IMPLEMENTATION PLAYBOOK · TIAGOSCARVALHO.COM

Choosing and Sequencing Microsoft Purview Controls

A print-and-follow manual for deciding whether a requirement needs sensitivity labels, DLP or retention, and then building them in an order that does not create rework.

> ⚠ **The expensive mistake here is not a misconfiguration. It is a correctly built control that answers the wrong question.**

Work through the phases in order. Phases 0 to 2 are decision work and take days; phases 3 to 5 are build and take weeks, mostly waiting. Each phase ends with a gate that has to be true before the next one starts. Keep the completed copy as your design record.

RECORD HEADER — COMPLETE BEFORE THIS COPY IS USED AS EVIDENCE			
Organisation / tenant		**Change or project reference**	
Document owner		**Date issued**	
Classification of this record		**Review due**	

Leave the record header blank if you are using this as a working document. Fill it in only when the completed copy becomes the design record for a specific tenant, because from that point it carries tenant configuration detail and should be classified accordingly.

Version 1.1, fillable edition · August 2026 · The checkboxes and form fields in this PDF are interactive: tick and type directly, then save. Blank text fields print as ruled lines and checkboxes as empty squares; completed field values also print. · Verified against Microsoft Learn on 10 August 2026 · Purview documentation changes frequently and several licensing pages contradict each other: verify licence entitlements against the tenant, not against a page, and record the date of the check.
Author: Tiago S. Carvalho · tiagoscarvalho.com · Companion to the article *Sensitivity Labels vs DLP vs Retention: Which Control Solves Which Problem?*

What is in this playbook

Why the first three phases are not optional

Most Purview projects fail on the decision, not the build. A control that is configured perfectly and answers a question nobody asked is worse than nothing, because it consumes the budget and the goodwill that the right control needed. Phases 0 to 2 cost a few days. Rebuilding after a quarter costs the project.

Read this before Phase 0. Since 2026, eligible new customers may receive automatically created default sensitivity labels, a publishing policy that sets a default label on unlabelled content, and auto-labelling configurations. The service-side policy starts in **simulation** and can then be turned on automatically if nobody edits it within a set number of days. If you are inheriting a tenant, assume something may already be running until Phase 0 proves otherwise.

Phase 0 · Inventory: what the tenant already does

An afternoon of looking, before anyone designs anything. The output is a written statement of the current position that everyone has seen.

0.1 Sensitivity labels

Microsoft Purview portal › Information Protection › Labels, and › Label policies

1. List every published label and every label policy. Note who each policy targets, and whether a **default label** is set for documents, email and meetings.
2. Check **Auto-labeling** for policies in simulation or on. A policy created by default starts in simulation and does not label anything yet, but if left unedited it can be turned on without a further decision: verbatim, "if you don't change the default setting, the policy will be automatically turned on for you if there aren't any changes to the policy within a set number of days".
3. Record whether sensitivity labels are **enabled for Office files in SharePoint and OneDrive**. This is a one-time manual step and it matters enormously in Phase 3.
4. Note any container labels applied to Teams, Groups or sites, and who can change them. Site owners can apply and change these settings, and there is no validation that the dependencies are in place.

0.2 DLP

Microsoft Purview portal › Data loss prevention › Policies

1. List every policy, its locations, its mode (simulation, tips only, enforce) and who it targets.
2. Include the **four default DLP policies Microsoft creates in every tenant**: Office 365, Teams, devices and the Microsoft 365 Copilot location. Confirm the mode and scope of each, and whether anybody has edited or enabled them.
3. For any policy whose rules use a **sensitivity label as a condition**, check the locations. If Teams is among them, that condition is disabled for the whole policy.
4. Note whether devices are onboarded for endpoint DLP, and whether they are already onboarded to Defender for Endpoint. The two share one onboarding object.

0.3 Retention

Microsoft Purview portal › Data lifecycle management, and › Records management

1. List retention policies and their scopes, distinguishing **adaptive** from **static**, and noting any that are org-wide.
2. List retention labels, their policies, and whether any use disposition review or are marked as records.
3. Check for **Preservation Lock** on any policy. A locked policy cannot be deleted or made less restrictive by anyone, including you. Note whether it is configured for delete-only, because that is the condition under which priority cleanup (preview) can override it in SharePoint and OneDrive. Check at the same time whether priority cleanup is enabled at all in the tenant: it is on by default, and it can be turned off. Record it as a constraint, not as a setting.
4. Check for eDiscovery holds. They sit above every retention principle.

GATE 0 · ALL MUST BE TRUE BEFORE PHASE 1

- ☐ Every published sensitivity label and label policy listed, including any default label.
- ☐ Auto-labelling policies identified, with their state, including any left unedited in simulation.
- ☐ Known whether sensitivity labels are enabled for SharePoint and OneDrive, and the answer written down.
- ☐ Every DLP policy listed with its locations and mode, including the four Microsoft creates by default.
- ☐ Any label-based DLP policy checked for the Teams location.
- ☐ Retention policies and labels listed, with adaptive versus static noted.
- ☐ Preservation Lock and eDiscovery holds identified and recorded as constraints.
- ☐ The current position written down in one page and shared with whoever asked for the project.

Phase 1 · Capture the requirement in business language

Before any control is named. The failure mode this phase prevents is a requirement arriving pre-solved: "we need sensitivity labels" is an answer wearing the costume of a question.

1.1 Write it as a sentence the business would recognise

One requirement per row of Appendix A. Each one must survive being read aloud to the person who asked. Useful shapes:

- "*Stop <who> from <action> with <what> to <where>.*"
- "*Keep <what> for <how long>, then <delete or review>.*"
- "*Make sure <what> is still <protected how> when it is <where>.*"
- "*Tell me where <what> is.*"

1.2 Attach the three things that decide the answer

1. **The trigger.** Is there a moment in time when something must happen? A send, a share, a paste, an upload. If yes, this is probably DLP. If the requirement is about a state rather than an event, it is not.
2. **The boundary.** Does the protection need to survive the file leaving Microsoft 365? Only a sensitivity label with encryption does that.
3. **The clock.** Is there a period, a deadline or a legal obligation? That is retention, and it needs its own track because it has the longest lead time.

1.3 Name the owner and the evidence

Who will answer for this control when it fires at an inconvenient moment, and what evidence will be produced to whom. Requirements without an owner do not survive their first false positive.

GATE 1 · ALL MUST BE TRUE BEFORE PHASE 2

- [ ] Every requirement written as a business sentence, with no Purview feature named in it.
- [ ] Trigger, boundary and clock recorded for each requirement.
- [ ] A named owner per requirement, not a team.
- [ ] The evidence each requirement must produce, and for whom, written down.
- [ ] Requirements that turned out to be "tell me where the data is" separated out: those are classification work, not enforcement.

Phase 2 · Choose the control, and record why not the others

Complete one row of Appendix A per requirement. The column that matters most is the last one: **why not the other two**. Writing it down is what stops the decision being reopened every month by someone who was not in the room.

2.1 The short test

IF THE REQUIREMENT SAYS	THE CONTROL IS
stop, and names an action	DLP
keep or **delete**, and names a period	Retention
outside, **even if it leaks**, **who can open it**	Sensitivity label, with encryption
where is	Classification and posture management, which enforces nothing. A DLP simulation scoped to SharePoint and OneDrive is a useful second source, because it scans at rest there, but it is not an inventory
prove that something was deleted	Retention label with disposition review, or marked as a record

2.2 The four boundaries that settle most arguments

1. **A label does not evaluate a recipient.** Classification and encryption are properties of the item, not decisions about a transaction. Only DLP has conditions like recipient domain, and only DLP can block a send.
2. **DLP is not an inventory, even where it scans at rest.** In SharePoint and OneDrive it does scan existing content, and a simulation scoped to only those locations reports *Completed* when "all data at rest has been scanned". But it reports only what your policy matches, displays only the first 100 matched items there, keeps results 30 days, and in Exchange, Teams and on devices it evaluates activity rather than storage.
3. **Sensitivity labels retain nothing.** There is no retention semantic in a sensitivity label, at all.
4. **Only the sensitivity label leaves with the file.** Retention labels explicitly do not persist outside Microsoft 365, and DLP is a boundary control by definition.

2.3 Two combinations that are correct, and one that is not

Correct: a sensitivity label used as a DLP condition. Microsoft routes you there itself: "Prevent or warn users about sharing files or emails with a specific sensitivity label → Use sensitivity labels as conditions in DLP policies."

Correct: a sensitivity label driving an auto-applied retention label, for content that must be both classified and kept.

Not correct: a container label expected to protect the files inside it. Items do not inherit container labels, so they receive no content marking and no encryption from them. Uploading a more sensitive document into a less sensitive site is not even blocked.

The join that silently fails. Sensitivity labels are supported as a DLP condition in some locations and not in others, and Microsoft's rule is that "a 'no' value for a content definition category takes precedence over 'yes' value". Teams chat and channel messages do not support the condition. Add Teams to a label-based policy and the condition stops working **for the entire policy**, not just for Teams. If you plan to combine these two controls, decide the locations at design time.

GATE 2 · ALL MUST BE TRUE BEFORE PHASE 3

- ☐ Appendix A completed: one row per requirement, with the chosen control and the rejected ones.
- ☐ Every rejection has a one-line reason a colleague could repeat.
- ☐ Any requirement needing two controls has the integration named explicitly (label as a DLP condition, or label driving auto-applied retention).
- ☐ No requirement relies on a container label protecting the items inside it.
- ☐ Any label-based DLP requirement has its locations decided, with the Teams question answered.
- ☐ The person who funded the project has seen the matrix and agreed with it.

Phase 3 · Clear the dependencies before building

One of the items in this phase is a one-way door. The others are ordinary prerequisites.

3.1 The one-way door: labels for SharePoint and OneDrive

Do this before any content is labelled and encrypted, not after. Verbatim: "SharePoint and OneDrive don't support sensitivity labels if you applied the labels before enabling these services for sensitivity labels. The labels aren't recognized and if the labels applied encryption, the contents aren't processed." Those files are invisible to search, DLP and eDiscovery until they are re-uploaded. And two encryption settings break processing permanently, even if the file is edited afterwards: an expiry on user access to content, and Double Key Encryption. Microsoft's words: "these documents aren't returned in search results, even if they're updated."

1. Confirm whether the tenant setting is already on. If it is not, and you intend to apply sensitivity labels to supported Office or PDF files in SharePoint or OneDrive, or to use service-side auto-labelling in those locations, turn it on now, and expect about 15 minutes for the tenant-level change to take effect. It is *not* required to use sensitivity labels on email only, or on containers only.
2. If content was already labelled and encrypted before the switch, list it. The remedy is re-uploading, and it needs a plan and an owner.
3. Decide the position on the two breaking encryption settings before anyone configures a label with them.

3.2 Classification before enforcement

1. Confirm which sensitive information types and trainable classifiers you will rely on, and test them against real content rather than trusting the name.
2. Use content explorer to see what is actually there. Allow up to two days for it to show newly labelled items, and up to seven after an on-demand classification scan.
3. Only now write DLP conditions or retention scopes. A rule written against unverified classification is a guess with a policy ID.

3.3 Labels before the controls that consume them

A sensitivity label can be a DLP condition and can drive an auto-applied retention label. Neither integration can be built before the label exists and has propagated. Sequence accordingly, and remember that labels take 24 hours to propagate, so "created" and "usable" are not the same afternoon.

3.4 Endpoint prerequisites, if endpoint DLP is in scope

1. Confirm device onboarding. Onboarding devices in the Purview portal also onboards them into Defender for Endpoint, so coordinate with whoever owns that.
2. Confirm the licence position for endpoint DLP specifically, rather than for DLP in general.

GATE 3 · ALL MUST BE TRUE BEFORE PHASE 4

- ☐ Sensitivity labels for SharePoint and OneDrive: state known, and enabled if labels are in scope.
- ☐ Any pre-existing labelled and encrypted content identified, with a re-upload plan and an owner.
- ☐ A decision recorded on user-access expiry and Double Key Encryption, with the consequences understood.
- ☐ Classifiers tested against real content, not accepted on the strength of their names.
- ☐ Content explorer consulted, with the two-day to seven-day delay accounted for.
- ☐ If endpoint DLP is in scope: onboarding confirmed and coordinated with the Defender owner.
- ☐ Licence entitlements verified **in the tenant**, with the date of the check recorded. Microsoft's own pages contradict each other on several rows.

Phase 4 · Build, in the order that avoids rework

There is no Microsoft page that sequences these three against each other. This order is a synthesis from the documented dependencies, and it is flagged as such: only step 1 is a hard requirement, the rest is argued rather than cited.

#	BUILD	WHY HERE
1	Enable labels for SharePoint and OneDrive, if you will label files there	**Hard dependency where it applies.** Needed for Office and PDF files in those locations and for service-side auto-labelling there; not for email-only or container-only labelling. A one-way door in time: everything encrypted before it is invisible afterwards.
2	Classification	You cannot write a defensible DLP condition or retention scope for data you have not located.
3	Sensitivity labels	Two other controls can consume them. Neither integration exists until the label does.
4	Retention, on its own track	Longest lead time, legal audience, least dependency on the other two. Starting it last is how it slips.
5	DLP, in simulation	Fastest to take effect, most visible to users when wrong, benefits most from the classification already done.

4.1 Roll each one out the same way

1. **Simulate or audit first.** Sensitivity auto-labelling and retention auto-labelling both have simulation; DLP has simulation and tips-only. Use them. Sensitivity simulation takes about 12 hours to complete; retention simulation typically one to two days.
2. **Pilot on a named group.** Small enough to phone, representative enough to be informative.
3. **Watch for a full business cycle** before widening. Month-end is where the surprises live.
4. **Widen in rings**, and re-check after each one rather than assuming the previous result transfers.

Two build-time traps worth a checklist line each. Visual markings are a client-side behaviour: "If the labels you select are configured to use visual markings (headers, footers, watermarks), these markings aren't applied to documents when you use auto-labeling." And auto-labelling changed materially in 2026: it can now remove labels and override manually applied lower-priority labels in SharePoint and OneDrive. Any guidance written before mid-2026 saying an auto-labelling policy "will never remove a label" is out of date.

GATE 4 · ALL MUST BE TRUE BEFORE PHASE 5

- ☐ Build order followed, or a written reason for departing from it.
- ☐ Every control ran in simulation or audit before enforcing.
- ☐ A named pilot group per control, and a full business cycle observed.
- ☐ If watermarking was promised: confirmed it is delivered client-side, not through auto-labelling.
- ☐ Auto-labelling behaviour confirmed against current documentation, including its ability to remove labels.
- ☐ Helpdesk briefed on what each control looks like to a user, and what to tell them.

Phase 5 · Operate: the calendar, the review, the way back

5.1 Plan around the slowest control in scope

The three run at three different speeds and it is an order of magnitude. Appendix B is the planning calendar; the headline is that **DLP lands in about an hour, labels in 24 hours, retention in up to seven days**. A pilot scheduled around DLP's speed will report failure for the other two before they have had a chance to work.

5.2 The precedence rules you will be asked about

Retention has four published principles, and the third is the one repeated incorrectly almost everywhere. Verbatim, in order: **1. Retention wins over deletion. 2. The longest retention period wins. 3. Explicit wins over implicit for deletions. 4. The shortest deletion period wins.** Above all four sits eDiscovery: a hold always takes precedence.

The 2026 exception to know before you promise immutability, and it is **still in preview and subject to change**: priority cleanup applies retention labels under the covers and "can override existing holds for retention and eDiscovery". It can also override **Preservation Lock**, but only in Exchange unconditionally; in SharePoint and OneDrive only when the locked policy is configured for delete-only. It cannot process records or regulatory records, and it cannot delete copies already added to an eDiscovery review set. Verify tenant availability and current behaviour before treating it as a compliance control: Microsoft notes that "highly regulated organizations that use Preservation Lock might want the additional safeguard of turning off priority cleanup at the tenant level".

Keep the questions separate, because the answers are not interchangeable. **Preservation Lock** protects the policy. A **record** blocks deletion, but an unlocked record can still have its contents edited and a locked one can have its label changed or removed by a container administrator. Only a **regulatory record** is irreversible: nobody, not even a global administrator, can remove the label. **Priority cleanup** is the documented exception to Preservation Lock, and it is blocked on every kind of record.

5.3 Standing review

1. **Monthly:** DLP matches by policy, and false positives raised by users. A sudden change usually means a new business process, not a new threat.
2. **Quarterly:** label usage against the taxonomy. Labels nobody applies are a taxonomy problem; labels everyone applies to everything are a training problem.
3. **Quarterly:** disposition review queue, if you use it, and any retention labels approaching their first disposition.
4. **On any Purview change announcement:** re-read the parts of this design that depend on documented behaviour. The 2026 changes to default labels and to auto-labelling both invalidated previously correct guidance.

GATE 5 · STEADY STATE REACHED

- [ ] Every control at its target state, or with a documented reason for not being there.
- [ ] Planning calendar (Appendix B) used for any future change, not just the initial build.
- [ ] Rollback position (Appendix C) written and understood per control.
- [ ] Monthly and quarterly reviews scheduled with a named owner.
- [ ] Appendix D signed.

Appendix A · Decision worksheet

One row per requirement. Duplicate this worksheet as needed. The last column is the one that stops the decision being reopened.

REQUIREMENT, IN BUSINESS LANGUAGE	TRIGGER?	LEAVES TENANT?	CLOCK?	CONTROL CHOSEN	WHY NOT THE OTHERS	OWNER

Trigger: is there a moment when something must happen (send, share, paste, upload)? Leaves tenant: must the protection survive the file leaving Microsoft 365? Clock: is there a period or a legal obligation? Control: Sensitivity label / DLP / Retention policy / Retention label / Classification only.

Appendix A · Decision worksheet, continued

Requirements 4 to 6. If you need more, print this page again: the field names repeat, so a second copy of the same page is a second set of rows, not a conflict.

REQUIREMENT, IN BUSINESS LANGUAGE	TRIGGER?	LEAVES TENANT?	CLOCK?	CONTROL CHOSEN	WHY NOT THE OTHERS	OWNER

Trigger: is there a moment when something must happen (send, share, paste, upload)? Leaves tenant: must the protection survive the file leaving Microsoft 365? Clock: is there a period or a legal obligation? Control: Sensitivity label / DLP / Retention policy / Retention label / Classification only.

Quick reference while you fill it in

WHAT THE BUSINESS ASKS FOR	THE CONTROL THAT ANSWERS IT	THE TEMPTING WRONG ANSWER
"Stop staff emailing customer data out"	DLP on Exchange, block with override	Labels with encryption: a label does not evaluate a recipient
"We need to know where our IP lives"	Classification, content explorer, posture management	DLP simulation: scans at rest in SPO/ OneDrive only, caps at 100 shown items, 30-day results
"Legal needs seven years"	Retention policy at container level	Sensitivity labels: no retention semantics at all
"Seven years on these documents, with sign-off"	Retention label with disposition review	Retention policy: disposition review is label-only
"Stop external sharing"	Depends on boundary: container label, tenant settings, or DLP	Picking one and assuming it covers the others
"Stop pasting client data into a public AI tool"	Endpoint DLP and inline web traffic DLP	Labels: paste-to-browser supports SITs, not labels
"Stop Copilot summarising the HR folder"	DLP for the Copilot location **(preview)**, label as condition	Container label: items do not inherit it
"Protect it even after it leaks"	Sensitivity label with encryption	DLP: it is a boundary control and stops at the boundary
"Delete Teams messages after a year"	Retention policy, Teams locations	Retention label: Teams messages do not support them
"Watermark confidential documents"	Label content marking, client-side	Auto-labelling: visual markings are not applied
"Prove we deleted it"	Retention label with disposition review, or record	Retention policy: no proof of disposition
"Nobody may weaken the policy"	Preservation Lock, PowerShell only, no adaptive scopes	Assuming a label does the same
"Nobody may delete the item"	A record. Deletion is blocked, locked or unlocked	Assuming it is fully immutable: an unlocked record can still be edited, and a locked one can have its label changed by a container admin
"Nobody, not even a global admin, may edit it or remove its protection"	A regulatory record	A standard record. Regulatory means irreversible: period can only be extended, no auto-labelling, PowerShell to enable
"We need a documented emergency exit"	Priority cleanup **(preview)**, with its approval process	Assuming there is none, or that it is stable. Preview and subject to change; can be turned off at tenant level

Appendix B · The three-speed planning calendar

Every figure below is Microsoft's own. Plan any change window around the slowest item in scope, and put these numbers in the plan rather than in your head.

WHAT YOU CHANGED	DOCUMENTED DELAY	NOTE
DLP — about an hour		
Policy turned on	**~1 hour**	"In general, policies take effect about an hour after being turned on."
Policy update reaching endpoints	~1 hour	Authorized Groups changes need 24 hours
Policy change reaching Copilot *(preview location)*	**up to 4 hours**	Catches people who test Copilot behaviour too early
Alert configuration change	up to 3 hours	Before new alerts are generated
Sensitivity labels — a day		
Label and label policy changes	**24 hours**	Some web edge cases within the hour; group-dependent settings 24 to 48 hours
New container label	at least 1 hour	At least 24 hours if Teams shared channel controls are configured
Existing container label changed	at least 24 hours	
Container label removed from a SharePoint site	48 to 72 hours	Quicker for Teams and Groups
SharePoint/OneDrive tenant setting	~15 minutes	
Auto-labelling simulation	12 hours	To complete
Co-authoring tenant setting	24 hours	Before using the feature
Retention — a week, sometimes much more		
Retention policy applied	**up to 7 days**	"It's best to plan for the maximum of seven days."
Auto-applied retention labels	up to 7 days	
Retention labels visible to users	~1 day, up to 7	Exchange needs at least 10 MB in the mailbox
Retention simulation	1 to 2 days	
Adaptive scope population	**up to 5 days**	Queries run daily; changes are not immediate
Teams "delete after 1 day", worst case	**16 days**	Before it stops being returned in eDiscovery
Preservation Hold library cleanup	up to 37 days	30 days minimum plus a job that runs every 7
SharePoint recycle bin	93 days	Across both stages
Retention policy released — **SharePoint and OneDrive only**	30 days	Retained content continues to be preserved for 30 days. **Not** when an individual site or OneDrive account is explicitly excluded from the policy: those files are cleaned up without the delay
Disposition approved to deleted	within 15 days	
Visibility		
Content explorer shows labelled items	up to 2 days	Up to 7 days after an on-demand classification scan

Appendix C · Rollback position per control

Decide these before you need them. The three controls are not equally reversible, and that asymmetry should influence the order you take risk in.

CONTROL	REVERSIBILITY	HOW TO BACK OUT	WHAT DOES NOT COME BACK
DLP	High	Switch the rule to simulation or tips-only, or disable the policy. Takes about an hour.	Nothing. This is the safest of the three to experiment with.
Sensitivity label (no encryption)	Medium	Unpublish the label, or remove it from the policy. Labels already applied stay on the content.	Applied labels persist on items until removed. Auto-labelling can now remove labels, which helps but is a change in itself.
Sensitivity label (with encryption)	**Low**	Removing encryption from a label does not decrypt content already protected. Plan a remediation pass.	Content encrypted before labels were enabled for SharePoint and OneDrive is not recognised at all. Two settings break processing permanently.
Retention policy	Medium	Delete the policy, turn the location off, or disable it. In SharePoint and OneDrive retained content is then preserved for a further 30 days, so re-enabling within that window loses nothing. Excluding a specific site or account instead skips the grace period entirely.	Content already deleted at the end of a period. And a policy under **Preservation Lock** cannot be deleted or made less restrictive by anyone.
Retention label	**Low**	Some settings are immutable once published. Removing a label from content may not be possible for users.	Deleted content. Records and regulatory records are deliberately one-way.

The asymmetry is the point. DLP is cheap to try and cheap to undo. Encryption and records are the opposite. Take your experimental risk in DLP, and take your time over anything that encrypts or deletes. If a stakeholder wants to "just turn something on and see", steer them to the control where that is a reasonable sentence.

Appendix D · Sign-off, changelog and sources

Licence position, verified in the tenant

Microsoft's own licensing pages contradict each other on several rows, including manual sensitivity labelling and container labels. Record what the tenant actually shows, and the date.

CAPABILITY	AVAILABLE?	VERIFIED HOW	DATE
Service-side auto-labelling			
Endpoint DLP			
Adaptive scopes			
Disposition review			

Sign-off

PHASE	COMPLETED BY	DATE	NOTES
Phase 0 · Inventory			
Phase 1 · Requirement			
Phase 2 · Decision			
Phase 3 · Dependencies			
Phase 4 · Build			

PHASE	COMPLETED BY	DATE	NOTES
Phase 5 · Operate			

Final approval

Sign this only when every gate in phases 0 to 5 is ticked, or when the exceptions are written into the notes column above. Two signatures, because the person who accepts the design record is often not the person accountable for the decision it records.

APPROVAL	NAME AND ROLE	SIGNATURE OR APPROVAL REFERENCE	DATE
Approved for implementation Accountable for the decision, and for the residual risk of the controls not chosen			
Accepted as the design record Owner of this document once it is filed			

A name typed into a PDF field is not a signature and will not survive a challenge. If this copy is completed on screen, put the reference from your change or approval system in that column and keep the signed authority there.

Changelog

VERSION	DATE	CHANGE
1.1	August 2026	Record and regulatory record separated: a record blocks deletion but an unlocked one can be edited and a locked one can have its label changed by a container admin; only a regulatory record is irreversible. Preservation Lock override by priority cleanup scoped: unconditional in Exchange, delete-only policies in SharePoint and OneDrive, never for records, and no effect on copies already in an eDiscovery review set. DLP corrected: it also scans content at rest in SharePoint and OneDrive. Default labels qualified to eligible new customers. Four default DLP policies added to the inventory. Sources expanded. Priority cleanup and the Microsoft 365 Copilot DLP location marked as preview; the 30-day grace on releasing a retention policy scoped to SharePoint and OneDrive, with the site-exclusion exception. Record header and final approval added so a completed copy can be filed as evidence; contents, site and article made clickable; PDF now tagged, with the full requirement text in each field tooltip.
1.0	August 2026	First release. Decision matrix, precedence rules, propagation figures and dependency chain verified against Microsoft Learn on 6 August 2026.

Sources

Every statement here comes from Microsoft's own documentation. The load-bearing pages, with direct links:

PAGE	URL
Learn about sensitivity labels The three defining properties	learn.microsoft.com/en-us/purview/sensitivity-labels

PAGE	URL
Get started with sensitivity labels The scenario table that routes to DLP and retention	learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels
Default labels and policies What new tenants get automatically	learn.microsoft.com/en-us/purview/default-sensitivity-labels-policies
Labels for Teams, Groups and sites No inheritance to items	learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites
Labels for Office files in SharePoint and OneDrive The one-way door	learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files
Create and publish sensitivity labels The 24-hour figure	learn.microsoft.com/en-us/purview/create-sensitivity-labels
Apply a sensitivity label automatically Client-side vs service-side, visual markings	learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically
Learn about DLP Deep content analysis, the 1-hour figure	learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
DLP policy reference Location support and the "no beats yes" rule	learn.microsoft.com/en-us/purview/dlp-policy-reference
DLP for the Copilot location The 4-hour figure	learn.microsoft.com/en-us/purview/dlp-microsoft365-copilot-location-learn-about
Learn about retention The four principles, verbatim	learn.microsoft.com/en-us/purview/retention
Retention for Teams The 16-day worst case	learn.microsoft.com/en-us/purview/retention-policies-teams
Retention for SharePoint Preservation Hold library timings	learn.microsoft.com/en-us/purview/retention-policies-sharepoint
Adaptive scopes The 5-day population window	learn.microsoft.com/en-us/purview/purview-adaptive-scopes
Disposition of content Review and proof of disposition	learn.microsoft.com/en-us/purview/disposition
Records management What a record and a regulatory record block	learn.microsoft.com/en-us/purview/records-management
Preservation Lock Restricting changes to retention policies	learn.microsoft.com/en-us/purview/retention-preservation-lock
Priority cleanup for Exchange The documented administrative exception	learn.microsoft.com/en-us/purview/priority-cleanup-exchange
Priority cleanup for SharePoint and OneDrive The delete-only condition on Preservation Lock	learn.microsoft.com/en-us/purview/priority-cleanup-onedrive-sharepoint
DLP simulation mode Scan status by location, and data at rest	learn.microsoft.com/en-us/purview/dlp-simulation-mode-get-started
What's new in Microsoft Purview The April 2026 auto-labelling change	learn.microsoft.com/en-us/purview/whats-new