into Defender for EndPoint they will automatically be onboarded. In addition, your devices must be Windows 1809 and above for EPDLP to operate. Extra information is provided in the Onboarding link below.

7.1 Contributing Links: -

- Get Started with EPDLP:
    - Get started with Microsoft 365 Endpoint data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Onboarding Devices:
    - Onboarding tools and methods for Windows 10 devices - Microsoft 365 Compliance | Microsoft Docs
- Using EPDLP:
    - Using Endpoint data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Plan for EPDLP:
    - Plan for data loss prevention - Microsoft 365 Compliance | Microsoft Docs

8. Cloud App Security & Information Protection Integration (E5)

MCAS and MIP integration offer added controls for Sensitivity Labels, Sensitive Information Types, and DLP Policies. The business can connect third-party solutions like Dropbox, Box to prevent items that have been labelled with a Sensitivity Label from being uploaded and stored on these Cloud Solutions. In addition, it provides a retrospective encrypting solution for data at rest in SPO/ODB, investigation of files is also possible, creating the ability to view all classified data within the MCAS Portal.

8.1 Contributing Links: -

- MIP/AIP to MCAS Integration:
    - Integrate Azure Information Protection with Cloud App Security | Microsoft Docs
- MCAS Documentation Library:
    - Microsoft Cloud App Security documentation | Microsoft Docs

- MCAS DP Blog:
  - MCAS Data Protection Blog Series: Do I use MCAS or MIP? - Microsoft Tech Community

9. Unified Labelling Client vs Built-In Labelling Client

Two clients offer similar controls, these are the Unified Labelling Client, which, is installed onto the Windows Devices. Then there is the Built-In Client, which, comes with Apps for Enterprise as an offering within the application's ribbon. The standout differences for the Unified Labelling Client are the capabilities to protect non-Microsoft files, for example, PDF, TXT, JPEG, to name a few. This protection type is offered from Windows File Explorer by Right-Clicking on an item, selecting, Classify & Protect, this then offers the user the ability to choose a Sensitivity Label. However, it's important to note, when offering the Classify and Protect option, there is a Protect with Custom Permissions Option, which, presents the user with a custom set of permissions they can choose which will override the organisation Labelling configurations thus leading to potential data exfiltration. This is achieved when the user selects the; Protect with Custom Permissions, supplying the ability to bypass the deployed Sensitivity Labels. As a result, I will always advise this option is disabled. There are instructions within the custom configurations link below on how to disable this feature.

9.1 Contributing Links: -

- Benefits of Deploying the Built-in Client:
  - The benefits of deploying built-in labeling within Microsoft 365 apps - Microsoft Tech Community
- Compare the Labelling Clients:
  - https://docs.microsoft.com/en-us/azure/information-protection/rms-client/use-client#compare-the-labeling-solutions-for-windows-computers
- Disable Custom Permissions in File Explorer:
  - Custom configurations - Azure Information Protection unified labeling client | Microsoft Docs
- Sensitivity Labelling Capabilities in Word, Excel & PowerPoint
  - https://docs.microsoft.com/en-gb/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide#sensitivity-label-capabilities-in-word-excel-and-powerpoint

10. Compliance Boundaries with Compliance Filters*

Setting up Compliance Boundaries with Compliance Filtering provides filtering configurations that can be set up to segment searches into compliance boundaries. This is often used when a global company is required to restrict searches of data from within EMEA from NAM, or from APAC into EMEA, building Compliance Boundaries out with Compliance Filters delivers this. This is also extendable into what can be searched and viewed, which are built out within the Security Filtering, therefore, providing the business with a segmented search and permissions solution. I have also designed this in the past to protect V.I.P users within an organisation from having their data searched by restricting it to only a single person or a very small group.

*** Note:**
Compliance Boundaries are an Advanced eDiscovery feature. However, the question of; can I separate who can search for what data, within each department or a geo-region, always comes up when talking about Information Protection and organisational data. Therefore, I have included it for reference.

10.1 Contributing Links: -

- Set up Compliance Boundaries:
  - Set up compliance boundaries for eDiscovery investigations - Microsoft 365 Compliance | Microsoft Docs
- Permissions Filtering:
  - Configure permissions filtering for Content Search - Microsoft 365 Compliance | Microsoft Docs

11. Encryption; BYOK, HYOK & Customer Lockbox*

Using BYOK is an option and is often used as a regulatory requirement and the same can be said for HYOK. Although, HYOK in my experience will be used for On-Premises Data of which should not be shared onto the Cloud. BYOK allows you to encrypt data in the Cloud, either on its own or with a Microsoft Key, subsequently configuring two keys onto the data set, which is known as Double Key Encryption (DKE). However, in some scenario's there are limitations on these encryption solutions, therefore, I have compiled a list of links that will guide you through the know-how on M365 encryption.

* Note:
I have provided the link for Customer Lockbox, what it does and how to request it. Customer Lockbox is an Insider Risk Solution and is enabled to Approve or Reject Microsoft Support from accessing organisational data, therefore, the question of can Microsoft see my content, can Microsoft access my data, constantly comes up when talking about Information Protection and organisational data, therefore, I have included here for reference.

11.1 Contributing Links: -

- Azure Information Protection Keys:
  - Your Azure Information Protection tenant key | Microsoft Docs
- M365 Encryption:
  - Encryption in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
- DKE Option for Labelling:
  - Double Key Encryption (DKE) - Microsoft 365 Compliance | Microsoft Docs
- M365 Service Encryption:
  - Service Encryption - Microsoft 365 Compliance | Microsoft Docs
- Customer Lock Box:
  - Office 365: What is Customer Lockbox and How to Enable it - TechNet Articles - United States (English) - TechNet Wiki (microsoft.com)
  - Customer Lockbox Requests - Microsoft 365 Compliance | Microsoft Docs

12. AIP Super User – Encryption & Decryption

The AIP Super User is used to remove encryption from an item or item. This provides the business with a safety net when supplying the capability to encrypt for users. Therefore, offering an AIP Super User allows for the encryption to be removed. This comes in handy when users have left the business and managers require access to encrypted data or, users have moved roles, offering the same unencrypt capabilities. Consequently, this is a must-have feature for the businesses Joiners, Movers, Leaver's process.

12.1 Contributing Links: -

- AIP Super User Configuration:
  - Configure super users for Azure Rights Management - AIP | Microsoft Docs

13. Additional Links for Continued Information, Research, Updates and Announcements

What's New in Information Protection – these links provide a breakdown of everything that has recently been released, I am providing this as most people are not aware it exists. Additionally, I have included the new Microsoft Information Protection – One Stop Shop, where all MIP information is within a single link/library, this is a must-have link to bookmark.

13.1 Contributing Links: -

- What's New in MIP:
  - What's New in Information Protection? - Microsoft Tech Community
- MIP One-Stop Shop:
  - Microsoft Information Protection in Microsoft 365 One Stop Shop Resource Page - Microsoft Tech Community

14 Concluding This Kick-Start Guide

Thank you for taking the time to read through this document. I hope the information provided in this Kick-Start Guide has been a benefit to you, your company and/or even your customers.

In addition to this guide, I also have a Kick-Start Guide for the following solutions: -

- Information Governance & Records Management
- Insider Risk Management & Communications Compliance
- Advanced eDiscovery

If you would like me to compose these into what you have just read, please get in touch via the website below.

14.1 Important Notes: -

1. The information laid out in this guide is not a step-by-step numbered translation of how to implement these solutions, it is simply the way I prefer to engage with organisations to: -

   A: determine their requirements
   B: determine their priorities with MIP & DLP

2. I will try and make every effort to keep updating this document to new versions when the information within it changes. However, I cannot guarantee this will happen with the immediate effect of items changing.

3. Where advice is given always check the Microsoft official documentation and links of which may or may not be provided, therefore, being sure the information is still up to date.

msftcompliance.com
LinkedIn
Twitter