sosafe

DLP-Implementierungs-Checkliste für IT-Entscheider

Umfassender Leitfaden zur Einführung von Data-Leak-Prevention

Executive Summary

Diese Checkliste führt Sie Schritt für Schritt durch die Einführung einer wirksamen Data-Leak-Prevention-Strategie. Sie enthält:

- Detaillierte Implementierungsschritte mit Verantwortlichkeiten
- Vorlagen für DLP-Policies und Incident-Response-Pläne
- Messbare KPIs zur Erfolgskontrolle
- Compliance-Mapping für DSGVO, NIS2 und ISO 27001
- Tool-Evaluationskriterien
- Review- und Audit-Prozesse

Zeitrahmen: 3-6 Monate für vollständige Implementierung (abhängig von Organisationsgröße)

1 Phase 1: Vorbereitung & Bestandsaufnahme (Woche 1-4)

1.1 Stakeholder-Management

- [ ] Projektteam aufstellen
  - Verantwortlich: CISO / IT-Leitung
  - Benötigt: IT-Security, Legal/Compliance, HR, Betriebsrat, Datenschutzbeauftragter
  - Deliverable: Projekt-Charter mit Budget, Zeitplan, Verantwortlichkeiten
- [ ] Executive Buy-In sichern
  - Risiko-Assessment präsentieren (potenzielle Schadenshöhe bei Data Breach)
  - Business Case: ROI durch Vermeidung von Bußgeldern, Reputationsschäden
  - Benötigte Ressourcen: Budget, FTEs, externe Beratung
- [ ] Betriebsrat/HR einbinden
  - Betriebsvereinbarung für Monitoring vorbereiten
  - Transparenz-Vorgaben definieren
  - Mitarbeitenden-Information planen

1.2 Datenbestandsaufnahme

- [ ] Data-Discovery durchführen
  - Wo liegen sensible Daten? (Fileserver, SharePoint, Cloud-Storage, Endpoints)
  - Welche Datentypen? (PII, Finanzdaten, IP, Gesundheitsdaten)
  - Wer hat Zugriff? (Berechtigungsmatrix erstellen)
  - Tool-Empfehlung: Automated Discovery Tools (z.B. Microsoft Purview, Varonis, BigID)
- [ ] Datenfluss-Mapping
  - Datenquelle → Verarbeitung → Speicherung → Weitergabe → Archivierung/Löschung
  - Kritische Pfade identifizieren (E-Mail, Cloud-Uploads, USB, Drucker)
  - Visualisierung: Data-Flow-Diagramm erstellen
- [ ] Risiko-Bewertung pro Datenkategorie

Datenkategorie	Sensitivität (1-5)	Volumen	Zugriffe/Tag	Extern geteilt?	Risiko-Score
Kundendaten (PII)	5	Hoch	500+	Ja	Kritisch
Finanzdaten	5	Mittel	50	Selten	Hoch
Quellcode	4	Hoch	200	Nein	Hoch

Datenkategorie	Sensitivität (1-5)	Volumen	Zugriffe/Tag	Extern geteilt?	Risiko-Score
Interne Docs	2	Sehr hoch	2000+	Ja	Mittel

2 Phase 2: Policy & Klassifizierung (Woche 5-8)

2.1 Datenklassifizierungs-Schema definieren

☐ Klassifizierungsstufen festlegen

Stufe	Definition	Beispiele	Zugriffsregel	Handling
Public	Für Öffentlichkeit bestimmt	Pressemitteilungen, Marketing-Material	Keine Einschränkung	Keine Verschlüsselung nötig
Internal	Intern verwendbar	Projektpläne, Meeting-Notes	Nur Mitarbeitende	Basic Access Control
Confidential	Geschäftskritisch	Verträge, Finanzprognosen, M&A-Dokumente	Need-to-know	Verschlüsselung + MFA
Restricted	Hochsensibel	Personaldaten, Zahlungsinfos, Patientenakten, Trade Secrets	Explizite Autorisierung	Verschlüsselung + MFA + Audit-Trail + DLP-Block

☐ Labeling-Prozess etablieren

- Automatische Klassifizierung: Pattern-Matching (Kreditkartennummern, IBAN, etc.)
- Manuelle Klassifizierung: User-Training + Reminder in Office-Apps
- Default-Klassifizierung: Neue Dateien standardmäßig "Internal" bis Review

☐ Klassifizierungs-Policy dokumentieren

Vorlage: Datenklassifizierungs-Richtlinie

1. Zweck

Diese Richtlinie definiert, wie Daten klassifiziert, gekennzeichnet und geschützt werden.

2. Geltungsbereich

Alle Mitarbeitenden, Contractors, Partner mit Zugriff auf Unternehmensdaten.

3. Rollen

- Data Owner: Fachbereich, definiert Klassifizierung
- Data Custodian: IT, implementiert technische Kontrollen
- Data User: Nutzer, hält sich an Handling-Vorgaben

4. Klassifizierungs-Entscheidungsbaum

Enthält die Daten personenbezogene Informationen? → JA → Restricted
Würde Offenlegung dem Unternehmen schaden? → JA → Confidential

Ist es für interne Zwecke? → JA → Internal
Sonst → Public

5. Re-Klassifizierung
Jährliches Review durch Data Owner. Bei Änderung: Label aktualisieren.

2.2 DLP-Policy erstellen

☐ Policy-Dokument verfassen

Vorlage: Data-Leak-Prevention-Policy

1. Zweck
Verhinderung unbefugter Weitergabe sensibler Unternehmensdaten.

2. Geltungsbereich
Alle Systeme, Netzwerke, Endgeräte, Cloud-Dienste.

3. Verbotene Aktionen
- Transfer von "Restricted" oder "Confidential" Daten an private E-Mail-Adressen
- Upload sensibler Daten in nicht freigegebene Cloud-Dienste
- Kopieren sensibler Daten auf USB-Sticks ohne Verschlüsselung
- Screenshots von "Restricted" Dokumenten ohne Genehmigung

4. DLP-Kontrollpunkte
- E-Mail-Gateway (Inbound/Outbound)
- Web-Proxy (Cloud-Uploads)
- Endpoint-Agents (USB, Clipboard, Screenshot)
- Cloud-API-Integration (Microsoft 365, Google Workspace, Slack)

5. Enforcement-Modi
- Monitor: Nur Logging, kein Block (Pilotphase)
- Alert: Warnung an User + Security-Team
- Block: Automatische Blockade + Incident-Ticket

6. Ausnahmen
Ausnahmen nur durch CISO genehmigt, zeitlich begrenzt, dokumentiert.

7. Incident-Response
Bei Verstoß: Automatisches Ticket → Bewertung innerhalb 4h → Eskalation falls Restricted-Daten betroffen

8. Review
Quartalsweise Policy-Review, nach jedem Incident.

☐ Least-Privilege-Matrix erstellen

Rolle	Kundendaten	Finanzdaten	HR-Daten	Quellcode	Marketing-Docs
Vertrieb	Lesen + Bearbeiten	-	-	-	Lesen
Finance	-	Lesen + Bearbeiten	-	-	-
HR	Lesen (Namen /Kontakt)	-	Lesen + Bearbeiten	-	-
Engineering	-	-	-	Lesen + Bearbeiten	-
Marketing	Lesen (anonymisiert)	-	-	-	Lesen + Bearbeiten
Executives	Lesen (alle)	Lesen (alle)	Lesen (alle)	Lesen (alle)	Lesen (alle)

☐ Access-Review-Prozess definieren

- Quartalsweise: Jeder Manager reviewed Zugriffsrechte seines Teams
- Bei Rollenwechsel: Automatischer Entzug alter Rechte + Antrag neue Rechte
- Bei Austritt: Sofortiger Entzug aller Zugriffe

3 Phase 3: Tool-Evaluierung & -Auswahl (Woche 9-12)

3.1 Anforderungskatalog

- [ ] Must-Have-Features
  - [ ] Unterstützung aller Datenkanäle (E-Mail, Web, Endpoint, Cloud)
  - [ ] Content-Inspection (Pattern Matching, ML-basiert, OCR)
  - [ ] Integration mit bestehenden Systemen (SIEM, SOAR, Ticketing)
  - [ ] Verschlüsselungs-Integration
  - [ ] Granulare Policy-Kontrolle (pro Datenkategorie, User-Gruppe, Aktion)
  - [ ] Compliance-Reporting (DSGVO, NIS2, ISO 27001)
  - [ ] False-Positive-Management (User-Feedback-Loop, ML-Tuning)
- [ ] Nice-to-Have-Features
  - [ ] Behavioral Analytics (UEBA)
  - [ ] Data-at-Rest-Scanning (Discovery)
  - [ ] Automatische Klassifizierung
  - [ ] Remediation-Workflows (z.B. automatische Verschlüsselung statt Block)
  - [ ] User-Self-Service (Freigabe-Anfragen)

3.2 Vendor-Evaluation-Matrix

- [ ] Shortlist erstellen & bewerten

Kriterium	Gewichtung	Vendor A	Vendor B	Vendor C
Funktionalität				
E-Mail-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/Behavioral	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				

Kriterium	Gewichtung	Vendor A	Vendor B	Vendor C
Admin-UI	5%	8/10	7/10	9/10
False-Positive-Mgmt	10%	9/10	8/10	7/10
Kosten				
Lizenzkosten	5%	7/10	8/10	9/10
Impl.-Aufwand	5%	8/10	7/10	8/10
Gesamt-Score	100%	8,2	8,1	7,3

- [ ] POC durchführen
  - Testdauer: 4 Wochen
  - Test-Scope: E-Mail + Cloud + 50 Test-Endpoints
  - Success-Kriterien: <5% False Positives, <100ms Latenz, 95%+ Detection-Rate

4 Phase 4: Implementierung (Woche 13-20)

4.1 Technische Implementierung

- [ ] E-Mail-DLP
  - MX-Record-Anpassung oder SMTP-Relay-Konfiguration
  - Policy-Regeln: Outbound-Scan für Restricted/Confidential-Daten
  - Quarantäne-Postfach einrichten
  - Eskalations-Workflow: Security-Team + Manager bei Block
- [ ] Web/Cloud-DLP
  - Proxy-Integration oder Cloud-CASB
  - SSL-Inspection aktivieren (Achtung: Datenschutz-Implikationen)
  - API-Connectors: Microsoft 365, Google Workspace, Slack, Salesforce
  - Policy: Block Upload von Restricted-Daten in unapproved Cloud-Services
- [ ] Endpoint-DLP
  - Agent-Rollout (schrittweise: IT → Pilotgruppe → Vollrollout)
  - USB-Blockade für Restricted-Daten (Allow-List für verschlüsselte USBs)
  - Clipboard-Kontrolle, Screenshot-Prevention
  - Offline-Modus: Policy-Enforcement auch ohne Netzwerkverbindung
- [ ] Incident-Management-Integration
  - SIEM-Integration: DLP-Alerts → Correlation mit anderen Security-Events
  - Ticketing: Automatische Tickets bei High-Severity-Violations
  - SOAR-Playbooks: Automatische Kontosperrung bei kritischen Violations

4.2 Rollout-Plan

- [ ] Pilotphase (Woche 13-16)
  - Zielgruppe: IT-Abteilung (20-50 User)
  - Modus: Monitor-only
  - Ziel: Baseline etablieren, False-Positive-Rate ermitteln, Policies tunen
- [ ] Phased Rollout (Woche 17-20)
  - Woche 17: Finance (Alert-Modus)
  - Woche 18: HR + Legal (Alert-Modus)
  - Woche 19: Engineering + Sales (Alert-Modus)
  - Woche 20: Restliche Organisation (Alert-Modus)

- [ ] Enforcement-Phase (ab Woche 21)
  - Schrittweise Umstellung auf Block-Modus
  - Start mit Restricted-Daten
  - Nach 2 Wochen: Auch Confidential-Daten

5 Phase 5: Human-Risk-Management (parallel zu Phase 4)

5.1 Awareness-Kampagne

- [ ] Kommunikationsplan
  - Woche 12: Ankündigung durch CEO/CISO (All-Hands-Meeting)
  - Woche 13-16: Pilotgruppe: Intensive Schulung + Q&A-Sessions
  - Woche 17-20: Rollout-Kommunikation: Intranet-Artikel, E-Mail, Manager-Briefings
  - Ab Woche 21: Kontinuierliche Reminder (monatlicher Newsletter)
- [ ] Trainings-Module entwickeln
  1. Modul 1: Warum DLP? (5 Min)
     - Risiken von Data Breaches (Beispiel-Cases)
     - Rechtliche Verpflichtungen (DSGVO, NIS2)
     - Persönliche Verantwortung
  2. Modul 2: Datenklassifizierung (10 Min)
     - Stufen & Beispiele
     - Wie klassifiziere ich korrekt?
     - Praxis-Übung: 5 Beispiel-Dokumente klassifizieren
  3. Modul 3: Was darf ich (nicht)? (10 Min)
     - Do's & Don'ts
     - Was passiert bei Verstoß?
     - Wie beantrage ich Ausnahmen?
  4. Modul 4: Phishing & Social Engineering (15 Min)
     - Erkennung von Phishing-Mails
     - CEO-Fraud-Szenarien
     - Meldeprozess
- [ ] Phishing-Simulationen
  - Frequenz: Monatlich, randomisiert
  - Template-Rotation: CEO-Fraud, Fake-Invoice, Credential-Phishing, Malware-Attachment
  - Follow-Up: Bei Klick → Sofort Microlearning (3 Min)
  - Gamification: Leaderboard (anonymisiert), Badges für Melder

5.2 Human-Risk-Dashboard

- [ ] KPIs definieren & tracken

KPI	Zielwert	Messmethode
Phishing-Klickrate	<5%	Phishing-Simulation-Tool
Melderate (verdächtige Mails)	>30%	Phishing-Report-Button-Analytics
Training-Completion-Rate	>95%	LMS-Reporting
DLP-Violations pro 1000 User	<10/Monat	DLP-System-Logs
Wiederholungs-Violations (selber User)	<2%	DLP-System-Analytics
Human-Security-Index	>75/100	Human-Risk-Management-Dashboard

6 Phase 6: Compliance & Dokumentation (Woche 21-24)

6.1 Compliance-Mapping

☐ DSGVO-Anforderungen abdecken

DSGVO-Artikel	Anforderung	DLP-Maßnahme	Status
Art. 5 (1f)	Integrität & Vertraulichkeit	DLP-Policies + Verschlüsselung	☐
Art. 25	Privacy by Design	Default-Klassifizierung "Internal"	☐
Art. 32	Technische Maßnahmen	DLP + Access Control + Monitoring	☐
Art. 33	Meldepflicht (72h)	Incident-Response-Integration	☐
Art. 35	DSFA	DSFA für DLP-Monitoring durchgeführt	☐

☐ NIS2-Anforderungen abdecken

NIS2-Artikel	Anforderung	DLP-Maßnahme	Status
Art. 21	Cybersecurity-Risikomanagement	DLP als Teil der Risikomanagement-Strategie	☐
Art. 23	Meldepflicht (24h Erstmeldung)	Automatische Alerts + Eskalation	☐
Art. 32	Audit & Dokumentation	DLP-Logs, Policy-Dokumente, Audit-Trails	☐

☐ ISO 27001:2022 Annex A 8.12 abdecken

- Data-Leakage-Prevention als Kontrollmaßnahme dokumentiert
- Prozessbeschreibung: Wie verhindert die Organisation Exfiltration?
- Nachweisdokumente: DLP-Policy, Tool-Config, Logs, Incident-Reports

6.2 Dokumentation

☐ Pflichtdokumente erstellen

- ☐ DLP-Policy (siehe Vorlage oben)
- ☐ Datenklassifizierungs-Richtlinie
- ☐ Incident-Response-Plan (siehe unten)

- [ ] Betriebsvereinbarung (Monitoring)
- [ ] Datenschutz-Folgenabschätzung (DSFA)
- [ ] Admin-Handbuch (DLP-System)
- [ ] User-Guide (Datenklassifizierung, Ausnahme-Prozess)

7 Phase 7: Incident Response (kontinuierlich)

7.1 Incident-Response-Plan

Vorlage: DLP-Incident-Response-Playbook

Phase 1: Erkennung (0-15 Min)

- [ ] DLP-Alert empfangen (E-Mail, SIEM, Ticket)
- [ ] Severity-Einstufung:
  - Critical: Restricted-Daten + extern + großes Volumen
  - High: Confidential-Daten + extern
  - Medium: Confidential-Daten + intern
  - Low: Internal-Daten + ungewöhnliches Verhalten
- [ ] On-Call-Engineer assigned

Phase 2: Eindämmung (15-60 Min)

- [ ] Bei Critical/High: Sofortmaßnahmen
  - Betroffenes Konto sperren
  - E-Mail aus Empfänger-Postfach zurückrufen (falls noch möglich)
  - Netzwerkverbindung des Endpoints trennen (falls aktive Exfiltration)
- [ ] Forensik-Snapshot erstellen (Logs, Memory-Dump, Disk-Image)
- [ ] Incident-Commander informieren (CISO oder Deputy)

Phase 3: Bewertung (1-4h)

- [ ] Daten-Assessment:
  - Welche Daten? (Klassifizierung, Volumen, Anzahl betroffener Personen)
  - Wohin? (Empfänger intern/extern, Domäne, Cloud-Service)
  - Wie? (E-Mail, USB, Cloud-Upload, Screenshot)
  - Warum? (Versehen, Social Engineering, böswillig)
- [ ] User-Interview (falls erreichbar, nicht bei Verdacht auf böswillige Absicht)
- [ ] Rechtliche Bewertung: Meldepflicht DSGVO/NIS2?
  - DSGVO Art. 33: Meldung binnen 72h an Aufsichtsbehörde?
  - NIS2 Art. 23: Erstmeldung binnen 24h an CSIRT/Behörde?
  - Betroffene Personen informieren? (Art. 34 DSGVO)
- [ ] Entscheidung: Eskalation an Geschäftsführung/Legal?

Phase 4: Meldung (innerhalb gesetzlicher Fristen)

- [ ] Interne Meldung: Incident-Report an CISO, Legal, Datenschutzbeauftragten
- [ ] Externe Meldung (falls erforderlich):
  - DSGVO: Meldung an zuständige Aufsichtsbehörde (Formular)
  - NIS2: Erstmeldung an CSIRT/zuständige Behörde
  - Betroffene Personen: E-Mail/Brief mit Details + Handlungsempfehlungen
- [ ] Dokumentation: Incident-Ticket aktualisieren (Timeline, Maßnahmen, Kommunikation)

Phase 5: Nachbereitung (innerhalb 1 Woche)

- [ ] Root-Cause-Analyse:
  - Technische Ursache (Policy-Lücke, False Negative)
  - Menschliche Ursache (Unachtsamkeit, fehlende Schulung, Böswilligkeit)
- [ ] Remediation:
  - Policy anpassen
  - Zusätzliche Kontrollen (z.B. Zwei-Personen-Prinzip für sensible Daten)
  - User-Nachschulung (gezielt oder breit)
  - Disziplinarmaßnahmen (falls böswillig)
- [ ] Lessons Learned: Dokumentation + Präsentation im Security-Team
- [ ] Policy/Playbook-Update

Phase 6: Review (quartalsweise)

- [ ] Alle Incidents reviewen: Patterns? Wiederholungstäter? Schwachstellen?
- [ ] KPI-Reporting an Management

7.2 Eskalations-Matrix

Severity	Reaktionszeit	Wer wird informiert?	Maßnahmen
Critical	< 15 Min	CISO, Legal, CEO, Datenschutzbeauftragter	Konto sperren, Forensik, externe Meldung prüfen
High	< 1h	CISO, Security-Team, Manager des Users	Konto temporär sperren, User-Interview, Policy-Review
Medium	< 4h	Security-Team, Manager des Users	User-Warnung, Nachschulung, Monitoring verschärfen
Low	< 24h	Security-Team	Logging, bei Wiederholung → Medium

8 Phase 8: KPIs & Reporting (kontinuierlich)

8.1 DLP-KPI-Dashboard

☐ Technische Metriken

KPI	Formel	Zielwert	Erfassungsintervall
Detection-Rate	(Erkannte Violations / Alle Violations) × 100	>95%	Monatlich (Test mit Dummy-Data)
False-Positive-Rate	(False Positives / Alle Alerts) × 100	<5%	Wöchentlich
Policy-Coverage	(Abgedeckte Datenkanäle / Alle Datenkanäle) × 100	100%	Quartalsweise
MTTR (Mean Time to Respond)	Durchschnittliche Zeit von Alert bis Eindämmung	<1h (Critical)	Pro Incident
System-Uptime	Verfügbarkeit DLP-System	>99,5%	Monatlich

☐ Compliance-Metriken

KPI	Beschreibung	Zielwert	Reporting
Violations pro 1000 User	Anzahl DLP-Violations normalisiert	<10/Monat	Monatlich
Repeat-Offenders	User mit >2 Violations in 3 Monaten	<2% der User	Quartalsweise
Incident-Meldungen (DSGVO/NIS2)	Anzahl meldepflichtiger Vorfälle	0 (Ziel)	Jährlich
Audit-Findings	Findings in internen/externen Audits	0 Critical/High	Nach Audit
Policy-Compliance-Rate	Anteil User, die Policy-Training absolviert haben	>95%	Quartalsweise

☐ Human-Risk-Metriken

KPI	Beschreibung	Zielwert	Tool
Human-Security-Index	Aggregierte Sicherheitsmetrik	>75/100	Human-Risk-Dashboard

KPI	Beschreibung	Zielwert	Tool
Phishing-Klickrate	% User, die in Simulation klicken	<5%	Phishing-Sim-Tool
Phishing-Melderate	% User, die verdächtige Mails melden	>30%	Report-Button-Analytics
Training-Completion	% User mit abgeschlossenem DLP-Training	>95%	LMS
Awareness-Score	Quiz-Ergebnisse nach Training	>80% korrekt	LMS

8.2 Management-Reporting

- [ ] Monatlicher Bericht (1-Seiter)
  - Anzahl Violations (Trend)
  - Top-3-Violation-Typen
  - Critical/High Incidents (Details)
  - False-Positive-Rate
  - Offene Action Items
- [ ] Quartalsweise Executive Summary
  - KPI-Dashboard (visuell)
  - Compliance-Status (DSGVO, NIS2, ISO 27001)
  - ROI-Berechnung (verhinderte Schäden, vermiedene Bußgelder)
  - Lessons Learned aus Incidents
  - Roadmap für nächstes Quartal

9 Phase 9: Continuous Improvement (kontinuierlich)

9.1 Review-Zyklen

- [ ] Wöchentlich (Security-Team)
  - Neue False Positives analysieren & Policies tunen
  - Kritische Violations reviewen
  - Tool-Performance (Uptime, Latenz)
- [ ] Monatlich (Security-Team + IT-Operations)
  - KPI-Review
  - User-Feedback auswerten
  - Policy-Adjustments
- [ ] Quartalsweise (CISO + Management)
  - Strategische Review: Erreichen wir die Ziele?
  - Budget-Review: Zusätzliche Tools/Ressourcen nötig?
  - Compliance-Check: Alle Anforderungen erfüllt?
  - Lessons Learned aus allen Incidents
- [ ] Jährlich (Vollständiger Audit)
  - Externer Penetration-Test (inkl. Data-Exfiltration-Szenarien)
  - Policy-Review: Ist alles noch aktuell?
  - Tool-Evaluation: Gibt es bessere Alternativen?
  - Betriebsvereinbarung: Anpassungen nötig?

9.2 Feedback-Loops

- [ ] User-Feedback-Kanal
  - Formular: "DLP-Blockade war falsch / berechtigt"
  - Auswertung: False Positives → Policy-Tuning
  - Response: User bekommt Rückmeldung innerhalb 24h
- [ ] Security-Champions-Programm
  - 1 Champion pro Abteilung (freiwillig)
  - Monatliches Treffen: Feedback, neue Bedrohungen, Use Cases
  - Champions schulen ihre Teams (Multiplikatoren)

Tools & Templates

Template 1: Incident-Response-Ticket

Incident-ID: DLP-2026-001

Datum/Zeit: 2026-01-22, 14:35 CET

Severity: [Critical / High / Medium / Low]

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

DETECTION

Alert-Quelle: [DLP-System / SIEM / User-Meldung]

Betroffener User: [Name, Abteilung, E-Mail]

Daten-Details:

- Klassifizierung: [Public / Internal / Confidential / Restricted]
- Datentyp: [PII / Finanzdaten / IP / Sonstiges]
- Volumen: [Anzahl Dateien / Datensätze / MB]
- Kanal: [E-Mail / Cloud / USB / Drucker / Sonstiges]

Ziel: [Intern / Extern: Domain/Service]

EINDÄMMUNG

Maßnahmen:

- ☐ Konto gesperrt (Zeitstempel: _____)
- ☐ E-Mail zurückgerufen (Erfolg: Ja/Nein)
- ☐ Endpoint isoliert
- ☐ Forensik-Snapshot erstellt

BEWERTUNG

Root Cause: [Technisch / Menschliches Versehen / Social Engineering / Böswillig]

Meldepflicht:

- ☐ DSGVO Art. 33 (Aufsichtsbehörde)
- ☐ DSGVO Art. 34 (Betroffene Personen)
- ☐ NIS2 Art. 23 (CSIRT)
- ☐ Keine Meldepflicht (Begründung: _____)

NACHBEREITUNG

Policy-Anpassungen: [Beschreibung]

User-Maßnahmen: [Nachschulung / Verwarnung / Disziplinarmaßnahme / Keine]

Lessons Learned: [Zusammenfassung]

Template 2: Policy-Exception-Request

Antragsteller: [Name, Abteilung]

Datum: [YYYY-MM-DD]

Geschäftsbegründung: [Warum ist die Ausnahme nötig?]

Betroffene Policy-Regel: [Z.B. "USB-Blockade für Restricted-Daten"]

Betroffene Daten: [Klassifizierung, Beschreibung]

Dauer der Ausnahme: [Befristet bis YYYY-MM-DD / Unbefristet]

Kompensationsmaßnahmen: [Z.B. "Verschlüsselter USB", "Vier-Augen-Prinzip"]

Genehmigung:

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

Template 3: Quartalsweise DLP-Review-Agenda

1. KPI-Review (15 Min)
   - Detection-Rate, False-Positive-Rate, Violations-Trend
   - Action Items aus letztem Quartal: Status?
2. Incident-Review (20 Min)
   - Alle Critical/High-Incidents: Patterns?
   - Lessons Learned umgesetzt?
3. Compliance-Status (10 Min)
   - DSGVO: Alle Anforderungen erfüllt?
   - NIS2: Meldeprozesse getestet?
   - ISO 27001: Audit vorbereitet?
4. User-Feedback (10 Min)
   - Häufigste False Positives → Policy-Tuning
   - Champions-Feedback
5. Roadmap (15 Min)
   - Neue Anforderungen (neue Cloud-Tools, neue Datentypen)
   - Tool-Optimierung
   - Budget für nächstes Quartal
6. Action Items (10 Min)

- Wer macht was bis wann?

Anhang: Glossar & Referenzen

Glossar

- **CASB (Cloud Access Security Broker):** Kontrollschicht zwischen Nutzern und Cloud-Diensten
- **DLP (Data-Leak-Prevention):** Technologie zur Verhinderung unbefugter Datenoffenlegung
- **DSFA (Datenschutz-Folgenabschätzung):** Pflichtanalyse bei risikoreichen Datenverarbeitungen (DSGVO Art. 35)
- **False Positive:** Fehlalarm (DLP blockt harmlose Aktion)
- **MTTR (Mean Time to Respond):** Durchschnittliche Reaktionszeit bei Incidents
- **PII (Personally Identifiable Information):** Personenbezogene Daten
- **SIEM (Security Information and Event Management):** Zentrales Logging und Correlation-Tool
- **SOAR (Security Orchestration, Automation and Response):** Automatisierung von Security-Workflows
- **UEBA (User and Entity Behavior Analytics):** Verhaltensbasierte Anomalie-Erkennung

Regulatorische Referenzen

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