Forcepoint

Data Loss Prevention Policy Checklist

Check every item before you approve the policy and switch on a rule

This checklist walks through the sections of the data loss prevention (DLP) policy template in the order that matters. Print it, work down the list and sign off at the end.

1. Scope and ownership

- ☐ Name the policy owner and the DLP lead
- ☐ Assign an owner to every data set
- ☐ List the systems, people, vendors and AI tools in scope
- ☐ Name the privacy lead who decides whether an incident is a personal data breach

2. Data classes

- ☐ Define four classes: Restricted, Confidential, Internal and Public
- ☐ Scan your repositories before owners assign classes
- ☐ Give every data set one owner and one class
- ☐ Set the rule that a file mixing classes takes the highest class
- ☐ Build a handling matrix for external email, link sharing and AI tools

3. Channels and AI use

- ☐ List the approved file, email and transfer tools
- ☐ Mark personal email, personal cloud storage and removable media as unapproved for Confidential and Restricted data
- ☐ Decide which USB drives, if any, are allowed and who may use them
- ☐ State what may enter AI prompts for each data class
- ☐ Set what copilots may retrieve and when sharing permissions get reviewed
- ☐ Give every AI agent a named owner, a documented purpose and minimum access

4. Rules and modes

- ☐ Pair each policy clause with a detector, a channel, an action and a mode
- ☐ Start every new rule in Monitor mode
- ☐ Set a Monitor period, a false-positive threshold and a review count. The template defaults are four weeks, 5% and two consecutive reviews
- ☐ Review new matches each week and record false positives for each rule
- ☐ Limit who can read alert content
- ☐ Have Legal review monitoring practices against local law before launch

© 2026 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks are the property of their respective owners.

Guidance only, not legal advice. Defaults in the template are starting points, not requirements of any framework.

5. Incidents and exceptions

- [ ] Set how fast people must report a suspected leak
- [ ] Define severity levels and an owner for each
- [ ] Record the data class, the people affected and the encryption status for every incident
- [ ] Decide who notifies regulators. Under the General Data Protection Regulation (GDPR), notice is due within 72 hours of awareness where feasible
- [ ] Require written approval, a compensating control and an end date for every exception
- [ ] Keep an exception register and review it on a set schedule

6. Review and proof

- [ ] Set a review cycle of at least once a year and name the triggers for an early review: a new regulation, a new cloud or AI service, a merger or a serious incident
- [ ] Review the rules more often than the document
- [ ] Track the false-positive rate for each rule, exceptions open past their end date and sensitive data sets with no rule
- [ ] Map the policy to the frameworks you follow, such as ISO/IEC 27001:2022 Annex A control 8.12, GDPR Article 33 and the National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5
- [ ] Confirm the current text of each framework with your auditor
- [ ] Approve the policy, publish it and record the version and date

Sign-off

Policy owner	Approved on	Next review

See these rules run in one console

Forcepoint DLP applies one policy across AI, cloud, web, email and endpoint. Learn more at forcepoint.com/product/dlp-data-loss-prevention.

© 2026 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks are the property of their respective owners.
Guidance only, not legal advice. Defaults in the template are starting points, not requirements of any framework.