# Basic Data Loss Prevention (DLP) Advisory

## Introduction & Purpose

The purpose of this engagement is to help organisations establish a foundation for protecting sensitive information across Microsoft 365 using Data Loss Prevention (DLP).

DLP is often misunderstood as a purely technical control. In reality, it is both a **business enabler** (protecting customer data, IP, and compliance posture) and a **risk control**.

This advisory is not intended to produce a fully customised set of DLP rules or deep policy engineering. Instead, it provides the customer with:  
- An understanding of **what DLP can and cannot do**  
- A **baseline set of policies** aligned to business risks (PII, financial info, government IDs, etc.)  
- Guidance on how to monitor, tune, and expand DLP over time

## Rules of Engagement

Keep in mind the E2 charter: customers should feel **knowledgeable, confident, and supported** in securing their business in Microsoft 365.

* **Stay high level**: focus on policies, information types, and outcomes — not regex strings or advanced config.
* **Solution centric**: tie DLP back to **business goals** — preventing accidental sharing, compliance reporting, protecting regulated data.
* **Avoid tactical debates**: if customers want to dive into policy tuning (e.g., specific rules for a business unit), park that for a follow-up engagement.
* **Red flags**: if a customer asks about custom regex, EDM schema design, or large-scale insider risk — steer them toward advanced Purview or IRM engagements.
* **Strategic lens**: reinforce that DLP is not “set and forget” — policies must evolve as the business changes.

## Step-by-Step Delivery

### Step 1 – Define Goals & Objectives

* Ask: *What are the business drivers for DLP?* (compliance, IP protection, customer trust).
* Align to existing policies: privacy statements, contracts, regulatory obligations (PSPF, GDPR, HIPAA).
* Establish scope: which workloads matter most (Exchange, SharePoint, OneDrive, Teams).
* Clarify whether they see DLP as compliance-driven (regulators, audits), risk-driven (IP leakage), or productivity-driven (support Copilot adoption). This shapes what they value most in the policies.

### Step 2 – Identify Sensitive Information Types

* Review Microsoft’s built-in sensitive info types (credit card, bank account, TFN, passport).
* Discuss industry-specific requirements.
* Capture “must-protect” categories vs “nice-to-have”.

### Step 3 – Build Baseline Policies

* Create 2–3 starter policies in **audit mode** (no blocking yet).
* Focus on **visibility first**: where is sensitive data flowing?
* Examples: outbound email with PII, Teams chat with financial data, OneDrive sharing of IDs.
* Position these as ‘starter guardrails’, not permanent solutions, the point is to learn before enforcing.

**Facilitator notes** - Use the blueprint to frame a two-step path: observe (audit-mode DLP) → enforce (graduated controls).  
- Tie DLP policy scope and admin roles back to the blueprint’s “secure defaults” to avoid one-off exceptions.

### Step 4 – Review & Tune

* After ~2 weeks, review policy match reports.
* Discuss false positives and adjust rules.
* Escalate findings: *“Did you know HR data is being shared via Teams without encryption?”*

### Step 5 – Move to Enforcement

* Transition selected policies from audit to enforcement.
* Start light: block external sharing of PII, require justification for internal sharing of TFNs.
* Build governance process: who approves exceptions, who reviews reports.

## Engagement Outputs

By the end of this advisory, the customer should have:  
- A documented **DLP baseline policy set** (at least 2–3 active policies).  
- A **sensitive information register** (top 5 data types to protect).  
- A **policy monitoring plan** (who reviews, how often).  
- A list of **quick wins** and a roadmap for advanced DLP (endpoint DLP, EDM, IRM). - Defined reporting cadence (e.g., monthly DLP report to IT Security + quarterly update to executives).

## References & Learning Resources

* [Microsoft Learn – Implement and Manage DLP](https://learn.microsoft.com/en-us/training/paths/purview-implement-manage-dlp/)
* [Beginner’s Guide to M365 DLP (HubSite365)](https://www.hubsite365.com/en-ww/crm-pages/data-loss-prevention-in-microsoft-365-easy-guide-for-beginners-01a76489-6ca2-405e-b57a-afc94ad6f880.htm)
* [Microsoft Purview DLP Best Practices (Nikki Chappell)](https://nikkichapple.com/microsoft-purview-dlp-best-practices/)
* [Data Loss Prevention Guide for M365 (ArchTIS)](https://www.archtis.com/data-loss-prevention-guide-for-microsoft-365-and-sharepoint/)
* [Microsoft Blog – Securing Data with Purview](https://www.microsoft.com/en-us/security/blog/2025/04/25/explore-practical-best-practices-to-secure-your-data-with-microsoft-purview/)