DLP and sensitivity labels: does E3 cover what you need?

Tighten sharing links first, then use what Microsoft 365 E3 includes: four manually applied sensitivity labels and DLP policies for payment cards, IBANs and national ID numbers in email, SharePoint and OneDrive[1]. Buy E5 or an add-on only for a specific gap, such as automatic labeling, DLP for Teams chats or endpoints, or keeping Copilot away from labeled files[1].

Reviewed	Next review	Version	Written for	Latest version
2 Nov 2026	**2 Dec 2026**	**1.0**	**IT and security teams on Microsoft 365, including in the EU**	**sheets.einblick.dev/dlp-labeling/**

If you only do five things

1. **Tighten sharing first.**
   Set the default sharing link to Specific people or Only people in your organization, and make Anyone links expire and view-only[2]. Turn on guest access expiration and, if you share with a known set of partners, limit external sharing to their domains[2].
2. **Publish four labels with a default.**
   Public, Internal, Confidential and Highly Confidential are enough to start; Microsoft reports that labeling becomes noticeably less effective beyond five main labels[3]. Choose a default label without encryption and require a justification when someone lowers a label[3].
3. **Encrypt only your top label.**
   Encryption stays with the file, so partners can open it only with an account the label authorizes[4] and an app that supports the encryption[3]. Copilot returns content from an encrypted file only to users who have the copy (EXTRACT) usage right[3].
4. **Block card numbers and IBANs with DLP.**
   Microsoft's built-in sensitive information types cover credit card numbers, IBANs and German identity card (Personalausweis) and tax ID (Steuer-ID) numbers[5]. Run each DLP policy in simulation mode and show policy tips before you block external sharing[6].
5. **Fix oversharing before you roll out Copilot.**
   Copilot runs with each user's own permissions[7], so it can surface overshared files that user can open. Run the data access governance reports in SharePoint Advanced Management, which comes with Microsoft 365 Copilot, to find sites shared with Everyone except external users[8].

Roll out labels without breaking work

1. **Enable sensitivity labels for SharePoint and OneDrive.**
   Do this before any label applies encryption. Until then, search, eDiscovery, DLP and co-authoring don't work on encrypted files stored there[9]. Files encrypted before you enable it stay closed to search and DLP until someone edits or re-uploads them[9].
2. **Pilot the labels without encryption.**
   Publish them to one department with a default label and content markings, and review which labels people choose over a few weeks.
3. **Add encryption to the top label.**
   Assign permissions to groups rather than individual users, and configure super users so eDiscovery and data recovery can still read encrypted content[4].
4. **Publish to everyone and require labels.**
   Do this once the pilot shows people choose the right labels, and keep the default label: Microsoft warns that mandatory labeling without one can frustrate users with frequent prompts[3].
5. **Add auto-labeling last, in simulation.**
   Auto-labeling policies need E5 or an add-on and must run at least one simulation before they label anything[10]. Review the matches with the data owners before you turn a policy on.

What E3 and E5 give you

Feature names follow Microsoft's Purview service description of 29 October 2026[1]. "E5 or an add-on" means Microsoft 365 E5, Microsoft Purview Suite or Microsoft 365 E5 Information Protection and Governance unless noted.

Included in Microsoft 365 E3

- **Manual Sensitivity Labeling** in Office apps and **Message Encryption** for email to any address[1].
- **DLP for Exchange Online, SharePoint Online and OneDrive for Business**, which also covers files stored in Teams[1].
- **DLP to safeguard prompts** for all users of Microsoft Copilot and Copilot Chat[1].
- **Inheriting labels from input to output** in Copilot, with a Microsoft 365 Copilot license[1].
- **Audit (Standard)** and **eDiscovery (standard)**[1].

Needs E5 or an add-on

- **Client and service-side automatic sensitivity labeling** and default labels for SharePoint document libraries[1].
- **DLP for Teams** chat and channel messages and **Endpoint DLP** on Windows and macOS[1].
- **DLP to restrict Copilot from processing files and emails** that carry a chosen label[1].
- **Insider Risk Management**, which needs E5, Microsoft Purview Suite or the Microsoft 365 E5 Insider Risk Management add-on[1].
- **Data classification analytics** (content and activity explorer), **Advanced Message Encryption** and **Double Key Encryption**[1].

Check before you buy

- **Default labels on E3.** The service description lists Manual Sensitivity Labeling for E3 but also says labeling, including policy-based labeling, needs E5 or Information Protection and Governance[1]. Check your agreement.
- **Who needs a license.** Some tenant-level services can't be limited to licensed users[17]. Owners and members of sites that a Purview policy covers, and shared mailboxes that use E5 features, need licenses too[1].
- **Pay-as-you-go extras.** DLP for unmanaged cloud apps in Edge for Business and network DLP are billed pay-as-you-go[1].
- **SharePoint Advanced Management.** Its sensitivity label report needs E5, even with a Microsoft 365 Copilot license[8].

- **Agents.** Microsoft says Purview protection for agents on Microsoft Foundry will come with Microsoft 365 E7 and Agent 365[1].

What you can skip

- **Custom sensitive information types first.** Write your own only for data the built-in types miss, such as customer numbers.
- **Sublabels for every department.** Add one only when a group needs different encryption permissions, and keep each label to five sublabels or fewer[3].
- **Double Key Encryption and Customer Key.** Both need E5 or an add-on[1], and SharePoint search, co-authoring and DLP don't work on files protected with Double Key Encryption[9]. Wait until a contract or regulator requires them.
- **Endpoint DLP before the cloud policies work.** It extends DLP to USB copies, printing and browser uploads on Windows and macOS[11]. Tune the email, SharePoint and OneDrive policies first.
- **Insider Risk Management before the basics.** It needs E5, Microsoft Purview Suite or an Insider Risk Management add-on[1], and in Germany the works council co-determines tools designed to monitor employees' behavior or performance[12].

Mistakes that cost the most

- **Setting access to expire in a label.** SharePoint can't process files whose label sets an access expiry, so search doesn't return them[9].
- **Trusting a DLP template's name.** Microsoft's Germany Financial Data template looks for credit card numbers but not IBANs, and its Germany PII Data template leaves out the identity card and tax ID, which the Enhanced GDPR template includes[13].
- **Treating Restricted Content Discovery as an oversharing fix.** It limits how sites surface in Copilot and organization-wide search but doesn't change who can open them[14].

What changed in 2026

- **E3 and E5 prices rose without new Purview features.** From 1 July 2026 the US list price of Microsoft 365 E3 went from $36 to $39 per user per month and E5 from $57 to $60. Microsoft added Defender, Intune, Cloud PKI and Copilot features to the suites and lists the Microsoft Purview Suite add-on at $12[15].
- **Copilot can ignore external email.** Since June 2026 a preview DLP policy can keep Copilot from grounding answers in mail from outside your domains, which Microsoft offers as a way to reduce prompt-injection risk[16,7].
- **Auto-labeling can override manual labels.** Since April 2026 auto-labeling policies can replace a lower-priority label that a user applied to a SharePoint or OneDrive file[16].
- **Labels and DLP extend to Box and Google Workspace.** In preview since August 2026, auto-labeling and DLP policies can protect files at rest there through Defender for Cloud Apps connectors[16].

Version history

2 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check of every licensing statement against the Microsoft Purview service description of 29 October 2026.

Sources

1. Microsoft Purview service description. Microsoft Learn, 29 Oct 2026. learn.microsoft.com
2. Manage sharing settings for SharePoint and OneDrive in Microsoft 365. Microsoft Learn, 1 Jul 2026. learn.microsoft.com
3. Learn about sensitivity labels. Microsoft Learn, 25 Jun 2026. learn.microsoft.com
4. Apply encryption using sensitivity labels. Microsoft Learn, 29 Oct 2026. learn.microsoft.com
5. Sensitive information type entity definitions. Microsoft Learn, 15 Jun 2026. learn.microsoft.com
6. Learn about data loss prevention. Microsoft Learn, 16 Sep 2026. learn.microsoft.com
7. Microsoft Purview DLP for Microsoft 365 Copilot and Cowork. Microsoft Learn, 27 Oct 2026. learn.microsoft.com
8. SharePoint Advanced Management features in Microsoft Copilot licenses. Microsoft Learn, 18 Aug 2026. learn.microsoft.com
9. Enable sensitivity labels for files in SharePoint and OneDrive. Microsoft Learn, 19 Oct 2026. learn.microsoft.com
10. Automatically apply a sensitivity label to Microsoft 365 data. Microsoft Learn, 30 Oct 2026. learn.microsoft.com
11. Learn about Endpoint data loss prevention. Microsoft Learn, 15 Oct 2026. learn.microsoft.com
12. Works Constitution Act (Betriebsverfassungsgesetz), Section 87. Federal Ministry of Justice and Consumer Protection (Germany), as amended 19 Jul 2024. gesetze-im-internet.de
13. What DLP policy templates include. Microsoft Learn, 15 Jun 2026. learn.microsoft.com
14. Restrict discovery of SharePoint sites and content. Microsoft Learn, 31 Oct 2026. learn.microsoft.com
15. Microsoft 365 Pricing and Packaging Updates. Microsoft Licensing Resources, 16 Feb 2026. microsoft.com
16. What's new in Microsoft Purview. Microsoft Learn, 20 Oct 2026. learn.microsoft.com
17. Microsoft 365 guidance for security & compliance. Microsoft Learn, 21 Aug 2026. learn.microsoft.com