



★ Data security & compliance

Identity & Access management

Power Platform

GenAI & AI security

Modern work



Tatu Seppälä
 Security & Compliance Architect



Best practices for **Information Protection & Data Loss Prevention** rollouts

Tatu Seppälä
CollabDays Bremen 2024



By 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents.

[Gartner \(February 22, 2023\)](#)





Sensitivity labels

- > Indicate risk level
- > Encryption
- > Visual markings
- > Access events
- > Integrates w/ DLP





Data Loss Prevention

- > Movements & actions
- > Guidance & awareness
- > Auditing and restrictions
- > Email encryption
- > Integrates w/ sensit. labels



Data Security

Prepare

Design

Discover

Build awareness

Protect & prevent



Stage 0

Prepare



Why?

Understand the risks of inaction

What?

Define the desired outcomes

Who?

Involve the right people



Why is **data security** important?



Why?

Understanding the challenges



Constant growth of data estates



Expanding data mobility & discoverability



Lack of sensitive information awareness



Evolving regulatory environment

Hey Copilot, how would you phrase these four data security challenges to explain them to a five-year old:
Constant growth of data estates
Expanding data mobility & discoverability
Lack of sensitive information awareness
Evolving regulatory environment



You have a **toy box** that keeps getting more and more **toys** added to it every day.



You can take your **toy box** with you wherever you go and easily find any **toy** you want.



There might be **special toys** in your **toy box** that you shouldn't share with others – but you don't know which ones are **special**



There are rules about how you can **play** with your **toys**. These rules keep changing as we learn more about what is safe and fair.

This is how you explain the 'Why'



You have an **information estate** that keeps getting more and more **unstructured data** added to it every day.



You can now take your **documents** with you wherever you go and easily find any **information** you want.



There might be **sensitive data** in your tenant that you shouldn't share with others – but you don't know which **data** it exactly is.



There is regulation about how you should handle your **data**, which keeps changing as we learn more about what is safe and fair.

What?

Define the desired outcomes



Typical starting point

- > Several TB of *something* in our SharePoint Online, OneDrive, on-prem file shares etc.
- > No shared idea of what the most critical data looks like
- > No visibility into what people are doing with our data
- > Only initial, one-time training in organizational guidelines (which most forget in a week)

What?

Define the desired outcomes



Targets to aim for..

- > Granular understanding of data estate
- > Key business data are automatically identified, classified and protected
- > Unbroken audit trail across data lifecycle
- > Data security awareness constantly reinforced in everyday work
- > Unnecessary sensitive data purged when no longer relevant

Who?

Involve the right people



> **Data security is a team sport**

> Which roles need to be involved?

Legal & compliance

End user services

HR

C-levels

Comms

Data Protection Office

IT

CyberSec

Best practice #0: Get organized

Include folks from..

Legal & compliance

IT & Cybersec

HR

Comms

End user services

Data Protection Office

etc.



Compliance & Insider Risk

General

1 🔍 Discovery

2 🔒 Protection and guidance

3 ⚠️ Insider Risk

4 ♻️ Data lifecycle



Bi-weekly checkups to raise requirements & follow progress



Stage 1

Design



When designing your **sensitivity label** taxonomy..

..remember the **KISS** principle

Keep It Simple, Stupid!





Personal



Public



General



Confidential



...



...



Highly confidential



...



...



Secret



...



...





Public



General



Confidential



...



...



Secret





General



Confidential



...



...



Start from a **baseline** label taxonomy that **most** will use..

Parent label

→ indicates **risk level**



General



Confidential

Sublabel

→ indicates **audience**



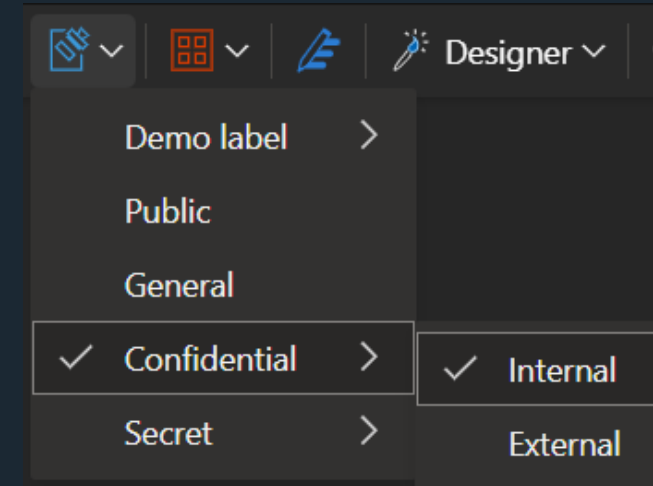
Internal only



Encrypted email (*email only*)



Unrestricted



..then translate **label names** & tooltips to relevant languages.



```
Set-Label -Identity "Confidential" -LocaleSettings
{
  "localeKey": "DisplayName",
  "Settings": [
    {
      "Key": "en-US",
      "Value": "Confidential"
    },
    {
      "Key": "de-DE",
      "Value": "Vertraulich"
    }
  ]
}
```



..then translate label names & **tooltips** to relevant languages.



```
Set-Label -Identity "Confidential" -LocaleSettings
{
  "localeKey": "Tooltip",
  "Settings": [
    {
      "Key": "en-US",
      "Value": "Information intended for authorized use only and may cause
damage to the organization if disclosed to unauthorized parties."
    },
    {
      "Key": "de-DE",
      "Value": "Informationen, die nur für den autorisierten Gebrauch bestimmt
sind und der Organisation Schaden zufügen können, wenn sie an Unbefugte
weitergegeben werden."
    }
  ]
}
```



Best practice #1: Design sensitivity labels & DLP together



Confidential Internal

From sensitivity labels..

- > **Encryption** - Allow interaction only by internal users
- > **Markings** - Add custom (dynamic) footer and watermark to documents











From Data Loss Prevention rules..

- > Create **audit trail** & provide **policy tips**
- > **Prevent** copying to USB, **limit** external sharing..
- > **Require justification** to upload to unapproved cloud services



Best practice #1: Design sensitivity labels & DLP together





	Encryption	Policy tip	Shareable externally?	Etc.
 General				
 Confidential Internal				

Best practice #1: Design sensitivity labels & DLP together

Label name	Label color	Usable by..	Tooltip	Encrypted	Encryption controls	DLP controls	Document markings
Public	#0078D7	Limited audience (if possible)	Content is specifically prepared and approved for public consumption by the information owner.	FALSE	No encryption applied	No DLP controls	No markings
General	#317100	Everyone	Can be shared internally or with authorised 3rd parties without causing damage to the business or its stakeholders.	FALSE	No encryption applied	No DLP controls	No markings
Confidential External	#FFEF00	Everyone	Would cause damage to the organization or its stakeholders if shared with unauthorized people. Should only be shared with authorized external parties.	TRUE	<p>Files: User-defined permissions</p> <p>Email: Automatically apply encryption (content only available for authenticated users, can be forwarded)</p>	<p>Audit-only actions EXO, SPO, OD - External sharing Show policy tip</p> <p>Blocked actions Endpoints Show policy tip Copy to USB Upload to unauthorized cloud apps Transfer over Bluetooth Transfer over RDP</p>	<p>Header Text: Confidential - Internal use only Font size: 10px Font color: Black Alignment: Center</p> <p>Footer Text: Confidential - Internal use only Font size: 10px Font color: Black Alignment: Center</p>
Confidential Internal	#FFEF00	Everyone	Would cause damage to the organization or its stakeholders if shared with unauthorized people. Cannot be shared with external parties.	TRUE	<p>Offline use: 14d Permission: Internal users only - Co-owner</p> <p>Allowed actions: All</p> <p>Only enforce more restrictive encryption if you clearly understand the implications and use cases!</p>	<p>Blocked actions EXO, SPO, OD - External sharing Show policy tip</p> <p>Endpoints Show policy tip Copy to USB Upload to unauthorized cloud apps Transfer over Bluetooth Transfer over RDP</p>	<p>Header Text: Confidential - Authorized use only Font size: 10px Font color: Black Alignment: Center</p> <p>Footer Text: Confidential - Authorized use only Font size: 10px Font color: Black</p>

Note: This is a suggested template and is not fit for production deployment as-is.





Best practice #2: Be very careful with encryption

	 Email and  Files											 Email only			
	View	Open	Read	Save	Edit content & Edit	Copy (Extract)	View rights	Change rights	Allow Macros	Save As, Export	Print	Reply	Reply All	Forward	Full Control
Viewer	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗
Reviewer	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗
Co-Author	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Co-Owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Don't use anything stricter than **Co-owner** for internal user permissions in baseline labels.







Best practice #2: Be very careful with encryption

	 Email and  Files											 Email only			
	View	Open	Read	Save	Edit content & Edit	Copy (Extract)	View rights	Change rights	Allow Macros	Save As, Export	Print	Reply	Reply All	Forward	Full Control
Viewer	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗
Reviewer	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗
Co-Author	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Co-Owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓


Remember that you can also give **other domains** permissions – for ex. trusted partners.



Best practice #2: Be very careful with encryption

	 Email and  Files											 Email only			
	View	Open	Read	Save	Edit content & Edit	Copy (Extract)	View rights	Change rights	Allow Macros	Save As, Export	Print	Reply	Reply All	Forward	Full Control
Viewer	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗
Reviewer	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗
Co-Author	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Co-Owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



Copilot for Microsoft 365 requires users to have both **View & Copy (EXTRACT)** permissions to reference content from an  encrypted document.



Best practice #3: Default labels can be a poisoned chalice

Apply a default label to documents

The label you choose will automatically be applied to Word, Excel, and PowerPoint documents when they're created or modified. Users can always select a different label to better match the sensitivity of their document. [Learn which Office app versions support this setting](#)

Default label

General

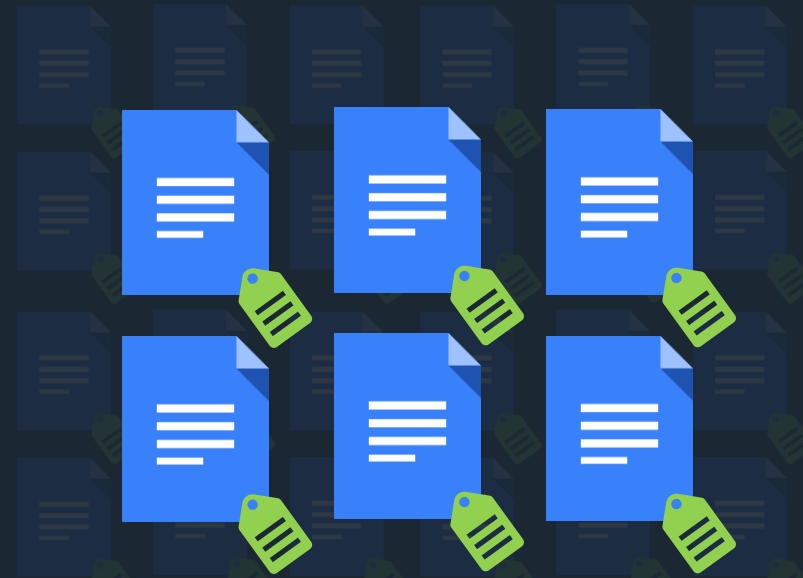


Best practice #3: Default labels can be a poisoned chalice

- > Using default labels too early is a very common mistake!
- > Doing so will almost certainly lead to *massive* underclassification of documents, devaluing sensitivity labels as an instrument.



All other labels



Default label

Best practice #3: Default labels can be a poisoned chalice

OK - how do we approach this then?

My experience: Implement manual sensitivity labeling with..

- > Proper **training**, clear tooltips w/ examples
- > **Recommended labeling** helps get the important stuff right
- > **Mandatory labeling** configured
- > Support from **leadership** and **champion users**



 Move **gradually** towards an automated approach

Mandatory manual sensitivity labeling

Client-side recommended sensitivity labels
Document library differentiated default labels

**Build routine
& educate**



Automatic client-side sensitivity labels
Service-side auto-labeling (simulation mode)



Service-side auto-labeling



Default labels

Automate

Best practice #4: Dedicated DLP policies for each workload

 Exchange Online

 SharePoint Online

 OneDrive for Business

 Teams

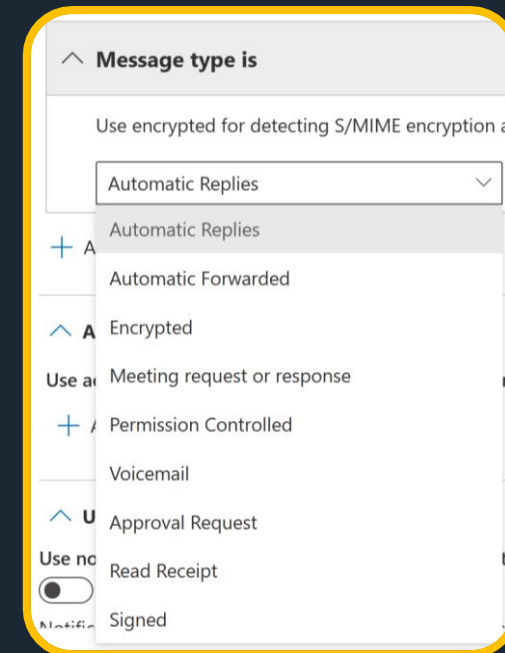
 Endpoints

 Power BI

 On-premises file shares

Benefits:

- + Differentiated **policy tips**
- + Differentiated **controls**
- + More **granular auditing**
- + Can use **workload-specific DLP rule conditions**



Best practice #5: Naming convention & ring model for DLP policies



% of all users

<20 people

3-5%

10-20%

99%+

 Ring 1

 Ring 2

 Ring 3

 Baseline



Best practice #5a: Naming convention & ring model for DLP policies

Workload index#-Ring index#-Workload-Deployment ring



100-EXO-Baseline

Org-level production policy



210-SPO-Ring1

Ring 1: Technical validation



320-OD-Ring2

Ring 2: Functional testing



430-TMS-Ring3

Ring 3: Pre-production



540-ENDP-VIPs

High-priority users



690-PBI-Experimental

Exploration & proof-of-concept rules



Best practice #5b: Consistent naming convention for DLP rules

Index# **Workload** **Conditions** **Controls**



101-EXO/Confidential-Internal/Shared:Ext/Block



212-SPO/Confidential-Trusted/Shared:Ext/Audit



323-OD/Secret/Shared:Ext/Block



435-TMS/SIT:AllCredentials/Shared:Int/PolicyTip



541-EP/Secret/Exfiltration/BlockOverride



696-PBI/SIT:FinlandPII/PolicyTip



Best practice #5b: Consistent naming convention for DLP rules

Date: 8/29/2023-9/5/2023 ▾ Activity: Any ▾ Location: ▾

Rule: Any ▾ Show less

<input type="checkbox"/>	EXO/SIT:Credentials/Shared:External/AuditOnly	138
<input type="checkbox"/>	SPO/SIT:FinlandPII/Shared:InternalOnly/AuditOnly	106
<input type="checkbox"/>	TM/SIT:Credentials/Shared:InternalOnly/AuditOnly	99
<input type="checkbox"/>	TM/SIT:FinlandPII/Shared:External/AuditOnly	32
<input type="checkbox"/>	SPO/SIT:FinlandPII/Shared:External/AuditOnly	30

Easy filtering!



Build your DLP solution in phases



Discovery

Auditing



Awareness

Policy Tips



Justification

Block w/ override



Protect & prevent

Block / Encrypt



Investigate

Trigger IRM



Stage 2

Discover



We can't protect what we don't know about

Visibility is the key to a sensible data security strategy



What we need to see

- > **Sensitive data accumulations in..**
 - ☁ Cloud
 - 🖥 On-premises
- > Sensitive data **movements & activities**
- > Sensitivity labeling **events**
- > Data Loss Prevention **rule matches**
- > **Justifications** for various overrides



How we build visibility

Data locations and accumulations

“What information do we have and where does it reside?”

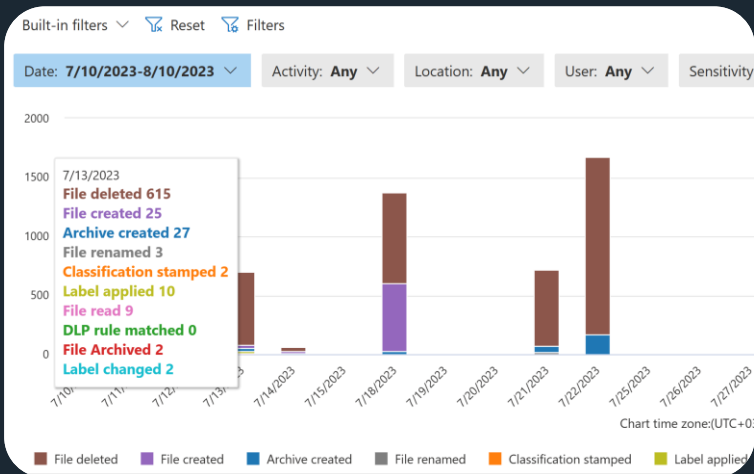
- Content Search & eDiscovery
- Defender for Cloud Apps File Policies
- On-premises MIP Scanner
- Content Explorer

Usage scenarios and trends

“How is information handled and moved around?”

- DLP rules in audit mode
- Insider risk analytics insights
- Defender for Cloud Apps
- Activity Explorer
- Sentinel & Log Analytics

Understanding of risks informs design



↓ Start here

Activity Explorer

+ Easy and effective

- Only goes 1 month back

Microsoft Sentinel | Logs

Selected workspace: log-sentinel

New Query 1*

log-Sentinel | Run | Time range: Set in query | Save | Share

```

1 MicrosoftPurviewInformationProtection
2 | where TimeGenerated >= ago(90d) and Operation has "SensitivityLabeledFileOpened"
  
```

Results | Chart | Add bookmark

TimeGenerated (Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius)	Id	RecordType
7/13/2023, 10:21:19.000 AM	cfd7ddac-b858-415f-b095-3a2...	84

Schema and Filter

TenantId	
Id	cfd7ddac-b858-415f-b095-3a274dc934d
RecordType	84
RecordTypeName	SensitivityLabeledFileAction
TimeGenerated [UTC]	2023-07-13T07:21:19Z
Operation	SensitivityLabeledFileOpened
OrganizationId	
UserType	Regular
UserKey	

☁ Ingest into..

Sentinel / Log Analytics

+ Powerful and granular

+ Opens up long term trend analysis

+ Can export into Azure Data Explorer (100y retention)

- Exploring data takes time and effort

- Not very accessible by non-techy people



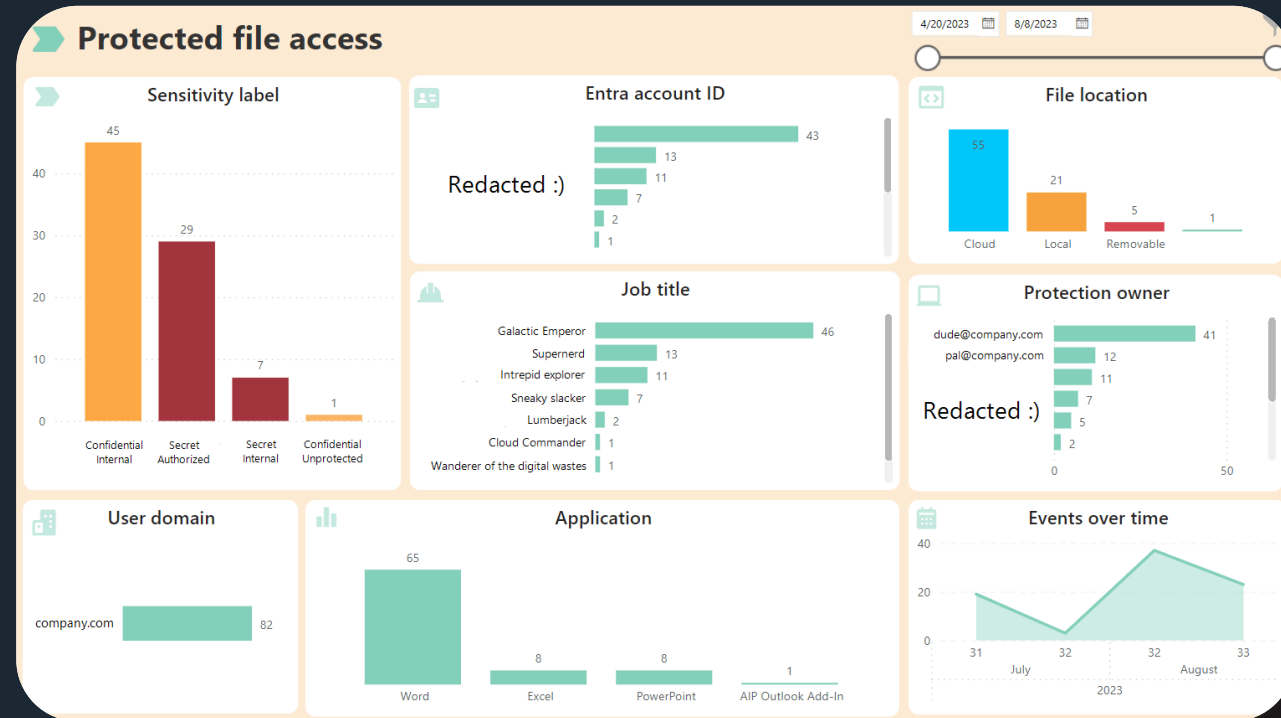


Visualize Log Analytics data with..



Power BI

- + Visual and approachable
- + Best tool for discovering insights & trends
- + Can exclude PII from datasets
- + Bring reports to Teams & mobile
- Takes effort to build



Protected file access

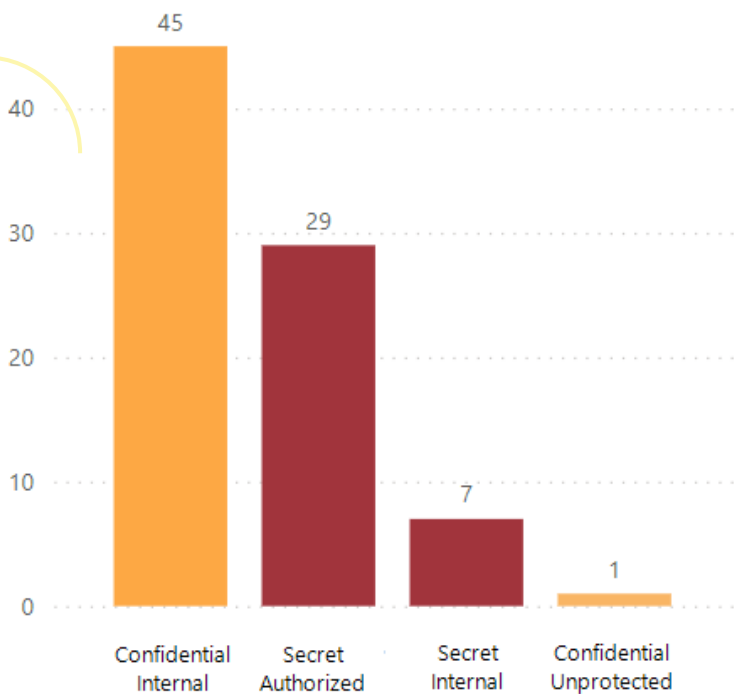
4/20/2023



8/8/2023

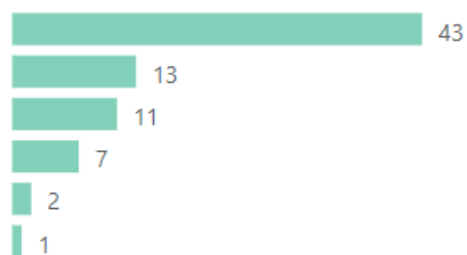


Sensitivity label

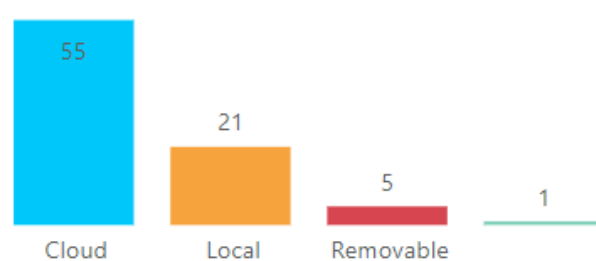


Entra account ID

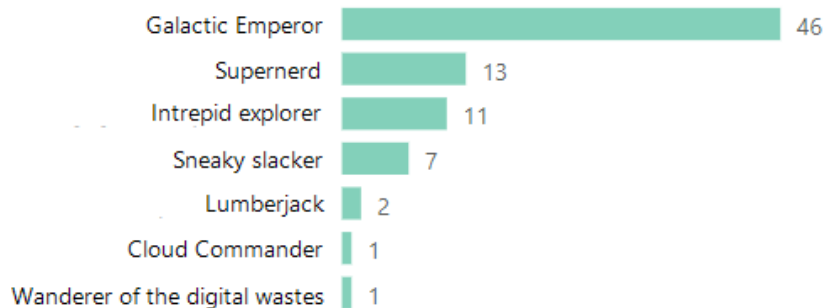
Redacted :)



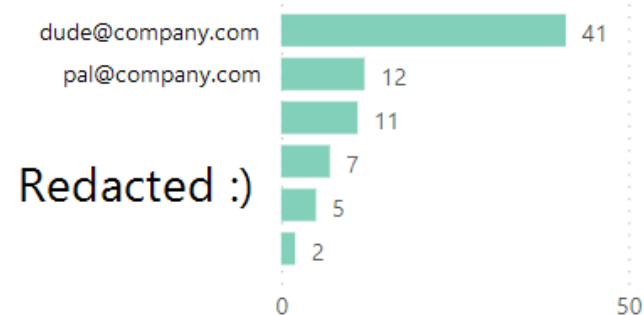
File location



Job title



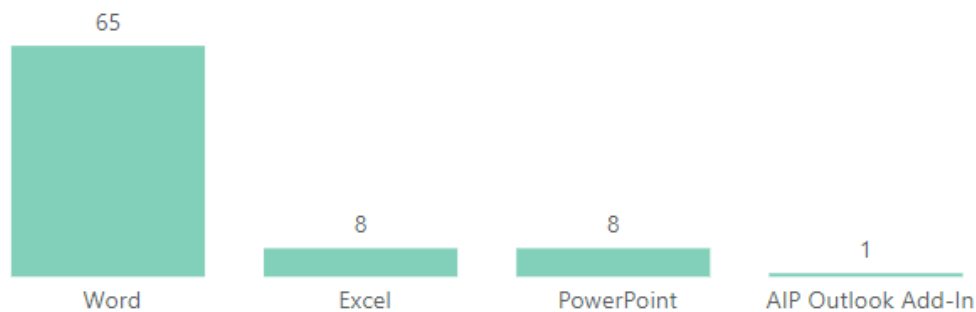
Protection owner



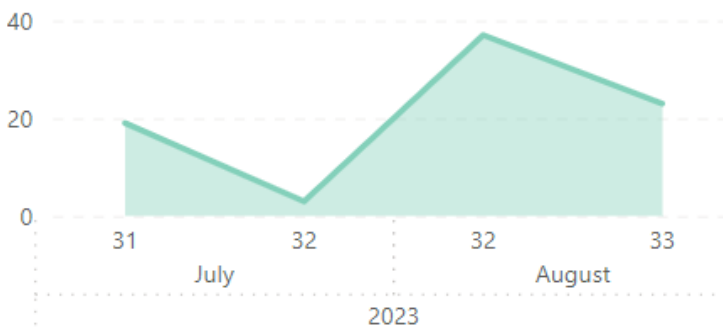
User domain



Application



Events over time



Best practice #6: Ensure visibility

- > Train key people to use the **Activity Explorer**
- > Configure Sentinel connectors



Microsoft Purview Information Protection (Preview)
Microsoft

Labeling events



Microsoft 365 Defender
Microsoft

DLP rule matches
Endpoint events



Microsoft 365 (formerly, Office 365)
Microsoft

Office activities

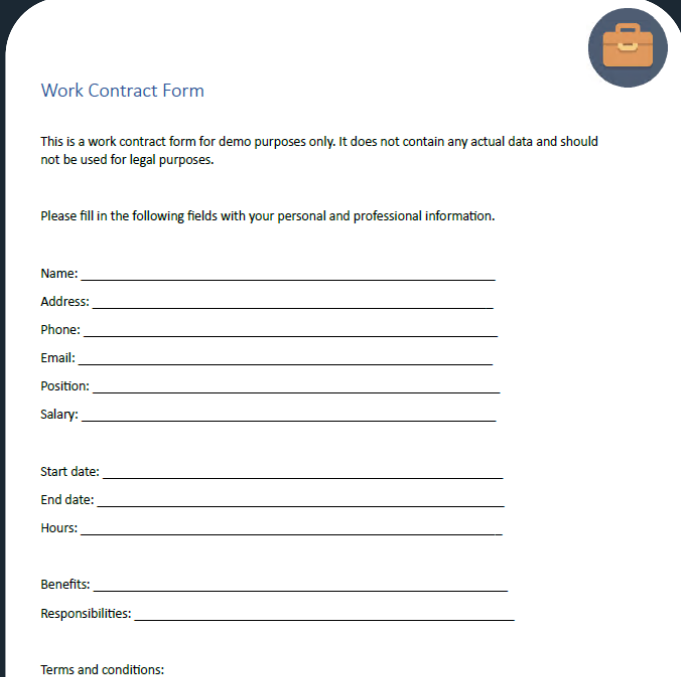


- > [Set up the on-premises MPIP scanner](#)



Best practice #6: Ensure visibility

- > **Document Fingerprints:** an easy starting point for custom SITs
- > Ask HR for work contract templates, Finance & Ops for **project budget planning** and other Excel templates etc.
- > It takes 5min to make a Fingerprint SIT once you have a document
- > Use them for auditing in..
 - Data Loss Prevention rules
 - Defender for Cloud Apps file policies



Work Contract Form

This is a work contract form for demo purposes only. It does not contain any actual data and should not be used for legal purposes.

Please fill in the following fields with your personal and professional information.

Name: _____

Address: _____

Phone: _____

Email: _____

Position: _____

Salary: _____

Start date: _____

End date: _____

Hours: _____

Benefits: _____

Responsibilities: _____

Terms and conditions: _____

Best practice #7: Extend Log Analytics data retention

> Configure 1 year (or longer) **table-level retention** for key data

<input type="checkbox"/> Table name ↑↓	Type ↑↓	Plan ↑↓	Interactive retention ↑↓
<input type="checkbox"/> CloudAppEvents	Azure table	Analytics	1 year
<input type="checkbox"/> MicrosoftPurviewInformationProtection	Azure table	Analytics	1 year

Data retention settings

Workspace settings ⓘ

Use default workspace settings

Interactive retention ⓘ

1 year

[Configure data retention for logs in Microsoft Sentinel or Azure Monitor | Microsoft Learn](#)



Best practice #8: Be mindful of privacy protection

- > Exclude personally-identifying fields from analytics if not *explicitly* required
 - UserPrincipalName
 - DisplayName
 - Etc.
- > Focus on larger trends and guidance to avoid an adversarial mindset
- > **Tip:** Log Analytics supports table-level read access



Stage 3

Build awareness



We generally want to do the right thing..

..as long as we know what is **expected** of us.



Repeated reminders are necessary to build awareness.

Initial training for new employees

Continued **policy tip** reminders during daily work in various contexts

January

February

March

April

...

Your message was blocked due to organization policy

- All Credential Types

Company policy prevents you from sharing suspected credentials sent over Teams. If you have an acceptable business justification, you can override this restriction.

Here's what you can do

Override the policy and send the message. If you think the error, you can also report it to your admin.

- Override and send
Type your justification
- Override and send and report it to my admin

Temporary - OneDrive

https://onedrive.live.com/?id=A7BA3B0E588E2F01%2199644&cid=A7BA3B0E588E2F01

Microsoft 365 Teams Outlook Share

Your organization has protected the content you're trying to drop.

You're about to drop protected content into an unprotected location. To proceed, you must submit an override.

Learn more

Override Cancel

POLICY TIP: Sharing information with internal recipients about projects designated as sensitive is only permitted by providing a business justification. [More Options](#)

	A	B	C	D	E	F	G
	projectName	projectID	summary	projectLead	allocatedBudget	estimatedCompletion	status
1	Elevate	PRJ-005	Create AI-powered personal shopping assistant	John Doe	12500	Q2/CY2024	On track
2	Zenith	PRJ-024	Design sustainable smart cities	Jane Doe	228300	Q3/CY2026	Delayed
3	Nirvana	PRJ-028	Develop teleportation technology	Michael Smith	360000	Q1/CY2023	Completed
4	Aurora	PRJ-072	Create biodegradable packaging	Sarah Johnson	149000	Q3/CY2025	On track
5	Radiance	PRJ-096	Harvest clean energy from sea waves	David Brown	450000	Q4/CY2026	On track
6	Eclipse	PRJ-113	Build self-sustaining agriculture	Lisa Garcia	310000	Q1/CY2024	Delayed



Best practice #9: Consistency is key

Sensitive information type(s)	Scenario	Intent	Exchange Online	SharePoint Online & OneDrive	Teams
All credentials	External sharing	When sharing credentials with external recipients, encryption should be ensured where possible.	This message was detected to contain one or more credentials. It will be automatically encrypted when sent to external recipients.	This message was detected to contain one or more credentials. Please ensure the document isn't exposed to unauthorized recipients.	Sharing credentials in Teams chats with external recipients isn't allowed by company policy. Please consider using secure email instead.

- > Deploy **Policy Tips** widely and early
- > Work with Comms & pilot users to design accessible tips
 - **Avoid all tech jargon**
 - *Explicitly* tell people what is expected of them
- > Document your policy tip texts to stay consistent



Best practice #9: Consistency is key

Bad policy tip:

“Please handle this sensitive information according to company policy.”



Good policy tip:

“This information must only be shared with external recipients over secure email.”




Assume **nobody** remembers what the company policy is.



Best practice #9: Consistency is key

› Localize your Policy Tips to reach new audiences:

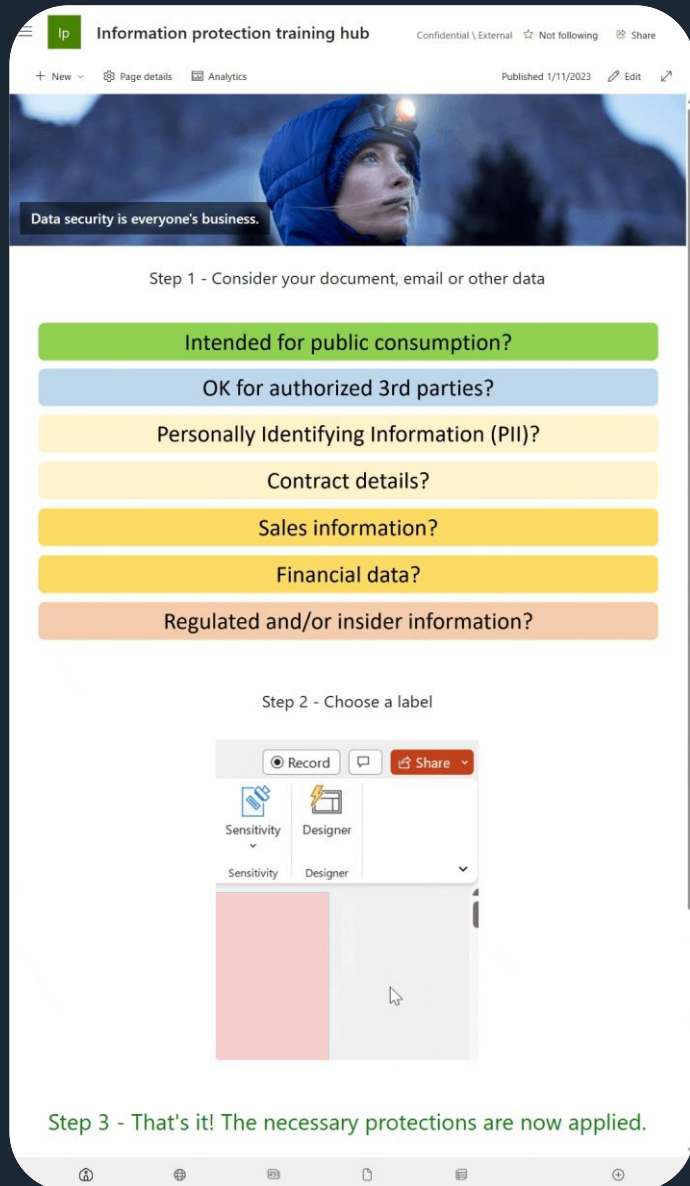


```
$translations =  
"en:Please handle this information responsibly.",  
"fi:Käsittelethän tätä tietoa vastuullisesti.",  
"de:Bitte gehen Sie verantwortungsvoll mit diesen Informationen  
um."  
  
Set-DlpComplianceRule  
-Identity <RuleId>  
-NotifyPolicyTipCustomTextTranslations $translations
```

Reference: [Microsoft Learn](#)



Best practice #10: Build a data security info site, then direct people to it



← Link on Intranet frontpage & in global navigation

← Learn More link in the sensitivity label dropdown menu



Provide users with a link to a custom help page
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. [Learn more about this help page](#)

Configurable per Label Policy

← Guidance link shown when external sharing is blocked

```
Set-SPOTenant -CustomizedExternalSharingServiceUrl  
"https://your-site.here"
```



← Link in email when you upload a file with a higher sensitivity to a site with a lower one

```
Set-SPOTenant -LabelMismatchEmailHelpLink  
"https://your-site.here"
```



Stage 4

Protect & prevent



When something is *explicitly* disallowed..

..it should also not be possible to do by mistake.



Best practice #11: Prepare for encryption

Configure this:



Co-authoring for files with sensitivity labels



Consistent user experience

 Know how to decrypt as well!



```
Unlock-SPOSensitivityLabelEncryptedFile -FileUrl "https://path-to/file.docx"  
-JustificationText "Reason for decryption"
```



[Reference](#)

 + [AIP Super User](#) role enabled & assigned

```
Set-AIPFileLabel "C:\Path\To\file.docx" -RemoveProtection -RemoveLabel  
-JustificationMessage 'Reason for decryption'
```



[Reference](#)



How to Block things without messing up?

Can you **reliably** detect and monitor a scenario that is deemed risky?

No

 Audit

Yes

Are you **confident** that the scenario isn't required in *any* business process?

Yes

 Block

No

 Block w/ override

Analyze justifications

Refine DLP rules



Best practice #12: Configure Endpoint DLP settings

- > Turn on **advanced classification scanning and protection**
 - Gives you access to **document fingerprints, exact data match SITs** etc. on Endpoints
 - Work with network team to determine **bandwidth limits**
- > **Decide & define which browsers should access your sensitive data**
 - If **Chrome** or **Firefox** → Deploy Purview extension to get visibility & control
 - Mark other browsers as unallowed
- > **Configure service domain groups & use them in Endpoint DLP policies**
 - For ex. Approved domains, Unapproved domains, Consumer services
 - Or by department: Services for Legal, Services for Finance
- > Turn on both..
 - **Coverage of network shares & mapped drives**
 - **Just-in-time protection in Allow (Audit) mode**



Wrapping up..

JUST ONE MORE THING...



I PROMISE

The seven golden keys

- > Understand that **data security** is a new kind of **team sport**
- > Avoid **disrupting** business processes at all costs..
- > ..but understand that you'll probably have to do so anyway 😊
- > Design your solution based on **data** - not guesswork
- > Aim for **clarity** and **consistency** in all messaging
- > **Communicate** well & **protect privacy** to build trust
- > **Patience & determination** are your friends

Remember..

The story only begins with sensitivity labels & DLP

Insider Risk Management
Communication Compliance
Container & meeting labeling
New custom info types
Auto-labeling
Trainable classifiers
Data Lifecycle Management
Purview AI Hub

...



Comments or
questions?

Connect with me!

