sosafe

DLP implementation checklist for IT decision-makers

Comprehensive guide to implementing data leak prevention

Executive Summary

This checklist guides you step by step through the implementation of an effective data leak prevention strategy. It contains:

- Detailed implementation steps with responsibilities
- Templates for DLP policies and incident response plans
- Measurable KPIs for monitoring success
- Compliance mapping for GDPR, NIS2 and ISO 27001
- Tool evaluation criteria
- Review and audit processes

Timeframe: 3-6 months for full implementation (depending on organisation size)

1 Phase 1: Preparation & inventory (weeks 1-4)

1.1 Stakeholder management

- [ ] Set up project team
  - Responsible: CISO / IT management
  - Required: IT security, legal/compliance, HR, employee representative body, data protection officer
  - Deliverable: Project charter with budget, schedule, responsibilities
- [ ] Secure executive buy-in
  - Present risk assessment (potential damage in the event of a data breach)
  - Business case: ROI through avoidance of fines, reputational damage
  - Resources required: Budget, FTEs, external consulting
- [ ] Involve employee representative body/HR
  - Prepare employee representation agreement for monitoring (where applicable in your jurisdiction)
  - Define transparency requirements
  - Plan employee information

1.2 Data inventory

- [ ] Perform data discovery
  - Where is sensitive data located? (File servers, SharePoint, cloud storage, endpoints)
  - What types of data? (PII, financial data, IP, health data)
  - Who has access? (create authorisation matrix)
  - Recommended tools: Automated discovery tools (e.g. Microsoft Purview, Varonis, BigID)
- [ ] Data flow mapping
  - Data source → Processing → Storage → Transfer → Archiving/deletion
  - Identify critical paths (email, cloud uploads, USB, printers)
  - Visualisation: Create data flow diagram
- [ ] Risk assessment per data category

Data category	Sensitivity (1-5)	Volume	Accesses/day	Shared externally?	Risk score
Customer data (PII)	5	High	500	Yes	Critical

Data category	Sensitivity (1-5)	Volume	Accesses/day	Shared externally?	Risk score
Financial data	5	Medium	50	Rare	High
Source code	4	High	200	No	High
Internal documents	2	Very high	2000	Yes	Medium

2 Phase 2: Policy & Classification (Weeks 5-8)

2.1 Define data classification scheme

☐ Define classification levels

Level	Definition	Examples	Access rule	Handling
Public	Intended for the public	Press releases, marketing material	No restrictions	No encryption required
Internal	For internal use	Project plans, meeting notes	Employees only	Basic access control
Confidential	Business-critical	Contracts, financial forecasts, M&A documents	Need-to-know	Encryption + MFA
Restricted	Highly sensitive	Personnel data, payment information, patient records, trade secrets	Explicit authorisation	Encryption + MFA + Audit Trail + DLP Block

☐ Establish labelling process

- Automatic classification: pattern matching (credit card numbers, IBAN, etc.)
- Manual classification: User training + reminders in Office apps
- Default classification: New files classified as "Internal" by default until review

☐ Document classification policy

Template: Data classification guideline

1. Purpose

This policy defines how data is classified, labelled and protected.

2. Scope

All employees, contractors and partners with access to company data.

3. Roles

- Data owner: department, defines classification
- Data custodian: IT, implements technical controls
- Data user: any employee accessing the data, complies with handling requirements

4. Classification decision tree

Does the data contain personal information? → YES → Restricted
Would disclosure harm the company? → YES → Confidential

Is it for internal purposes? → YES → Internal
Otherwise → Public

5. Reclassification
Annual review by data owner. If changed: update label.

2.2 Create DLP policy

- [ ] Write policy document

Template: Data leak prevention policy

1. Purpose
Prevention of unauthorised disclosure of sensitive company data.

2. Scope
All systems, networks, end devices, cloud services.

3. Prohibited actions
- Transfer of "restricted" or "confidential" data to private email addresses
- Uploading sensitive data to unauthorised cloud services
- Copying sensitive data to USB sticks without encryption
- Taking screenshots of "restricted" documents without authorisation

4. DLP control points
- Email gateway (inbound/outbound)
- Web proxy (cloud uploads)
- Endpoint agents (USB, clipboard, screenshot)
- Cloud API integration (Microsoft 365, Google Workspace, Slack)

5. Enforcement modes
- Monitor: Logging only, no blocking (pilot phase)
- Alert: Warning to user + security team
- Block: Automatic block + incident ticket

6. Exceptions
Exceptions only approved by CISO, time-limited, documented.

7. Incident response
In case of violation: Automatic ticket → Assessment within 4 hours → Escalation if restricted data is affected

8. Review
Quarterly policy review, after each incident.

☐ Create least privilege matrix

Role	Customer data	Financial data	HR data	Source code	Marketing documents
Sales	Read + Edit	-	-	-	Read
Finance	-	Read + Edit	-	-	-
HR	Read (names/ contact)	-	Read + Edit	-	-
Engineering	-	-	-	Read + Edit	-
Marketing	Read (anonymised)	-	-	-	Read + Edit
Executives	Read (all)	Read (all)	Read (all)	Read (all)	Read (all)

☐ Define access review process

- Quarterly: Each manager reviews their team's access rights
- When roles change: Automatic revocation of old rights + request for new rights
- Upon departure: Immediate withdrawal of all access rights

3 Phase 3: Tool evaluation and selection (weeks 9-12)

3.1 Requirements catalogue

- [ ] Must-have features
  - [ ] Support for all data channels (email, web, endpoint, cloud)
  - [ ] Content inspection (pattern matching, ML-based, OCR)
  - [ ] Integration with existing systems (SIEM, SOAR, ticketing)
  - [ ] Encryption integration
  - [ ] Granular policy control (per data category, user group, action)
  - [ ] Compliance reporting (GDPR, NIS2, ISO 27001)
  - [ ] False positive management (user feedback loop, ML tuning)
- [ ] Nice-to-have features
  - [ ] Behavioural analytics (UEBA)
  - [ ] Data-at-rest scanning (discovery)
  - [ ] Automatic classification
  - [ ] Remediation workflows (e.g. automatic encryption instead of blocking)
  - [ ] User self-service (release requests)

3.2 Vendor evaluation matrix

- [ ] Create & evaluate shortlist

Criterion	Weight	Vendor A	Vendor B	Vendor C
Functionality				
Email DLP	15%	9/10	8/10	7/10
Cloud DLP (API)	20%	8/10	9/10	6/10
Endpoint DLP	15%	7/10	9/10	8/10
ML/Behavioural	10%	9/10	7/10	5/10
Integration				
SIEM/SOAR	10%	8/10	8/10	9/10
Existing stack	5%	7/10	9/10	6/10
Usability				

Criterion	Weight	Vendor A	Vendor B	Vendor C
Admin UI	5%	8/10	7/10	9/10
False positive management	10%	9/10	8/10	7/10
Cost				
Licence costs	5%	7/10	8/10	9/10
Impl. effort	5%	8/10	7/10	8/10
Overall score	100%	8.2	8.1	7.3

☐ Perform POC

- Test duration: 4 weeks
- Test scope: Email + cloud + 50 test endpoints
- Success criteria: <5% false positives, <100 ms latency, 95%+ detection rate

4 Phase 4: Implementation (weeks 13-20)

4.1 Technical implementation

- [ ] Email DLP
  - MX record adjustment or SMTP relay configuration
  - Policy rules: Outbound scan for restricted/confidential data
  - Set up quarantine mailbox
  - Escalation workflow: security team + manager in case of block
- [ ] Web/cloud DLP
  - Proxy integration or cloud CASB
  - Enable SSL inspection (caution: data protection implications)
  - API connectors: Microsoft 365, Google Workspace, Slack, Salesforce
  - Policy: Block upload of restricted data to unapproved cloud services
- [ ] Endpoint DLP
  - Agent rollout (step by step: IT → pilot group → full rollout)
  - USB blocking for restricted data (allow list for encrypted USBs)
  - Clipboard control, screenshot prevention
  - Offline mode: policy enforcement even without a network connection
- [ ] Incident management integration
  - SIEM integration: DLP alerts → correlation with other security events
  - Ticketing: Automatic tickets for high-severity violations
  - SOAR playbooks: Automatic account suspension for critical violations

4.2 Rollout plan

- [ ] Pilot phase (weeks 13-16)
  - Target group: IT department (20-50 users)
  - Mode: Monitor-only
  - Objective: Establish baseline, determine false positive rate, tune policies
- [ ] Phased rollout (weeks 17-20)
  - Week 17: Finance (alert mode)
  - Week 18: HR + Legal (alert mode)
  - Week 19: Engineering + Sales (alert mode)
  - Week 20: Rest of organisation (alert mode)

- [ ] Enforcement phase (from week 21)
  - Gradual transition to block mode
  - Start with restricted data
  - After 2 weeks: Confidential data as well

5 Phase 5: Human risk management (parallel to phase 4)

5.1 Awareness campaign

- [ ] Communication plan
  - Week 12: Announcement by CEO/CISO (all-hands meeting)
  - Weeks 13-16: Pilot group: Intensive training + Q&A sessions
  - Week 17-20: Rollout communication: intranet article, email, manager briefings
  - From week 21: Continuous reminders (monthly newsletter)
- [ ] Develop training modules
  1. Module 1: Why DLP? (5 min)
     - Risks of data breaches (example cases)
     - Legal obligations (GDPR, NIS2)
     - Personal responsibility
  2. Module 2: Data classification (10 min)
     - Levels & examples
     - How do I classify correctly?
     - Practical exercise: Classify 5 sample documents
  3. Module 3: What am I allowed to do (and not do)? (10 min)
     - Dos & don'ts
     - What happens in the event of a violation?
     - How do I apply for exceptions?
  4. Module 4: Phishing & social engineering (15 min)
     - Recognising phishing emails
     - CEO fraud scenarios
     - Reporting process
- [ ] Phishing simulations
  - Frequency: Monthly, randomised
  - Template rotation: CEO fraud, fake invoice, credential phishing, malware attachment
  - Follow-up: Upon click → Immediate microlearning (3 min)
  - Gamification: Leaderboard (anonymised), badges for reporters

5.2 Human risk dashboard

- [ ] Define & track KPIs

KPI	Target value	Measurement method
Phishing click rate	<5%	Phishing simulation tool
Reporting rate (suspicious emails)	>30%	Phishing report button analytics
Training completion rate	>95%	LMS reporting
DLP violations per 1,000 users	<10/month	DLP system logs
Repeat violations (same user)	<2%	DLP system analytics
Human security index	>75/100	Human risk management dashboard

6 Phase 6: Compliance & Documentation (Weeks 21-24)

[LOCAL PART]

6.1 Compliance mapping

The following mapping uses the EU regulatory framework (GDPR, NIS2, ISO 27001) as a worked example. Adapt the specific articles, deadlines and authorities to whichever regulatory framework applies in your jurisdiction.

☐ Cover GDPR requirements

GDPR articles	Requirement	DLP measure	Status
Art. 5 (1f)	Integrity & Confidentiality	DLP policies + encryption	☐
Art. 25	Privacy by Design	Default classification "Internal"	☐
Art. 32	Technical measures	DLP + Access Control + Monitoring	☐
Art. 33	Reporting obligation (72 hours)	Incident response integration	☐
Art. 35	DPIA	DPIA performed for DLP monitoring	☐

☐ Cover NIS2 requirements

NIS2 articles	Requirement	DLP measure	Status
Art. 21	Cybersecurity risk management	DLP as part of the risk management strategy	☐
Art. 23	Reporting obligation (24-hour initial report)	Automatic alerts + escalation	☐
Art. 32	Audit & documentation	DLP logs, policy documents, audit trails	☐

☐ Cover ISO 27001:2022 Annex A 8.12

- Data leakage prevention documented as a control measure
- Process description: How does the organisation prevent exfiltration?
- Supporting documents: DLP policy, tool configuration, logs, incident reports

6.2 Documentation

- [ ] Create mandatory documents
  - [ ] DLP policy (see template above)
  - [ ] Data classification policy
  - [ ] Incident response plan (see below)
  - [ ] Operating agreement (monitoring)
  - [ ] Data protection impact assessment (DPIA)
  - [ ] Admin manual (DLP system)
  - [ ] User guide (data classification, exception process)

7 Phase 7: Incident response (continuous)

7.1 Incident response plan

Template: DLP Incident Response Playbook

Phase 1: Detection (0-15 min)

- [ ] Receive DLP alert (email, SIEM, ticket)
- [ ] Severity classification:
  - Critical: Restricted data + external + large volume
  - High: Confidential data + external
  - Medium: Confidential data + internal
  - Low: Internal data + unusual behaviour
- [ ] On-call engineer assigned

Phase 2: Containment (15-60 min)

- [ ] For Critical/High: Immediate measures
  - Lock affected account
  - Recall email from recipient's mailbox (if still possible)
  - Disconnect the endpoint's network connection (if active exfiltration)
- [ ] Create forensic snapshot (logs, memory dump, disk image)
- [ ] Inform incident commander (CISO or deputy)

Phase 3: Assessment (1-4 hours)

- [ ] Data assessment:
  - What data? (classification, volume, number of people affected)
  - Where? (internal/external recipient, domain, cloud service)
  - How? (e-mail, USB, cloud upload, screenshot)
  - Why? (Mistake, social engineering, malicious)
- [ ] User interview (if available, not in cases of suspected malicious intent)
- [ ] Legal assessment: Reporting obligation under applicable data protection and cybersecurity law? [LOCAL PART - EU example below]
  - GDPR Art. 33: Notification to supervisory authority within 72 hours?
  - NIS2 Art. 23: Initial report to CSIRT/authority within 24 hours?
  - Inform affected persons? (Art. 34 GDPR)

- [ ] Decision: Escalation to management/legal?

Phase 4: Notification (within legal deadlines)

- [ ] Internal reporting: Incident report to CISO, legal department, data protection officer
- [ ] External reporting (if necessary): [LOCAL PART - EU example below]
  - GDPR: Notification to the competent supervisory authority (form)
  - NIS2: Initial report to CSIRT/competent authority
  - Affected persons: Email/letter with details + recommendations for action
- [ ] Documentation: Update incident ticket (timeline, measures, communication)

Phase 5: Follow-up (within 1 week)

- [ ] Root cause analysis:
  - Technical cause (policy gap, false negative)
  - Human cause (carelessness, lack of training, malicious intent)
- [ ] Remediation:
  - Adjust policy
  - Additional controls (e.g. two-person principle for sensitive data)
  - User retraining (targeted or broad)
  - Disciplinary measures (if malicious)
- [ ] Lessons Learned: Documentation + Presentation to the Security Team
- [ ] Policy/playbook update

Phase 6: Review (quarterly)

- [ ] Review all incidents: Patterns? Repeat offenders? Vulnerabilities?
- [ ] KPI reporting to management

7.2 Escalation Matrix

Severity	Response time	Who is informed?	Measures
Critical	<15 min	CISO, Legal, CEO, Data Protection Officer	Block account, forensics, check external report
High	<1 hour	CISO, security team, user manager	Temporarily lock account, user interview, policy review
Medium	<4 hours	Security team, user's manager	User warning, retraining, increased monitoring

Severity	Response time	Who is informed?	Measures
Low	< 24 hours	Security team	Logging, in case of recurrence → Medium

8 Phase 8: KPIs & reporting (continuous)

8.1 DLP KPI dashboard

☐ Technical metrics

KPI	Formula	Target	Detection interval
Detection rate	(Detected violations / All violations) × 100	>95%	Monthly (test with dummy data)
False positive rate	(False positives / All alerts) × 100	<5%	Weekly
Policy coverage	(Covered data channels / All data channels) × 100	100%	Quarterly
MTTR (Mean Time to Respond)	Average time from alert to containment	<1 hour (critical)	Per incident
System uptime	DLP system availability	>99.5%	Monthly

☐ Compliance metrics

KPI	Description	Target value	Reporting
Violations per 1,000 users	Number of normalised DLP violations	<10/month	Monthly
Repeat offenders	Users with >2 violations in 3 months	<2% of users	Quarterly
Incident reports (GDPR/NIS2)	Number of reportable incidents	0 (target)	Annually
Audit findings	Findings in internal/external audits	0 Critical/High	After audit
Policy compliance rate	Percentage of users who have completed policy training	>95%	Quarterly

☐ Human risk metrics

KPI	Description	Target value	Tool
Human security index	Aggregate security metric	>75/100	Human risk dashboard

KPI	Description	Target value	Tool
Phishing click rate	% of users who click in simulation	<5%	Phishing sim tool
Phishing reporting rate	% of users who report suspicious emails	>30%	Report button analytics
Training completion	% of users who have completed DLP training	>95%	LMS
Awareness score	Quiz results after training	>80% correct	LMS

8.2 Management reporting

- [ ] Monthly report (1 page)
  - Number of violations (trend)
  - Top 3 violation types
  - Critical/high incidents (details)
  - False positive rate
  - Open action items
- [ ] Quarterly executive summary
  - KPI dashboard (visual)
  - Compliance status (GDPR, NIS2, ISO 27001)
  - ROI calculation (damage prevented, fines avoided)
  - Lessons learned from incidents
  - Roadmap for next quarter

9 Phase 9: Continuous improvement (ongoing)

9.1 Review cycles

- [ ] Weekly (security team)
  - Analyse new false positives & fine-tune policies
  - Review critical violations
  - Tool performance (uptime, latency)
- [ ] Monthly (security team + IT operations)
  - KPI review
  - Evaluate user feedback
  - Policy adjustments
- [ ] Quarterly (CISO + management)
  - Strategic review: Are we achieving our goals?
  - Budget review: Are additional tools/resources needed?
  - Compliance check: Are all requirements being met?
  - Lessons learned from all incidents
- [ ] Annually (full audit)
  - External penetration test (including data exfiltration scenarios)
  - Policy review: Is everything still up to date?
  - Tool evaluation: Are there better alternatives?
  - Operating agreement: Are adjustments necessary?

9.2 Feedback loops

- [ ] User feedback channel
  - Form: "DLP block was incorrect/justified"
  - Evaluation: False positives → policy tuning
  - Response: User receives feedback within 24 hours
- [ ] Security champions programme
  - 1 champion per department (voluntary)
  - Monthly meeting: feedback, new threats, use cases
  - Champions train their teams (multipliers)

Tools & templates

Template 1: Incident response ticket

Incident ID: DLP-2026-001

Date/time: [YYYY-MM-DD, HH:MM, time zone]

Severity: [Critical / High / Medium / Low]

Status: [New / In Progress / Contained / Resolved / Closed]

DETECTION

Alert source: [DLP system / SIEM / User report]

Affected user: [Name, department, email]

Data details:

- Classification: [Public / Internal / Confidential / Restricted]
- Data type: [PII / Financial data / IP / Other]
- Volume: [Number of files / Data records / MB]

Channel: [Email / Cloud / USB / Printer / Other]

Destination: [Internal / External: Domain/Service]

CONTAINMENT

Measures:

- ☐ Account blocked (timestamp: _____)
- ☐ Email recalled (success: yes/no)
- ☐ Endpoint isolated
- ☐ Forensic snapshot created

ASSESSMENT

Root cause: [Technical / Human error / Social engineering / Malicious]

Reporting obligation: [LOCAL PART - adapt to applicable law]

- ☐ GDPR Art. 33 (Supervisory authority)
- ☐ GDPR Art. 34 (Data subjects)
- ☐ NIS2 Art. 23 (CSIRT)
- ☐ No reporting obligation (reason: _____)

FOLLOW-UP

Policy adjustments: [Description]

User measures: [Retraining / Warning / Disciplinary action / None]

Lessons learned: [Summary]

Template 2: Policy exception request

Applicant: [Name, Department]

Date: [YYYY-MM-DD]

Business justification: [Why is the exception necessary?]

Policy rule affected: [e.g. "USB block for restricted data"]

Data affected: [Classification, description]

Duration of exception: [Limited until YYYY-MM-DD / Unlimited]

Compensatory measures: [e.g. "Encrypted USB", "Dual control principle"]

Approval:

- ☐ Approved by: [CISO / Deputy]
- ☐ Denied (Reason: _____)

Template 3: Quarterly DLP review agenda

1. KPI review (15 min)
   - Detection rate, false positive rate, violation trend
   - Action items from last quarter: status?
2. Incident review (20 min)
   - All critical/high incidents: patterns?
   - Lessons learned implemented?
3. Compliance status (10 min) [LOCAL PART]
   - GDPR: All requirements met?
   - NIS2: Reporting processes tested?
   - ISO 27001: Audit prepared?
4. User feedback (10 min)
   - Most frequent false positives → policy tuning
   - Champion feedback
5. Roadmap (15 min)
   - New requirements (new cloud tools, new data types)
   - Tool optimisation
   - Budget for next quarter
6. Action items (10 min)

- Who is doing what by when?

Appendix: Glossary & References

Glossary

- **CASB (Cloud Access Security Broker):** Control layer between users and cloud services
- **DLP (Data Leak Prevention):** Technology for preventing unauthorised data disclosure
- **DPIA (Data Protection Impact Assessment):** Mandatory analysis for high-risk data processing (GDPR Art. 35)
- **False positive:** False alarm (DLP blocks harmless action)
- **MTTR (Mean Time to Respond):** Average response time to incidents
- **PII (Personally Identifiable Information):** Personal data
- **SIEM (Security Information and Event Management):** Central logging and correlation tool
- **SOAR (Security Orchestration, Automation and Response):** Automation of security workflows
- **UEBA (User and Entity Behaviour Analytics):** Behaviour-based anomaly detection

Regulatory references [LOCAL PART]

- **GDPR (EU 2016/679):** https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **NIS2 Directive (EU 2022/2555):** https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- **ISO/IEC 27001:2022:** https://www.iso.org/standard/27001