LM01_KDD024 - DLP framework at day 1

Status	DECIDED
Owner	Hachem Osmani
Stakeholders	CISO

Decision: Option 2 Re-adjusted DLP after Security Team Testing

Decision made by: CISO

Date: 26 Mar 2026

Online Meeting: M365 Workshop: DLP Framework day 1 [On-site & Online]

Issue

Decision on what Data Loss Prevention policies should be activated on day 1 after migration taking into consideration that at the same time, Syensqo is not yet sufficiently mature to deploy DLP with broad enforcement without risk of business disruption.

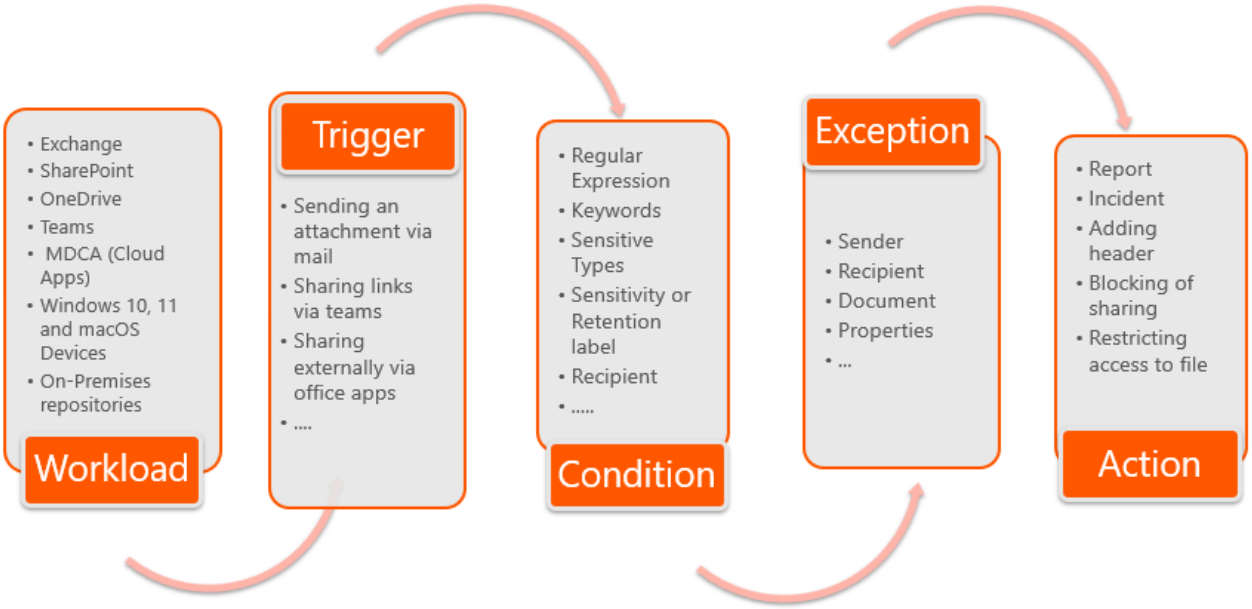
Recommendation

Option 2: Re-adjusted DLP after Security Team Testing

Background & Context

DLP policies define the rules and detection mechanisms used to identify, monitor, and restrict the unauthorized sharing or exfiltration of sensitive information across Microsoft 365 services. These policies apply content inspection, pattern matching, and classification logic to emails, documents, and chat messages, enforcing actions such as blocking, auditing, or notifying users when sensitive data is at risk. DLP policies act as a core governance layer, ensuring that data handling complies with Syensqo's security, regulatory, and compliance requirements across all supported workloads.

A policy can contain one or more rules, and each rule can consist of conditions and actions. For each rule, when the conditions are met, the actions are taken automatically. Rules are executed sequentially, starting with the highest-priority rule in each policy.



Assumptions

- **Information classification/labeling is not consistently applied**: not all files and emails are labeled, and auto-labeling/classification rules may not be fully defined or reliable. This creates gaps for DLP policies that depend on labels and increases the likelihood of false positives/negatives for content-based detection.
- **User behavior and data flows are not well understood**: there is no established baseline of how sensitive data is currently created, stored, and shared (including external collaboration and partner exchanges). Early enforcement could block legitimate business processes.
- **User readiness and guidance are limited**: without clear communication and training, DLP prompts/blocks can drive confusion, support burden, and potential workarounds

Constraints

- ## Copilot: permissions & oversharing

  Copilot responds based on what a user is allowed to access. If SharePoint/OneDrive/Teams permissions are messy (“Everyone” access, legacy broad groups), Copilot can surface information more widely than intended.

  - DLP can **reduce risky sharing**, but it does not automatically fix permissions sprawl.
  - Sensitivity labels + access controls (e.g., encryption / restricted access) help prevent oversharing.
  - **Labels and Copilot**
    - If sensitivity labels are used properly, they help enforce appropriate handling (e.g., encryption, restrictions), which limits where data can travel and who can open it.
    - Some controls are enforced by **Purview Information Protection / sensitivity labels**, while DLP focuses on **preventing risky actions** (sending/sharing).

- ## End User: Typical impacts users will notice

  Email

  - Warning banners / policy tips when sending sensitive content externally
  - Possible blocks (with or without override + business justification)
  - Attachments may be forced to **encrypted** formats or replaced with secure links

  OneDrive/SharePoint/Teams sharing

  - Restrictions on link types (e.g., “Anyone with the link” disabled)
  - External sharing might require **specific people** links, expiration dates, or approval
  - Users may be prevented from sharing labeled “Confidential/Highly Confidential” files externally

  Teams chats

  - Messages containing sensitive data may trigger warnings/blocks
  - Users may be nudged to share via approved channels rather than pasting content into chat

On the device (if Endpoint DLP is enabled)

- Copy to USB may be blocked for sensitive files
- Uploading to personal cloud (Dropbox, personal Google Drive) may be blocked
- Copy/paste or printing may be restricted for labeled content

Behavioral changes (and common friction points)

- Users must learn **when/how to apply labels** (or accept auto-labeling)
- “Quick sharing” habits (public links, forwarding threads, using personal tools) are reduced
- More interactions with justifications and “request access/exception” flows

What reduces disruption

- Start with **audit-only** + targeted warnings
- Clear “safe alternatives” for users (approved external sharing method, partner collaboration model)
- Tight tuning for top business scenarios (R&D collaboration, suppliers, customer exchanges)

Impacts

Business/operations impact

- Blocked legitimate work (false positives): users cannot email/share documents needed for customers, suppliers, or internal operations; project delays.
- Workarounds increase risk: users move to uncontrolled channels (personal email, personal cloud, screenshots, copy/paste into unmanaged tools) to get work done—often creating *more* exposure than before.
- High support load: spikes in IT helpdesk tickets and urgent “unblock” requests; loss of confidence in the program.

Security/compliance impact

- False sense of security: leadership assumes data is protected, while key sensitive content remains unprotected (false negatives, unlabeled documents, gaps in scope such as endpoints).
- Inconsistent enforcement: different teams experience different rules; exceptions are granted informally; auditability and defensibility are reduced.
- Alert fatigue: too many low-quality alerts; real incidents are missed or not investigated on time.

Options considered

Option 1: M365 Native Backup

Option 2: 3rd Party Backup (Veeam)

Evaluation

Option 1: Designed DLP

Option 2: Re-adjusted DLP after Security Team Testing

Name	Description	**Option 1:** Designed DLP	**Option 2:** Re-adjusted DLP after Security Team Testing
DLP-001-PCI-Exchange	Detects payment card information in Exchange emails sent internally. Notifies the sender with a policy tip to raise awareness of PCI handling requirements. Trusted Microsoft system emails are excluded to prevent false positives	ON	DISABLED
DLP-001-PCI-SharePoint&OneDrive	Detects payment card information stored or shared internally in SharePoint and OneDrive. Generates user notifications to promote compliant handling of PCI data without blocking access.	ON	DISABLED
DLP-001-PCI-Teams	Detects payment card information shared in Microsoft Teams chats and channels. Notifies users to discourage the use of Teams for transmitting PCI data while allowing collaboration to continue.	ON	DISABLED
DLP-002-PII-Exchange	Exchange-only PII detection policy.	ON	DISABLED
DLP-002-PII-Sharepoint&Ondrive	Protects files containing personal data in SharePoint Online and OneDrive. Enforces controls to prevent unauthorized sharing and data exposure.	ON	DISABLED
DLP-002-PII-Teams	Teams PII detection policy.	ON	DISABLED
DLP-003-FinancialInfo-Exchange	Detects global financial identifiers in Exchange emails for visibility and alerting.	ON	DISABLED

DLP-003-FinancialInfo-SharePoint&OneDrive	Enforces protection for SharePoint Online and OneDrive by blocking external sharing of files containing financial information. Overrides are allowed only with valid business justification and all actions are logged for compliance and investigation.	ON	DISABLED
DLP-003-FinancialInfo-Teams	Enforces protection in Microsoft Teams by restricting the sharing of messages containing financial information with external users. Prevents data exposure while allowing overrides with business justification and audit logging.	ON	DISABLED
DLP-004-SyensqoSensitiveKeywords-Exchange	Enforces protection for Syensqo-defined sensitive corporate keywords across Exchange Online. Content containing sensitive keywords is blocked by default. Users may override the restriction only with a valid business justification, and all overrides are logged and alerted.	ON	SIMULATION
DLP-004-SyensqoSensitiveKeywords-SharePoint&OneDrive	Enforces protection for Syensqo-defined sensitive corporate keywords across SharePoint & OneDrive. Content containing sensitive keywords is blocked by default. Users may override the restriction only with a valid business justification, and all overrides are logged and alerted.	ON	SIMULATION
DLP-004-SyensqoSensitiveKeywords-Teams	Enforces protection for Syensqo-defined sensitive corporate keywords across Microsoft Teams. Content containing sensitive keywords is blocked by default. Users may override the restriction only with a valid business justification, and all overrides are logged and alerted.	ON	SIMULATION
DLP-005-Labels-CorporateToPersonalEmail-Exchange	This policy enforces controls to prevent Corporate information from being sent to personal email services such as Gmail, Yahoo, Outlook.com, or iCloud. Personal mailboxes are not governed by corporate security, retention, or legal controls, and therefore represent a high-risk channel for data exfiltration. The policy ensures that Corporate information remains within managed and auditable communication channels.	OFF	OFF
DLP-006-Labels-SensitivityLabel-SharePoint&OneDrive	Control sending of Internal-labeled emails outside the organization	ON	SIMULATION
DLP-006-Labels-SensitivityLabel-Exchange	Control sending of Internal-labeled emails outside the organization	ON	SIMULATION

See also

The following section describes relevant documentation:

Description	Repository
Syensqo - M365 Build - LLD Configuration	
Syensqo - M365 Build - LLD	https://docs.google.com/document/d/1FKxTtu0M1xD5CU1DceoSXoH95TEq_8ZR/edit?rtpof=true&tab=t.0

Version	Published	Changed By	Comment
CURRENT (v. 2)	**Apr 21, 2026 11:55**	**CHUDZIAK-ext, Aleksander**	
v. 1	Apr 21, 2026 11:55	**CHUDZIAK-ext, Aleksander**	