eSHARE Data Attributes

Bridging the gap between classification and enforceable policy

The Context Gap

Microsoft Purview Sensitivity Labels are a strong foundation, but a label alone doesn't tell users what markings to apply or give downstream systems the metadata for context-aware enforcement. That gap creates risk across three dimensions:

For People

Need the ability to add important context about the data with consistent visual markings

For Security

Downstream systems need contextual metadata to enforce accurately policy decisions

For AI Systems

Requires signals to determine whether content should be included, restricted or excluded from models

Awareness & Compliance

Within Word, PowerPoint, Excel, or Outlook, users select only the data attributes mapped to their Sensitivity Label. eSHARE dynamically composes markings from those selections, not static label-level text.

Context & Enforcement

Structured metadata is embedded into document custom properties, giving DLP, sharing platforms, and governance tools the context to enforce policy accurately. Enforcement becomes context-driven, not pattern-based.

AI Governance & Control

The metadata eSHARE embeds becomes the governance signal for AI. Copilots, RAG pipelines, and training workflows can automatically determine whether content is eligible for ingestion, surfacing, or exclusion.

The Solution: eSHARE Data Attributes

The eSHARE Data-Attributes Add-In extends Microsoft Purview Sensitivity Labels by introducing attribute-based classification, allowing organizations to define and enforce additional security context.

How It Works

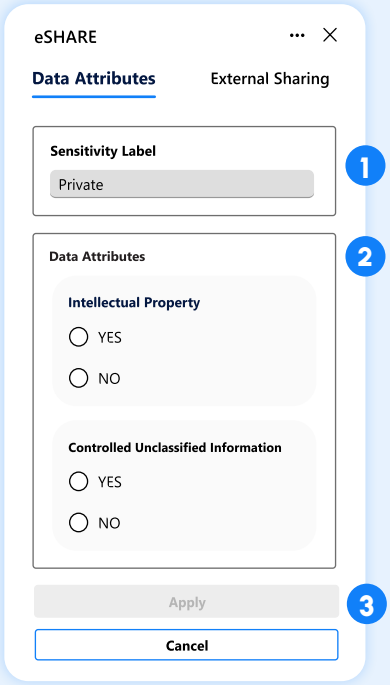
What the User Does

1. Begin with a Sensitivity Label

From within Word, PowerPoint, Excel, or Outlook, the eSHARE add-in reads the document's Sensitivity Label and surfaces only the relevant data attributes.

2. Select Required Data Attributes

Select values for each mapped data attribute (such as CUI category, IP designation, or AI training eligibility). Apply stays disabled until all required fields are complete.



What eSHARE Does

3. Apply Markings & Embed Metadata

eSHARE composes header and footer markings from selected data attributes and writes structured metadata into document custom properties. Existing markings can be appended, prepended, or replaced with guided prompts. The result: every document carries human-readable markings and machine-readable metadata for precise, context-aware enforcement.

In Practice

Defense & Aerospace: CUI with ITAR Controls

An engineer creates a technical spec in Word with a Confidential label. eSHARE surfaces the relevant data attributes; the engineer selects the CUI category and marks it ITAR-controlled. eSHARE applies CUI/ITAR markings and writes the metadata. When the file is shared through eSHARE, the policy engine automatically restricts access to U.S. persons.

Life Sciences: Pre-Clinical Data with HIPAA Constraints

A researcher labels a pre-clinical trial report Confidential. eSHARE presents the mapped data attributes; the researcher indicates it contains patient-adjacent data subject to HIPAA. eSHARE applies markings and embeds metadata. When shared through eSHARE, the appropriate permissions are applied automatically and AI security tools exclude it from training data. Without this metadata, the same document could be silently ingested into a training corpus with no policy check in place.

The Outcome

Every document carries **enforceable context**: consistently classified, clearly marked, and embedded with the metadata downstream systems need for accurate policy enforcement.

Turn Document Classification into Enforceable Policy

Discover how eSHARE extends Microsoft Sensitivity Labels with structured security attributes and metadata that make compliance-driven workflows enforceable from the start.