Securing by default, and training users to update labels to manage exceptions – instead of when to protect

How to secure by default with Purview Data Security?

01 Protect default label from external sharing and beyond

Confidential\All employees

Use a label that **protects for all employees by default**, reducing your risk surface. Control the scope of your deployment by selecting default at the user client level and/or in SharePoint sites.

Derive site label to files

SharePoint default library label provides a contextual option and allow having different defaults based on storage location. Starting Ignite 2024, use the feature linking site labeling to default library label to rapidly scale.

Control how you protect

Use **Data Loss Prevention** to prevent external sharing of the default label and content that is not labeled. Leverage built-in encryption to have the protection traveling with the content.

Auto-label higher sensitivity

Leverage auto-labeling for higher sensitivity, applying additional restrictions.

02 Train users to manage exceptions when sharing

Sharing is an exception

Secure by default while **empowering users to change labels** to permit them to share. Scale exception management with site labeling.

Data Loss Prevention

Inspect content permissible for sharing with sensitive classifiers available in Purview and prevent sensitive sharing with **Data Loss Prevention**.

Report on deviations

Leverage **Insider Risk Management** to find and address labeling deviations and inappropriate usage.

Protect Copilot responses

Copilot responses will carry the highest sensitivity label from content it used to create the response.

Recommended label taxonomy

Public
Public data is unrestricted data meant for public consumption, like publicly released source code and announced financials. Share it freely.

General
Business data that is not meant for public consumption, such as daily work product. Data that can be shared internally and with trusted partners.

Confidential
Sensitive business data crucial to achieving your organizational goals. Limited distribution.

Highly confidential
Your most critical data. Share it only with named recipients.

Label	Auto-labeling	Scope	External guest	Site privacy	Permissions	Default sharing	DLP limits
Public		File, Email	Allowed	N/A	N/A		
General [1]	Email default	File, Email, Meetings, Sites	Allowed	Private or Public	N/A	People in <company>	Block anyone
Confidential\All employees [2]	Documents default Yes (retroaction)	File, Email, Meetings, Sites	Not allowed	Private	FTE	People in <company>	Block anyone, Block external
Confidential\Specific People [1*]		File, Email, Meetings, Sites	Allowed*	Private	User specified	Specific People	Block anyone
Confidential\Internal exception [2,3]		File, Email, Meetings, Sites	Not allowed	Private	N/A	Specific People	Block anyone, Block external
Highly Confidential\All employees [4,5]	Optional	File, Email, Meetings, Sites	Not allowed	Private	FTE	Specific People	Block anyone, Block external
Highly Confidential\Specific People [5]	Yes (SIT)	File, Email, Meetings, Sites	Not allowed	Private	User specified	Specific People	Block anyone, Block external
Highly Confidential\Internal exception [5]		File, Email, Meetings, Sites	Not allowed	Private	N/A	Specific People	Block anyone, Block external

Notes:
1. Site label for external sharing with partners (* for customers with SAM licenses, Specific People is recommended, more details in 'iterate with new labeling scenarios')Default label for sites, documents
2. Provides a means for end users to lower severity and share externally. Leverage DLP/IRM to manage deviations/risks.
3. Leverages auto-labeling to define what constitute highly confidential for the organization and restrict sharing further
4. DLP for Copilot label candidates

Last updated: December 10, 2024

Secure by default with Microsoft Purview

Foundational

Start with recommended labels

Activities

- Start with default labels and protection at file and site level
- Turn on data security pre-requisites and adv. analytics
- Train users on managing exceptions
- Turn on DLP for labeled content

Outcomes

- M365 new/updated content protected

Efforts

- 1 week

Managed

Address files with highest sensitivity

Activities

- Manually configure priority sites default library labeling
- Autolabeling for credentials and contextual conditions
- Turn on DLP for content that is not labeled
- Turn on Adaptive Protection and data leak behavioral rules

Outcomes

- M365 priority content protected

Efforts

- 2 weeks

Optimized

Expand to your entire M365 data estate

Activities

- Auto-label sensitive files on clients (low thresholds)
- Simulate auto-labeling sensitive files at rest
- Reduce false positives with advanced classifiers
- Automate and improve M365 protection to historical and in use data

Outcomes

- M365 historical content protected

Efforts

- 2 weeks iterations

Strategic

Operate, expand, and retroactive actions

Activities

- Operational review of user labeling behaviors
- Iterate with new labeling scenarios
- Set up accountability chain and lifecycle management
- Extend protection to Azure SQL and non-M365 storage

Outcomes

- Protection beyond M365

Efforts

- Situational

Deployment guide available: https://aka.ms/PurviewDeploymentModels/SecureByDefault

Last updated: December 10, 2024

FAQ

- **Does this replace the "Crawl, Walk, Run" approach or the only deployment method?** No, this is an alternative method to deploy labeling at scale and secure organization by default. Review your organization requirements and adapt configurations to your needs.
- **Do I need to encrypt my default labels?** Not necessarily, or not necessarily for all users. While encryption will protect your information wherever it travels, DLP can for example be used more effectively on labeled and unlabeled content before having to look at sensitive classification.
- **Can I start without encryption and add it later?** Absolutely, with the understanding that the previously labeled content won't be automatically relabeled. As with the previous FAQ, having DLP policies on the default label helps you secure by default.
- **Do I need to migrate/relabel my existing content?** No. You could optionally decide on your DLP policies to prevent those label from being shared externally, requiring users to change the label if they need to before sharing. If you do not intend to use the 'old' labels further, you can remove them from the publishing policies.

Thank you

Microsoft Purview – Deployment models

Learn more

Read the detailed guide for this model at https://aka.ms/PurviewDeploymentModels/SecureByDefault

Learn more about our Microsoft Purview Deployment models at https://aka.ms/PurviewDeploymentModels

Appendix & notes from engineering

Addressing traditional labeling concerns

Traditional concerns or implementation delays	How to accelerate resolution
Complex taxonomy / label schema	▪ Recommended labels with intuitive naming based on protection rather than regulations
Encryption (impact to LOB applications and collaboration)	▪ Set tenant default to General ▪ Set SharePoint default to Confidential\All employees with encryption ▪ General allows users to remove encryption, when necessary. Risks managed via DLP and IRM ▪ SharePoint should be the primary location for sharing with external partners and set container label to "General"
Perfecting auto-labeling before starting	▪ Instead, start now with intelligent defaults to address most of your content (new/updated from today) ▪ Iterate with auto-labeling for your most sensitive content such as credentials and regulatory requirements ▪ Iterate with additional auto-labeling to retroactively address all previously created content with contextual conditions
Concerns about Site Owners changing container or default library labels	▪ Implement a chain of accountability and leverage audit/reporting to identify deviations
Securing "tented projects"	▪ Sensitivity labels secured with UDP and published to relevant users only (suggest limiting to <15 labels) ▪ Coming to preview with SharePoint Advanced Management: Extend SharePoint Permissions with sensitivity labels

Notes from engineering

Label schema recommendations

- **Do** use intuitive names that means something to users and how it protects
- **Do** keep the list of labels to no more than 5x5 (5 parent labels, 5 children labels)
- **Do** use container labels for all your SharePoint/Teams sites
- **Do** apply default library labeling and have your labeling derived from container
- **Do** plan for tenant default to General to prevent breaking automated business processes

- **Do** plan for defaults with encrypted content for all employes saving in SharePoint
- **Do** plan for unrestricted labels to address encryption challenges
- **Do** plan DLP and IRM policies for unrestricted labels
- **Do** inherit label from email attachments

- **Don't** mix conflicting terms such as confidential and restricted
- **Don't** wait for auto-labeling perfection to start with better defaults
- **Don't** wait on label exceptions (i.e.: tented projects, specific needs) to start with better defaults

Notes from engineering

Container and file labeling at scale and reduce automatic oversharing

- **Container labels** are a **must-have** for all your sites.
- Leverage SharePoint Admins and/or **Graph API to address sites without container labels**
- **Default your sites to private** privacy settings, and use **company shareable links** instead, providing a good balance between privacy and collaboration
- **Automate your default library label** configurations with templates or Graph API [1]

- **Auto-Labeling** is used to **label historical content** and/or to **catch exceptions** surrounding sensitive information types
- Set up an **auto-labeling rule on "All Credential Types"** and set to Highly Confidential\Specific People to reduce oversharing of credentials
- **Leverage contextual condition** such as **file properties or file type** to address historical content and set to Confidential\All Employees

Notes:

1. Keep a lookout on our public roadmap for upcoming capabilities automating this setting in the future

Notes from engineering

Training end users

Focus training on:

- Understanding why your organization switched to a secure by default model
- How users can change sensitivity label when external sharing is required
- Support channels readiness
- How and where to report challenges due to new protection in place

Considerations

- Create a “Learn more about” page in a SharePoint communication site, link this page in your label publishing policy.
- Raise awareness early with email communications
- Progressive deployment by departments, with quick iterative learnings before new deployment waves