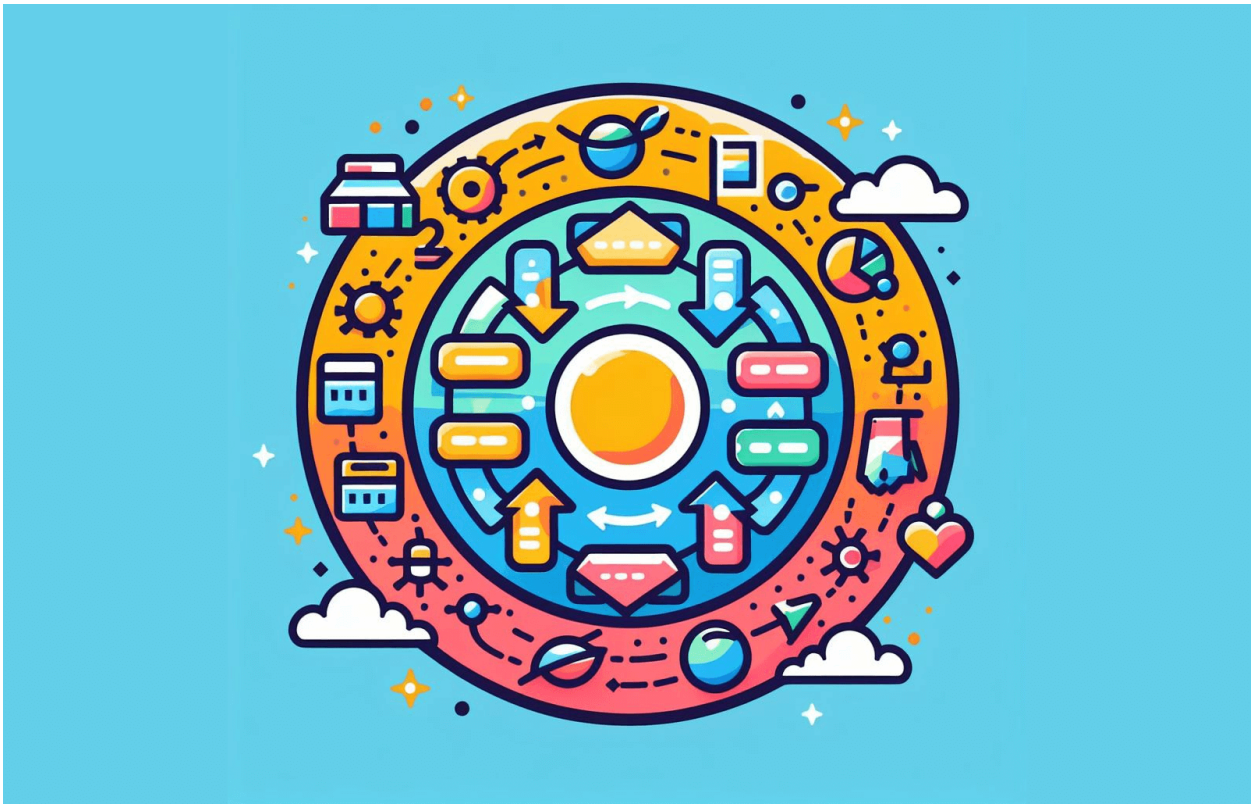
Empowering employee self-service with guardrails: How we're using sensitivity labels to make Microsoft more secure

Apr 3, 2024 | Lukas Velush



By creating a rigorous system of sensitivity labels that align with different levels of protection across our data estate, we're minimizing data loss and enabling autonomy for our employees.

At Microsoft, empowering our employees to do their best work means trusting them with self-determination. But to do that safely, we need clear data loss prevention systems in place.

We describe it as self-service with guardrails.

Giving employees that level of freedom relies on a robust governance strategy across our data estate that features employee-facing sensitivity labels for Microsoft 365 groups, SharePoint sites, Microsoft Teams, Viva Engage communities, and any other workspace or file employees create and use. The result of good governance is that employees can

confidently take action in a self-service environment without the risk of revealing sensitive information.

If you're considering updating your organization's governance strategy, our work in this space can be a roadmap for your journey.

[Learn how we're using sensitivity labeling to secure our meetings in Microsoft Teams Premium. Find out how we use self-service sensitivity labels in Microsoft 365. Check out how we're getting the most out of generative AI at Microsoft with good Governance.]

We had to really step back and think about data delineation in a way that's meaningful to the business and our employees. Labeling provides a way for us to impose policies onto objects and containers to prevent or contain any oversharing of sensitive content.

— David Johnson, principal PM architect, Microsoft Digital

What's at stake: The importance of getting self-service right

To operate according to zero trust principles, we need a coherent system that lets us see, label, and protect data. Otherwise, the burden of data loss prevention falls solely on employees, who would have to exercise individual discretion whenever they're deciding how to house and share potentially sensitive content.

That's a heavy burden to put on people every time they deal with working files.

"We had to really step back and think about data delineation in a way that's meaningful to the business and our employees," says David Johnson, principal PM architect for Microsoft Digital (MSD), the company's IT organization. "Labeling provides a way for us to impose policies onto objects and containers to prevent or contain any oversharing of sensitive content."

Aside from protecting internal content, customer data, and proprietary information, the principal risk is introducing vulnerability into our data estate by leaving access credentials out in the open. For example, internal documentation might include intellectual property, like source code.

"We have a lot of security investments in protecting our data centers and sources because they're where our most sensitive information lives, and credentials are a big part of

accessing them," says Maithili Dandige, partner group product manager with Microsoft Security and Compliance.

If malicious actors can access those credentials or other sensitive information, they can do a lot of damage. Properly classifying, labeling, and protecting files and containers is the best way to ensure sensitive information and credentials don't get compromised.

User-centric sensitivity labels

Our IT professionals within MSD—the organization that supports, protects, and empowers the company through technology—collaborated with a cross-disciplinary team to get our governance structures right.

"We spent a massive amount of time with the oversight committee," says Faye Harold, principal program manager for information protection services within Microsoft Security and Risk. "That involved our legal team, HR, security, and MSD to define what each label meant."

It's important to strike a balance between the depth necessary for supporting an array of data governance controls and the simplicity to ensure labeling isn't burdensome for users.

At Microsoft, we use four labels for container and file classification:

- **Highly confidential**: We only share Microsoft's most critical data with named recipients.
- **Confidential**: Any items crucial to achieving Microsoft's goals feature limited distribution on a need-to-know basis.
- **General**: Daily work like personal settings and postal codes can be shared internally throughout Microsoft.
- **Public**: We share unrestricted data meant for public consumption freely. That includes information like publicly released source code and openly announced financials.

The way to approach sensitivity labeling is to ask what problem it solves. Labeling dictates the automated controls you apply to certain items, like encryption, watermarking, or whether employees can share an item with someone outside our organization.

— Maithili Dandige, partner group product manager, Microsoft Security and Compliance

---

The administrators responsible for workspaces like SharePoint sites set default labels. That serves as a foundation for appropriate access and circulation for objects within those containers. It takes the burden of labeling off employees.

“The way to approach sensitivity labeling is to ask what problem it solves,” Dandige says. “Labeling dictates the automated controls you apply to certain items, like encryption, watermarking, or whether employees can share an item with someone outside our organization.”

The sensitivity labels users and admins apply map to several different categories of policies that anticipate and mitigate data loss and risk. They communicate four key areas:

- **Privacy level**. Labels determine whether the workspace is broadly available internally or is a private site.
- **External permissions**. Guest allowance is administered via the group’s classification, allowing specified partners to access teams when appropriate.
- **Sharing guidelines**. We tie important governance policies to the container’s label. For example, can an employee share this workspace outside of Microsoft? Is this group limited to a specific division or team? Is it restricted to specific people? The label establishes these rules.
- **Conditional access**. While not implemented at Microsoft, tying identity and device verification to container labels introduces additional governance controls.

Within MSD, we’ve put a lot of thought into how each of our labels aligns with relevant policies. For example, when a container receives the default label of “Confidential,” guest membership and sharing are disabled. That provides rights protection for the file, even if it leaves the SharePoint site where the employee created it. You can see more of the logic behind our sensitivity labels and their policies below.

Mapping sensitivity labels to information protection policies

	Public	Private
Privacy	• Membership to Group is open; anyone can join. • "Everyone except external guest" ACL onsite; content available in search to all tenant.	• Only owner can add members. • No-access beyond the Group Membership until someone shares or changes permissions.
	Allowed	**Not Allowed**
External guest policy	• Owners (only) can add guests as members to a group. • Members can share files to "specific people" outside of tenant.	• Owners are not allowed to add guest members to group. • No file sharing to guests.

What users will see when they create or label a Team, Group, or Site

Parent label	Child label	Container/item label or both	External guest policy	Privacy policy options	Current AAD mapping	Note
General		Both	Allowed	Private or public	General	Item default (current)
Confidential	Internal only	Container	Not allowed	Private	Confidential	Container default (new)
	Internal and NDA external	Container	Allowed	Private	Confidential	AAD container default (today)
Highly confidential	Internal only	Container	Not allowed	Private	Highly confidential	

This chart shares the logic behind the different policies at work, all prompted by our different sensitivity labels within Microsoft 365.

If a container owner needs different policies for a set of files to provide greater external access, they can self-service new groups without accidentally violating our governance practices.

Microsoft Purview, our suite of data estate management tools, is central to these governance efforts. It accomplishes three sets of tasks: mapping our labeling structure onto the relevant policies, verifying them against our standards, and backstopping self-service data loss prevention practices through automation.

Automation is particularly useful. We've configured Microsoft Purview Information Protection to scan automatically for wayward credentials, malicious user behaviors, and other sensitive information in items without the proper protections. When Purview detects

a violation, our governance team receives alerts that prompt them to contain the risk by upgrading an item's sensitivity label or requiring employees to remedy the issue.

The result is a system that allows flexibility for employees to self-manage their digital workspaces while providing guardrails that help our governance experts take appropriate actions without overtaxing their time and resources.

A blueprint for effective data governance

So how can you start your own governance journey? Many of the lessons we've learned will be adaptable across different business settings.

Your labeling, policies, and overall governance strategy won't be identical to ours. But by putting thought into your organization's unique needs and the problems you're trying to solve, the labeling features of Microsoft 365 and the data governance capabilities provided by Microsoft Purview will have most of the tools you need without having to build solutions from scratch.

Break things down into where your data is as an overall estate, how it's currently protected, and the most precious data that's unprotected. Then you can form a plan.

— Faye Harold, principal program manager for information protection services, Microsoft Security and Risk

---

Start by getting a firm grasp on the condition of your data estate.

"Break things down into where your data is as an overall estate, how it's currently protected, and the most precious data that's unprotected," Harold says. "Then you can form a plan."

After you have a solid overview of your data estate, you can apply a concerted strategy to labeling and governance. Here's a ten-step blueprint to consider for structuring your efforts.

Ten steps for getting tenant data governance right

We think you might find it easier to label your containers before you start thinking about how to label emails and files or think about auto-labeling.

1. Give employees the ability to create new workspaces across your Microsoft 365 applications. By maintaining all data on a unified Microsoft 365 tenant, you ensure that your governance strategy applies to any new workspaces.

2. Limit your taxonomy to a maximum of five parent labels and five sub-labels. That way, employees won't feel overwhelmed by the volume of different options.

3. Make your labels simple and legible. For example, a "Business-critical" label might imply confidentiality, but every employee's work feels critical to them. On the other hand, there's very little doubt about what "Highly confidential" or "Public" mean.

4. Label your data containers for segmentation to ensure your data isn't overexposed by default. Consider setting your container label defaults to the "Private: no guests" setting.

5. Derive file labels from their parent container labels. That consistency boosts security at multiple levels and ensures that deviations from the default are exceptions, not the norm.

6. Train your employees to handle and label sensitive data to increase accuracy and ensure they recognize labeling cues across your productivity suite.

7. Trust your employees to apply sensitivity labels, but also verify them. Check against data loss prevention standards and use auto-labeling and quarantining through Microsoft Purview automation.

8. Use strong lifecycle management policies that require employees to attest containers, creating a chain of accountability.

9. Limit oversharing at the source by enabling company-shareable links rather than forcing employees to add large groups for access. For highly confidential items, limit sharing to employees on a "need-to-know" basis.

10. Use Microsoft Graph Data Connect extraction in conjunction with Microsoft Purview to catch and report oversharing after the fact. When you find irregularities, contain the vulnerability or require the responsible party to repair it themselves.

Overall, it's important to be thoughtful about your governance strategy at each stage of this process. For a deeper dive into how we tackled these challenges and inspiration for your own initiatives, review our technical overview of Microsoft's self-service sensitivity labeling efforts.

David Johnson, Faye Harold, and Maithili Dandige helped us establish and implement our sensitivity labeling strategy internally here at Microsoft.

Extending governance throughout our productivity suite

Since we implemented our governance strategy and sensitivity labeling taxonomy, we've extended it internally throughout our Microsoft 365 productivity suite to solidify data protection across several different scenarios. Each one showcases a way that a unified data estate with consistent governance empowers employees and unlocks new technologies as it keeps our company's data safe.

- Proper governance and labeling ensure that Copilot for Microsoft 365 stays within bounds when sourcing information in support of employee productivity.

- Since the widespread emergence of generative AI and the application of these technologies across Microsoft, good governance is helping us get the benefits of this technology without risking overexposure through an information free-for-all.
- We've added a new layer of security to Microsoft Teams Premium meetings that activates specific configurations based on a meeting's level of sensitivity.
- Our Microsoft Teams meeting data is now subject to robust retention rules determined by the labels we apply, with implications for recordings, transcriptions, and intelligent recaps via Copilot.

These are just a few examples of how sensitivity labels paired with effective data governance are unlocking new capabilities across the Microsoft 365 suite, and our journey continues. By taking steps to apply good governance to your own data estate and building an effective labeling strategy, you can enable self-service for your employees and empower self-determination while maintaining security and minimizing risk.

Key takeaways

Here are some tips for getting started with labeling at your company:

- Assemble an oversight committee: Bring in professionals from all relevant disciplines, including HR, legal, security, IT, and anyone else who can share relevant expertise.
- Make a plan: Be intentional about addressing your unique needs around control and governance.
- Self-service requires accountability: Set up systems like attestation, site permissions reports, and guest access reviews that trace back to employees.
- People tend to take the easiest path: Make the IT-preferred path the best and easiest so that it doesn't erect roadblocks.
- Educate employees: Support your labeling implementation by making sure users know how and when to share files.
- Encourage focused sites: Site owners don't always have adequate knowledge of what they host.
- Make it simple: Ensure the system you develop makes sense to employees in the easiest possible terms.

Try it out

Get started with labeling at your company.

Related links

- Learn how we're using sensitivity labeling to secure our meetings in Microsoft Teams Premium.
- Find out how we use self-service sensitivity labels in Microsoft 365.
- Check out how we're getting the most out of generative AI at Microsoft with good Governance.

We'd like to hear from you!

Want more information? Email us and include a link to this story and we'll get back to you.

Please share your feedback with us—take our survey and let us know what kind of content is most useful to you.

Tags: digital transformation, Microsoft 365, security, Zero Trust