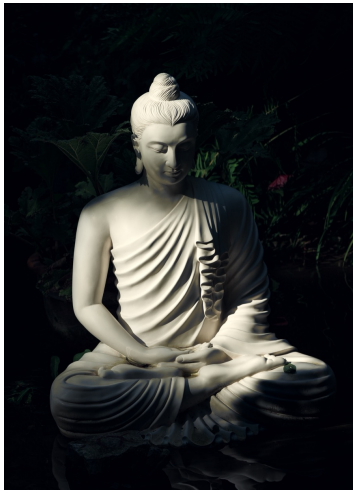
Simplifying Data Protection:

Leveraging TLP 2.0 for Sensitivity Labels in Small Businesses

Workplace Ninja
User Group Denmark



Microsoft CERTIFIED EXPERT

Microsoft CERTIFIED TRAINER MCT

MVP Microsoft® Most Valuable Professional

Mats Warnolf

Demo time

Information classification

Information classification organises data into clear categories (like traffic lights guiding drivers), so everyone knows when to stop, go or slow down.

By labelling information as Public, Internal, Confidential or Restricted, organisations protect sensitive details, meet compliance needs and help people share the right data with the right audience.

Senstitivity labels might be useful for:

Contracts & suppliers – protect agreements so only finance/management can access

Customer offers & pricing – safeguard quotes and price lists from unauthorised sharing

HR documents – ensure payroll, contracts, and medical records stay HR-only

Product ideas & R&D – keep innovations confidential from day one

Board minutes – restrict agendas and minutes to directors only

NIS 2 Directive

Under NIS 2, organisations must know which information is sensitive, protect it accordingly, and be able to prove it.

We must:

- Identify & Classify – Define categories such as Public, Internal, Confidential, Strictly Confidential to match your risk profile.
- Apply Protection – Restrict access, enforce encryption, and apply “need-to-know” policies automatically.
- Maintain Control – Protection travels with the document, even when shared outside your organisation.
- Track & Audit – Built-in logging shows who accessed the file, when, and under what label.
- Support Incident Response – Quickly identify if leaked or breached data was protected and how.

~~The complecs…~~

~~The complicatedness…~~

Labels are hard!

Sensitivity labels let you

- Mark your data
- Use Data Loss prevention
- Configure external sharing settings for Teams/Sites
- Encrypt contents
- Use Rights Management to prevent printing
- Force secure settings through Conditional Access Policies
- …

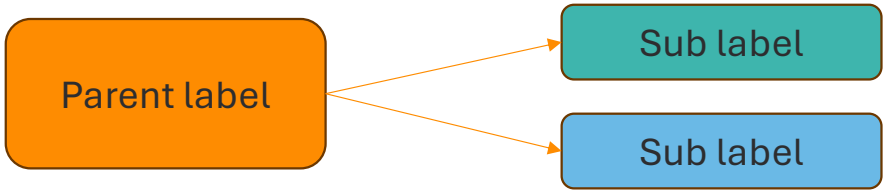
Challenges

This is what we get out of the box

Name	Priority	Scope	Created by	Last modified
Personal	0	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:48
Public	1	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:49
General	2	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:52
Anyone (unrestricted)	3	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:52
All Employees (unrestricted)	4	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:53
Confidential	3	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:57
Anyone (unrestricted)	6	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:29:57
All Employees	7	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:45:32
Trusted People	8	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:30:05
Highly Confidential	4	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:30:10
All Employees	10	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:45:32
Specified People	11	Files & other data assets, E...	Microsoft Corpor...	21 Jul 2025 23:30:12

Labels and sublabels

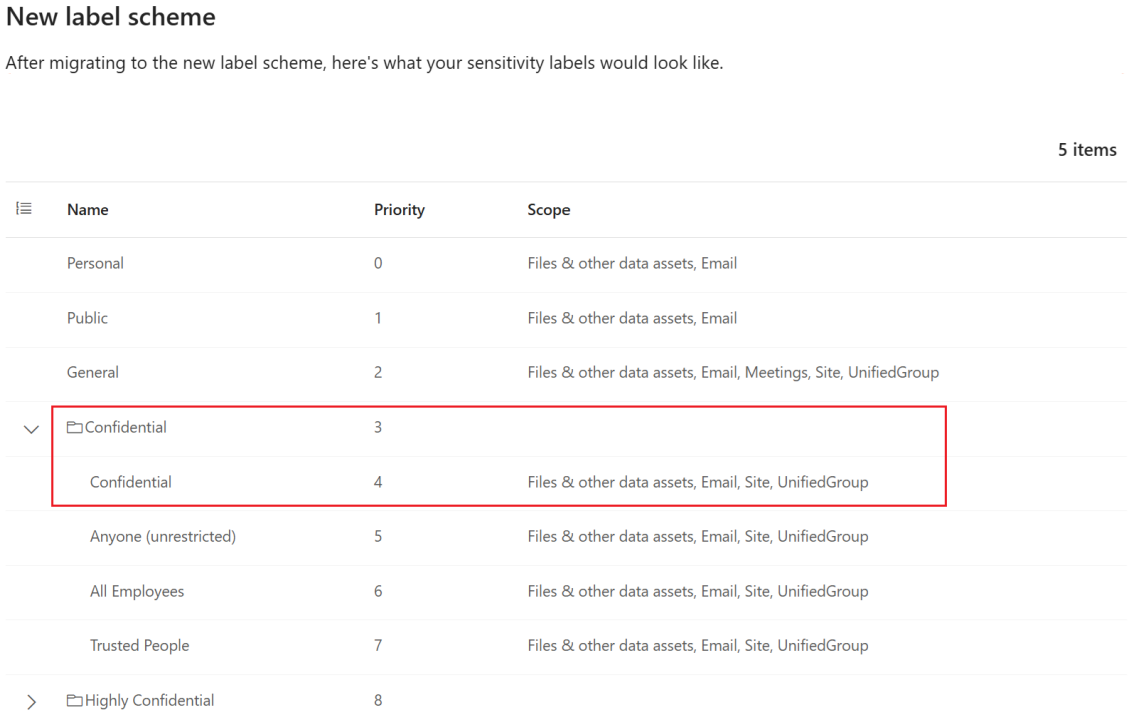
- Inheritance simplifies the setup of labels
- If a label has subordinate labels we refer to it as a parent label
- Parent labels have settings configured but can’t be applied to objects
  - Sublabels inherits these settings from the parent
  - Sublabels can add specific settings to inherited settings
  - Sublabels CAN be applied to objects



Label Groups.

NEW

- **Label Groups replace parent labels**
  Simple categories, not labels themselves
- **Cleaner admin experience**
  No settings on groups, fewer mistakes
- **Easier to reorganise**
  Move labels between groups without breaking anything
- **Same user experience**
  End users still pick real labels, nothing new to learn



New label scheme

After migrating to the new label scheme, here's what your sensitivity labels would look like.

5 items

Name	Priority	Scope
Personal	0	Files & other data assets, Email
Public	1	Files & other data assets, Email
General	2	Files & other data assets, Email, Meetings, Site, UnifiedGroup
Confidential	3	
Confidential	4	Files & other data assets, Email, Site, UnifiedGroup
Anyone (unrestricted)	5	Files & other data assets, Email, Site, UnifiedGroup
All Employees	6	Files & other data assets, Email, Site, UnifiedGroup
Trusted People	7	Files & other data assets, Email, Site, UnifiedGroup
Highly Confidential	8	

Where can I use sensitivity labels?

Where you can apply a label, the essentials.

- **Individual Files & Emails**
  - Word, Excel, PowerPoint (desktop/web/mobile)
  - Outlook emails and attachments
  - PDFs (Adobe support + AIP add-in)
  - Text & image files (.txt, .csv, .jpg, etc.)
- **Containers**
  - Microsoft 365 Groups
    - Microsoft Teams
    - SharePoint Team Sites
    - Planner plans *(inherits from Group/Team)*

These are the everyday touchpoints where labelling directly supports collaboration, sharing and access control.

Labelling in Meetings, AI and Business Intelligence

- **Meetings & Communication**
  - Teams meetings (encryption, lobby, recording settings)
  - Teams chats *(preview)* (restrict copy/paste, forwarding)
  - Channel messages *(label via Team container)*
- **AI & Analytics**
  - Microsoft Copilot
    - Exclude or include content based on label
    - Automatically sets the same label that the source data has.
  - Power BI
  - Block export, show label visually, DLP integration

Labelling now extends to your AI, meeting data and dashboard.

Advanced labelling for Security and Automation

- **Security & Governance Integration**
  - Defender for Cloud Apps (block uploads to unsanctioned apps)
  - DLP **(**apply or enforce based on label)
  - Insider Risk Management (trigger alerts)
  - eDiscovery & Audit (label = searchable classification)
- **System & Infrastructure**
  - File Explorer (manual labelling via AIP client)
  - Unified Labelling Scanner (bulk labelling on file shares)
  - Custom apps (via MIP SDK)

Labelling powers policy automation, security alerts, and governance.

Planning the labels

What is a classification scheme?

A classification scheme is a a set of rules that specifies what labels should be applied to which objects.

These labels help people know:

- Who should see the information
- How it should be protected
- What rules apply when sharing or storing it

A good classification scheme is simple, consistent, and easy for everyone to understand and use.

Sample classification scheme

Parent Label	Sublabel	Description	Typical Use Cases	Protection Settings
Confidential	Confidential – Executive	Information for the executive team only. Strictest confidentiality.	CEO communications, board papers, high-risk M&A, strategic legal cases	Encryption, limited to exec security group, watermark, external sharing blocked
	Confidential – HR	Sensitive HR content involving individuals or legal matters.	Disciplinary cases, salary reviews, investigations, medical leave	Encryption, HR group access only, watermark, no external sharing
	Confidential – Legal	Legally privileged content.	Contracts under negotiation, litigation files, NDA-covered info	Encryption, legal team only, watermark, external sharing disabled
	Confidential – Customer	Information about customers protected under data privacy or contractual terms.	Customer PII, sensitive commercial agreements, health info	Encryption, customer data team access, tracking, expiry, watermark
Restricted	Restricted – Projects	Sensitive internal content tied to projects or strategic initiatives.	High-impact internal projects, vendor selection, budget planning	Encryption, team-limited access, watermark, sharing to trusted domains only
	Restricted – Finance	Pre-release or sensitive financial data.	Forecasts, budget drafts, investment evaluations	Encryption, CFO group access, watermark, expiry
	Restricted – Audit	Internal or external audit-related documentation.	Compliance assessments, security reviews, auditor notes	Encryption, access for audit teams only, watermark, activity logging
Internal	Internal – General	Everyday internal communication and documentation.	Internal memos, intranet drafts, meeting minutes	Internal users only, watermark optional, external sharing disabled
	Internal – Product	Internal product or roadmap documentation.	Feature specs, roadmap decks, engineering notes	Internal only, watermark optional, sharing limited to Microsoft 365 groups
	Internal – Training	Content for internal knowledge or skills training.	eLearning, guides, onboarding materials	Internal only, no watermark needed
Public	Public – Approved	Content cleared for public consumption.	Website content, brochures, press releases	No encryption, no access restriction
	Public – Draft	Content intended for eventual publication but still under review.	Marketing drafts, PR text in review, draft reports	Internal access only, optional watermark, no external sharing

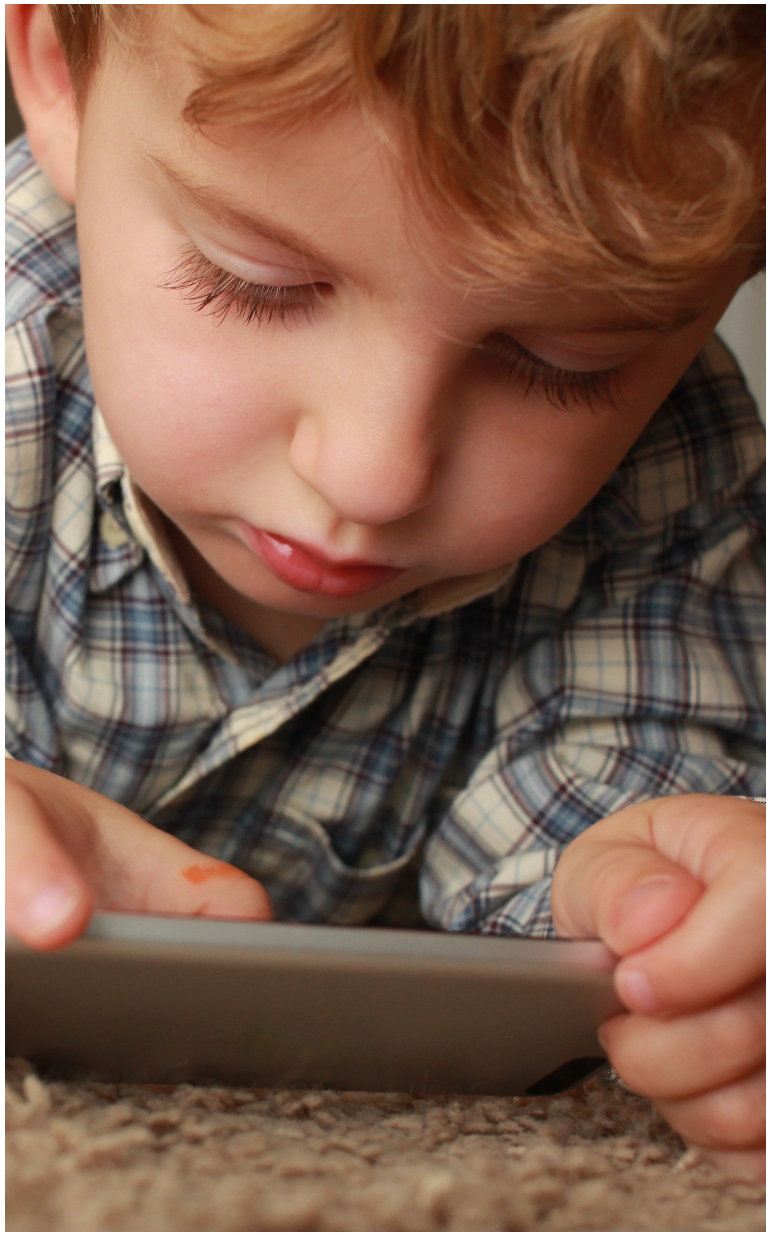
Scoped classification schemes

Parent Label	Sublabel	Description	Typical Use Cases	Protection Settings
HR – Confidential	Employee Relations	Personal HR cases, complaints, disciplinary actions	Disciplinary records, performance issues	HR-only, encryption, watermark, no external sharing
	Salary & Benefits	Compensation data and benefits	Salary tables, bonus plans, benefits packages	HR-only, encryption, watermark
	Recruitment	Sensitive candidate information	CVs, interview notes, background checks	HR+Hiring managers, encryption, limited sharing
R&D – Confidential	Intellectual Property	Proprietary inventions, algorithms, code	New product designs, source code, prototypes	Encryption, R&D-only, strict access, watermark
	Research Data	Ongoing experiments or technical reports	Lab results, technical memos	R&D group only, watermark, internal sharing only
	Collaboration (Partners)	Shared work with external R&D partners	Joint research projects, shared findings	Encryption, limited external domains, watermark
Finance – Confidential	Forecast & Budget	Non-public financial projections	Forecast models, budget reviews	Encryption, CFO team only, watermark
	Audit & Compliance	Documentation for internal or external audits	SOX documentation, audit reports	Access for audit/finance only, activity tracking
	Investor Communication (Draft)	Pre-release investor or board-level comms	Drafts of earnings releases, board reports	Encryption, watermark, draft disclaimer
Marketing – Internal	Campaign Planning	Planning documents for future campaigns	Campaign calendars, concept drafts	Internal access only, no external sharing
	Partner Materials (Pre-approved)	Materials to be shared with marketing partners	Brochures, banners, sales one-pagers	Shared externally with trusted partners, watermark optional
	Public – Approved Content	Finalised, published marketing content	Published blogs, website content, whitepapers	No protection, available to all
Legal – Confidential	Contractual Documents	Contracts, NDAs, service agreements	Signed contracts, standard terms	Legal group only, encryption, retention policy
	Litigation Material	Legal disputes or court documents	Evidence packs, legal arguments	Legal only, encryption, strict retention, do not delete policy
	Privileged Advice	Internal legal opinions or counsel advice	Legal analysis, policy reviews	Legal only, encrypted, watermark

The human factor

- Cognitive overload (too many choices)
- Lack of awareness or understanding
- Labelling doesn’t match how people work
- Confusion around responsibilities
- Inconsistent usage across organization
- Labelling takes time (or feels like it does)
- Fear of mislabelling or getting into trouble
- No visible benefit to the user

How can we make it easier?



The need for a universal language

A shared understanding of:

- What each label means
- When and how to use it
- Why it matters

Could a simplified labelling scheme be a solution?

- **Reduces cognitive load**
  Fewer choices = faster decisions = higher adoption.
- **Less training required**
  Users don’t need a manual to classify a document.
- **Fits real-world behaviour**
  Most users don’t deal with 5–7 nuanced levels of sensitivity.
- **Easier to maintain**
  Admins avoid policy sprawl and label confusion.
- **Supports automation**
  Simpler labels are easier to map to auto-labelling rules.
- **Improves consistency**
  Fewer options = fewer misclassifications.
- **Faster rollout**
  You don’t need to run a label awareness campaign for every department.
- **Good enough is great**
  A simple system used by 90% is better than a perfect system used by 10%.
- **Easier to evolve**
  You can always add scoped labels later as maturity grows.

Traffic Light Protocol to the rescue

TLP was designed for the IT Security Industry

"The Traffic Light Protocol (TLP) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration"

Five labels tells the recipient **how the information can be shared:**

- **TLP:RED** Recipient only
- **TLP:AMBER+STRICT** Organization only
- **TLP:AMBER** Organization and its clients
- **TLP:GREEN** Within the Security Community (not publicly)

TLP:CLEAR Publicly

"TLP-labeled documents MUST indicate the TLP label of the information, as well as any additional restrictions, in the header and footer of each page. The TLP label SHOULD be in **12-point type or greater** for users with low vision. It is recommended to right-justify TLP labels."

TLP – The good, the bad and the interesting

The Good

- Simplicity
- Shared, well documented model
- Purpose driven
- Colour coded (visual)

The Bad

- Limited nuance
- Not originally designed for internal content
- May clash with existing classification
- **TLP:RED** is problematic

The Interesting

- You can hybridise it
- Good fit for external collaboration
- Mental Model: Sharing, not secrecy

Two approaches to implementation

1-1 mapping

TLP Level	SME Label	Intended Audience
TLP:CLEAR	Public / General Release	Anyone (internal & external)
TLP:GREEN	Internal	Company + trusted partners
TLP:AMBER	Need-to-Know / Departmental	Company + business-critical external sharing
TLP:AMBER+STRICT	Confidential / Org-Only	Internal only
TLP:RED	Strict Confidential / Named	Specific individuals only

Simplified

TLP Level	SME Label	Intended Audience
TLP:CLEAR	Public / General Release	Anyone (internal & external)
TLP:GREEN	Internal	Company + trusted partners
TLP:AMBER	Department X Only	Internal to department
TLP:RED	Strict Confidential / Named	Specific individuals only

Alex original suggestion

TLP Level	SME Label	Intended Audience
TLP:CLEAR	Public	Anyone (internal & external)
TLP:GREEN	General	Company, customers, community
TLP:AMBER	Confidential – External	Company and clients
TLP:AMBER+STRICT	Confidential – Internal	Internal only
TLP:RED	Confidential – Eyes only	Specific individuals only

Creating sensitivity labels

Building the labels visually

"TLP-labeled documents MUST indicate the TLP label of the information, as well as any additional restrictions, in the header and footer of each page. The TLP label SHOULD be in **12-point type or greater** for users with low vision. It is recommended to right-justify TLP labels."

- There are limitations in labels names and visual appearance.
  - **\ \\ < > % & : ; ? / + |** are forbidden characters in a **Display name**
  - All of the above plus **,** ***** are forbidden in a **Label name**
- The is a limited selection of text colours in the visual markings
  - Black
  - Yellow (impossible to read on a white background)
  - Blue
  - Green
  - Red
- No real label formatting, only alignment (left, center, or right)
- We can't format the label like this **TLP:AMBER**

Demo time

Enhancements and features

- Privacy and external user access
- External sharing and conditional access
- Private teams discoverability and Shared channel settings

Practical scenarios and use cases

- Control Teams Sharing and External User access through label
- Control access to sensitive teams using Conditional Access Policy

Change management and adoption

Crawl, walk, run

The suggested method for implementing sensitivity labels.
(I have adapted it slightly to fit the SME needs)

1. Crawl
   Think about your needs. Make a plan. Communicate with the users
2. Walk
   Create the labels using visual markings only.
   Publish them.
3. Run
   Add external controls like Conditional Access och Data Loss Prevention where there is justification for it.

   Add the protections you want to the labels.
   - Rights Management
   - Teams settings
   - Encryption.

Add help for every label, and for the whole system

- When you publish labels, you are able to provide a support link.
- Create SharePoint pages to help users understand you labelling system.

Demo time

Summary and Q&A

- Go slow
- Go for a unified label approach
- A small set of universal labels that everyone understands
- Don’t turn on the protections from the start
  - Start with just document markings
  - Let people get used to the labels
  - Slowly introduce protection

Thank you