DATA LOSS PREVENTION EVERYONE CAN EMPLOY

A Guide for Any MSP or SMB

Abstract

This guide provides a practical approach for small and medium-sized businesses (SMBs) to implement Data Loss Prevention (DLP) strategies, using accessible technologies to protect sensitive data. It emphasizes the importance of DLP in safeguarding against unauthorized disclosure and offers actionable steps for adopting DLP within any Microsoft environment. The document serves as an educational resource, empowering businesses to take charge of their cybersecurity and compliance responsibilities.

Dom Kirby
domkirby.com

Introduction to Data Loss Prevention

According to Copilot:

Data loss prevention (DLP) is a set of technologies and policies that aim to prevent the unauthorized disclosure, modification, or deletion of sensitive data. DLP emerged in the early 2000s as a response to the growing threats of data breaches, insider attacks, and regulatory compliance. DLP systems can monitor, filter, and block the flow of data across networks, devices, applications, and cloud services. Some examples of DLP functions are detecting and preventing data leakage via email, web, USB, or other channels; classifying and encrypting data based on predefined rules; and alerting and reporting data incidents and policy violations.

Why use Data Loss Prevention?

The Safeguards within CIS Control 3 speak to the need for proper *Data Protection*. Implementation Group 1 (i.e.: the minimum we should do) covers some basic data management and protection practices such as:

- Establishing and documenting a process for data management
- Inventorying our data
- Configure Data Access Control Lists
- Enforce retention policies on our data (per our data management process)
- **Securely dispose of our data** (this is a big one)
- **Encrypt our data on end-user devices** (also a big one)

These Safeguards cover some of the most basic elements of protecting our data. We should all know by now that encrypting endpoint devices is both an inexpensive and significant win, for example. However, we can (and should) do more to protect our data.

As you dive into Control 3, IGs 2 and 3, things get more interesting. All the way up in Implementation Group 3, we have "Deploy a Data Loss Prevention Solution." This sits all the way up in IG3 because 1) DLP solutions are historically expensive and hard to deploy, and 2) a full DLP project depends on some of the prior controls (like developing a data classification scheme).

However, I'm a huge fan of leveraging DLP, *everywhere*, and SMB solutions like Microsoft 365 Business Premium make it possible for SMBs to employ the technology. You see, **every business** manages some sort of sensitive data. How do you or your clients complete

financial transactions? Ever caught an end user emailing credit card information? What about basic protection for patient data for smaller practices? The list goes on.

In this guide, we'll focus on the *basic* data loss prevention measures that *any* business can deploy right now to reduce the likelihood of an accidental or malicious data leakage and reduce their overall liability when interacting with data.

Two Notes Before We Dive In:

1. This document is in no way meant to be a comprehensive guide to DLP. On the contrary, it's meant to give you ideas for adopting DLP in *any* Microsoft environment.
2. The sensitive data types we're using in this example are mostly tailored to the *United States*. However, they can be easily adapted to any region/country.

EVERYONE IS RESPONSIBLE FOR THEIR OWN CYBERSECURITY AND COMPLIANCE. THIS GUIDE IS FOR EDUCAITONAL PURPOSES ONLY. YOU ARE USING IT AT YOUR OWN RISK.

The "DLP for All" Concept

The concept of DLP for all is really simple: *every business* deals with some kind of sensitive data. Also, there are certain data types that should *almost* never leave the organization in an email message or something similar. This technical implementation is based on this concept, protecting the data types that should *always* be protected, regardless of the customer/environment.

Getting Started: Purview DLP

The technical bits of this guide will be based on Microsoft Purview Data Loss Prevention tooling. The general concepts and policy-types can be recreated in most DLP platforms if you are not using Purview. This guide is built on the assumption that you or your client has **Microsoft 365 Business Premium** licensing. You may be able to combine other Microsoft SKUs to achieve the same goal (and this same concept will of course work in Microsoft 365 E3 or E5.

Getting to the Build

What We're Protecting

Before we get nerdy, let's talk about the general types of information we're going to place controls on. These data types can and should (in my opinion) have controls over them in *any* technology environment.

Financial Data

In most scenarios, we shouldn't just be emailing our (or anyone else's) financial data all *nimbly bimbly*[1]. In this category, we can place content types such as *credit card numbers, bank account numbers, etcetera*. Emailing your AMEX to your supplier isn't, has never been, and never will be a wise idea. We should prevent it or *at least* enforce encryption to protect that data.

Sensitive PII

I'm sort of inventing a category here: *Sensitive PII*. In most businesses, it's quite normal to send some basic information about a person. However, items such as *passport numbers, driver's license numbers, or Social Security numbers* are sensitive in nature. We don't want to leak anyone's SSN, and there are better ways to transport if necessary. We'll use Purview to stop it.

Actions We Can Take

I almost always deploy these policies such that they *prevent* these data types from leaving the organization. However, that might not be the right approach for some clients or information types. We have a couple of simple options we'll explore here:

- **Block:** This full-stop prevents the data from leaving the organization. The user and admins (and other contacts you choose) will be alerted.
- **Alert:** Using a combination of admin alerts, user notifications, and policy tips, we can let everyone know that a policy has been triggered. This is a useful way to make users rethink before sending, or simply alert on these activities if not preventing them from happening at all.

[1] *Nimbly Bimbly:* A reference to the popular movie *Super Troopers*: *"Am I jumpin' around all nimbly bimbly from tree to tree?"*

Breaking Down Policies

Like most Microsoft Security products, DLP uses the concept of Policies. This means that you can have several policies in an order or precedence chosen by you, each that look for different things and take different actions.

The way you structure your policies will depend primarily on how you want to manage different types of data. You may choose to alert on some while blocking others. Additionally, policies with a small scope make alert triaging easier. An alert on "sensitive stuff" is much harder to triage and react to than an alert that says, "Sensitive Personal Information Leakage." Consider both the actions to take and your own reporting when implementing DLP.

Alright, Let's Build Already

To keep this guide from being super long, I'll write a somewhat detailed list of steps for the first policy, and simply provide the settings for the others. To get familiar with Purview DLP, check out the following Microsoft documentation:

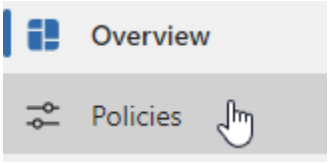
- Learn about data loss prevention | Microsoft Learn
- Plan for data loss prevention | Microsoft Learn
    - Design a Data loss prevention policy | Microsoft Learn
    - Data Loss Prevention policy reference | Microsoft Learn
- Create and deploy a data loss prevention policy | Microsoft Learn

We'll be doing most of our work from the *new Purview portal* at https://purview.microsoft.com.

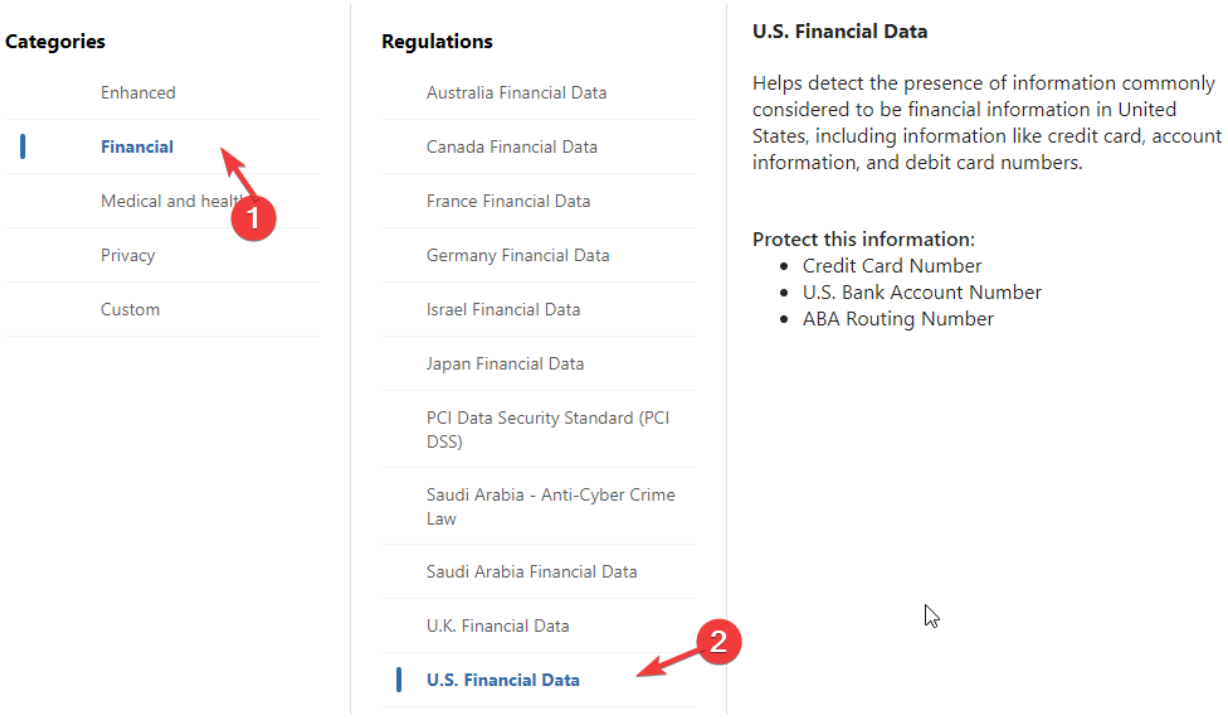
Policy 1: Financial Data

This policy prevents our users from sending out their corporate AMEX number in a lapse of judgement. Conveniently, Microsoft offers several built-in DLP templates you can leverage to make life easy, so let's take advantage of that!

1. Navigate to Data Loss Prevention in the Purview Portal
2. Navigate to the *Policies* section



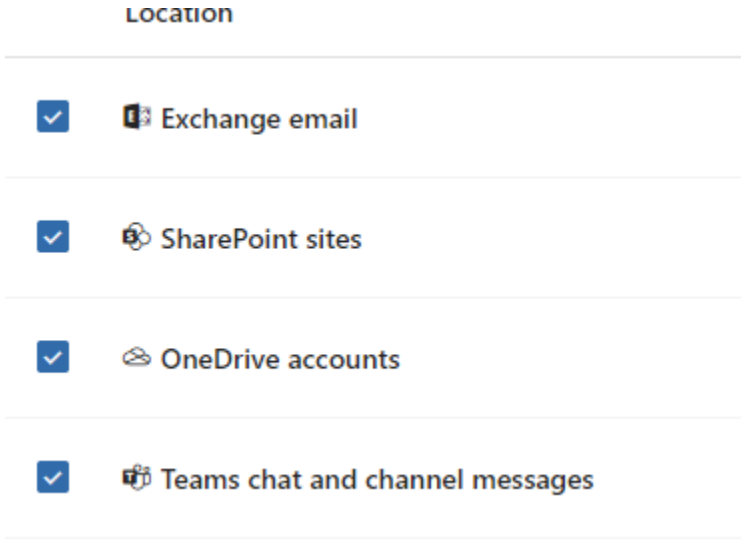
3. Click + Create policy and wait a moment for the templates to load.
4. Choose *Financial* and then *U.S. Financial Data* (or the appropriate option for your country)



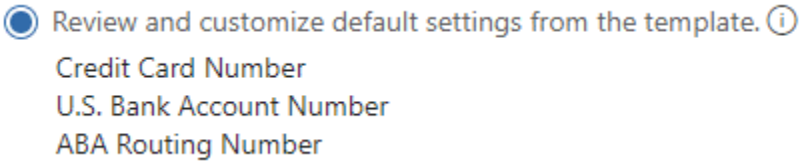
   a. You'll notice that this conveniently includes the key data types we're after: *credit card numbers, U.S. bank account numbers, routing numbers*.

5. Click Next
6. Give the policy a descriptive name such as "Prevent Leakage of U.S. Financial Data."
7. Skip over *Admin Units* unless you have an Enterprise tenant and use those.

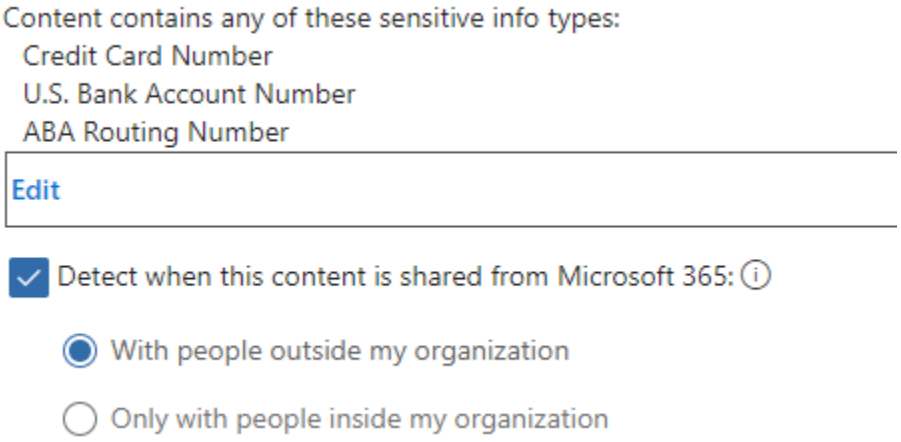
8. For simplicity, we'll want to select Exchange, SharePoint, OneDrive, and Teams for our locations (other locations require setup beyond the scope of this guide)



9. Leave the *Review* option selected and click Next



10. Check over the Info to Protect and scope (content shared inside or outside). For a basic deployment, I usually scope to information shared externally:



11. Next, we're on to *protection actions*, or what we're going to do when we find this info. There are a lot of important settings here:
    a. *When content matches the policy conditions, show policy tips to users and send them an email notification.* This is a **key element** of our DLP policy as this is what helps shape user behavior. Click Customize the tip and email to

customize what the users will see when the policy is triggered. I recommend customizing both the policy tip and the email to be informative to users (helping educate them why what they're doing is a bad idea and may not be allowed).

b. *Detect when a specific amount of sensitive info is being shared at one time.* I really hope your clients don't routinely need to send even one credit card number. But if they do, you can set this option to only act if a certain volume of this information is detected. I strongly recommend setting this option to **1** for this type of information.
c. *Send incident reports in email*. This option sets whether recipients of your choice will receive an email alert when this rule is triggered. This is helpful for notifying a business leader or compliance officer that something was triggered. Click Choose what to include in the report and who receives it to dive into these options.
d. *Send alerts if any of the DLP rules match*. This specifies whether to send alerts to administrators. I typically leave this *on* so that alerts are available in the Purview Portal.
e. *Restrict access or encrypt the content in Microsoft 365 locations*. This is where the policy does work. If you want an alerting only policy, leave this unchecked. Otherwise, check it!

12. Okay, now we need to customize what the enforcement actions do and whether users can override.
    a. With the *Restrict access* box checked, we're presented with options. Based on our scope, we'll have *Block users from receiving email…* selected.
    b. I recommend blocking people *outside your organization* from accessing the data. This will stop an external email or prevent a OneDrive sharing link from working that matches the DLP policy.
    c. **Overrides** can be a bit of a hot topic. However, if the client needs that capability, you can choose to allow users to override the policy in real time and provide a business justification. I recommend **not** enabling overrides for financial data.
13. **We're almost there!** We're just about ready to publish this policy! First, we must decide on a *mode*.
    a. **Simulation Mode:** This mode evaluates the policy but doesn't take enforcement actions. This mode is nifty for evaluating the impact of a policy over time, and you can even show the policy tips to prepare users for the upcoming policy requirements.

   i. **Note:** The automatic turn on after fifteen days option is nifty. This will warn users, admins, and compliance officers for 15 days on policy matches and then turn on the policy for enforcement.
b. **Turn the policy on immediately.** Self-explanatory, Purview will do exactly what you asked it to as soon as the policy finishes propagating. I recommend just turning these basic policies on[2].

14. **That's it!** Review the settings you're about to push and click the Submit button!

Note

The templates available for Purview policies offer several different coverage options. For example, you can cover both policies 1 and 2 using the "Gramm-Leach-Bliley Act (GLBA) Enhanced" template, which covers the above plus sensitive PII as well as other GLBA material such as business finances. Use the template that works best for you. In this approach, I'm simply using smaller policies for more granular reporting and user education.

Policy 2: Sensitive PII

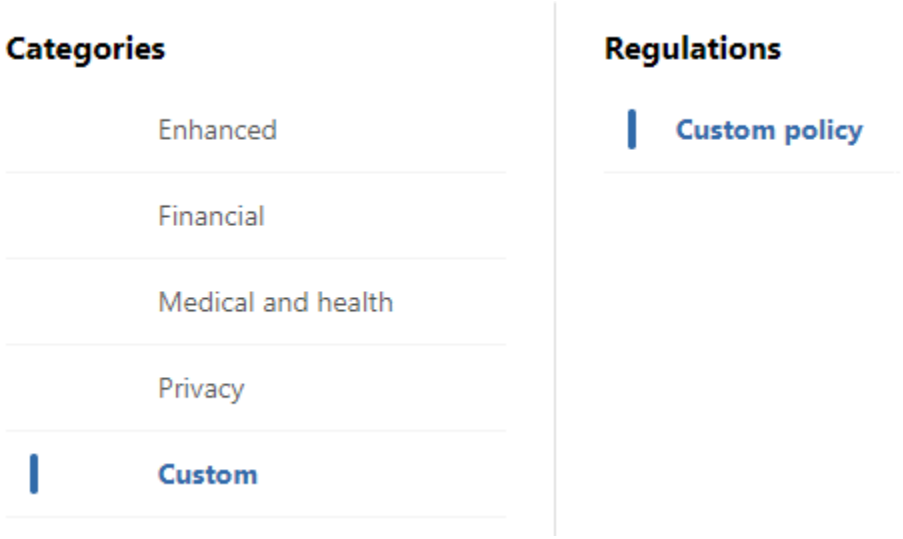
In this stage in our cybersecurity/compliance life, it's not uncommon for users to email around "general" PII such as email addresses. However, there are "sensitive" classes of PII that we shouldn't just be shooting out over the internet. That's what this policy covers. Most of the settings in this policy are like policy 1, so we will just cover the basics in this section to keep this guide from getting overly long.

This will be a **custom** policy as there aren't really any templates scoped to just the right kind of information we're covering.

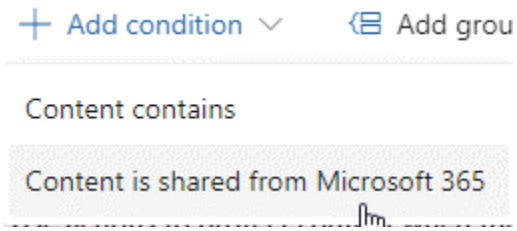
1. Follow steps 1-3 above to start the new policy creation.

[2] Obviously, be sure to have a discussion with your client before just kicking these on. However, sending this type of information over email or Teams is usually considered taboo, so I usually feel safe going straight into enforcement.

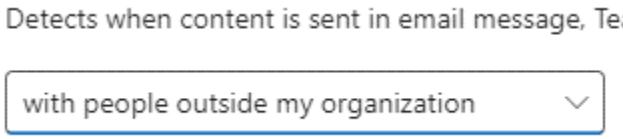
2. Choose *Custom* → *Custom Policy*



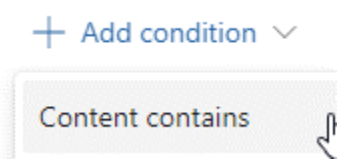
3. Give it a descriptive name such as “Sensitive PII Leakage.”
4. Skip over admin units (unless you use them) and use the same Locations as in policy 1.
5. “Next” your way into *Advanced DLP Rules*
6. Click + Create rule
    a. Name it “Sensitive PII Detection” (or the equivalent for your country)
    b. Add a condition for *Content is shared from Microsoft 365*



    c. Change the scope to *with people outside my organization*

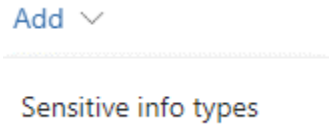


    d. Add another condition for *Content contains*, making sure that the operator in-between your conditions is **AND**



e. This will create a content *group*, name it "Sensitive PII" and use the *Any of these* operator

f. Add the following Sensitive Info Types

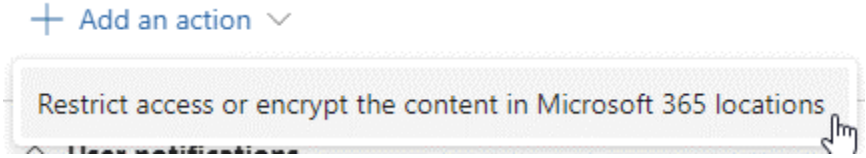


> **Sensitive Info Types**
>
> SITs are match conditions used to find information. You can add or remove them to fit your needs but remember not to be too broad in one policy.

   i. *U.S. Social Security Number (SSN)* (or your country's equivalent)
   ii. *U.S. Driver's License Number* (or your country's equivalent)
   iii. *U.S. / U.K. Passport Number* (or your country's equivalent, the U.S. and U.K. share an info type due to their similarities)

g. For all these sensitive info types, the instance counts should be "1 to Any." If you want to have a tolerance for some quantity of this information, set the left side of instance count to your maximum tolerance.

h. Under Actions, add the *Restrict* action



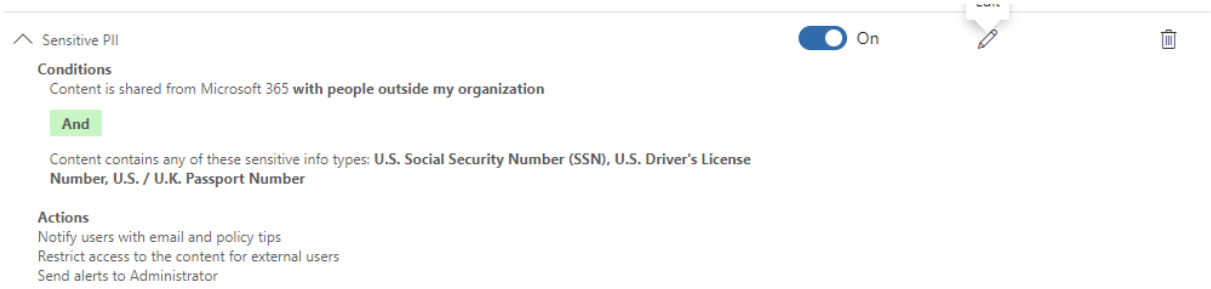
i. Set it to "Block only people outside your organization."

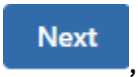
j. Turn **user notifications** *on* and set your desired settings. I recommend turning on and customizing policy tips and notification emails to help coach users on a better way to work with this information. This also prevents the "what happened to my email" helpdesk call because the user gets an alert explaining that their email was not sent.
   i. *Bonus:* The *compliance URL* option is handy as it can provide a link (perhaps on the customer's SharePoint intranet) to more information and guidance.

k. Customize **incident reports** as you see fit.

l. Click 

7. Your **advanced DLP rules** should now look something like this:



8. Click 

, select the policy deployment options as we did in policy 1, and save the policy.

BONUS: Check out these other Sensitive Info Types

DLP can be used to meet all kinds of risk reduction goals. Within your MSP (or even some customers), you might want to consider checking out some of the following sensitive info types and consider policies for them:

Sensitive info types can be accessed in the Purview Portal at https://purview.microsoft.com/datalossprevention/dataclassification/multicloudsensitiveinfotypes.

- General Password: Uses a variety of functions to detect a potential password present in content.
- A search for "Azure" will bring up all kinds of things such as shared access secrets, storage account keys, etc. This is super helpful to ensure that cloud secrets are properly managed.
- Amazon S3 Client Secret Access Key: Prevent secrets from being improperly managed.

Trainable Classifiers

Also be sure to check out the library of trainable classifiers. They offer all kinds of detections such as threats, profanity, harassment, pay information, M&A documentation etc. Trainable classifiers use advanced classification techniques beyond normal sensitive info types and allow for broader classification of data.

Conclusion

While DLP is typically considered a more advanced control (all the way up in Implementation Group 3), some simplified applications of DLP can go a long way in

reducing residual risk that occurs when handling data in **any** business. A baseline set of DLP policies can be a powerful value-add when talking to clients about managing and mitigating commonplace business risk.

Get access to all of my free MSP guides at https://domkirby.com/blog/category/guides/.

If this content is valuable, reach out on LinkedIn to let me know what else you'd like to learn. If you wish, you may also support my content creation by buying me a coffee. Caffeine helps the creative process.