sesame software

DLP Best Practices Cheat Sheet

A practical checklist for reducing data leakage and strengthening data protection

Quick Start (Fastest Wins First)

If you need to tighten DLP quickly, start here:

1. Define sensitive data categories
2. Restrict external sharing
3. Require MFA everywhere
4. Enforce least privilege
5. Reduce alert noise

The DLP Best Practices Checklist

Use this simplified implementation checklist:

- ✓ Define sensitive data categories
- ✓ Build a simple classification model
- ✓ Assign DLP ownership
- ✓ Start with high-impact policies
- ✓ Reduce alert noise
- ✓ Enforce least privilege
- ✓ Require MFA everywhere
- ✓ Restrict external sharing
- ✓ Protect SaaS-to-SaaS data movement
- ✓ Apply endpoint DLP to high-risk roles
- ✓ Monitor behavior anomalies
- ✓ Maintain a recovery plan for critical systems

Starter Policies to Implement First

If you don't know where to begin, these policies create immediate impact:

- Block public links for restricted data
- Require link expiration for external sharing
- Alert on sensitive data sent outside approved domains
- Restrict downloads on unmanaged devices
- Flag bulk access to customer or financial data
- Monitor third-party app authorizations

High-Risk Signals to Monitor

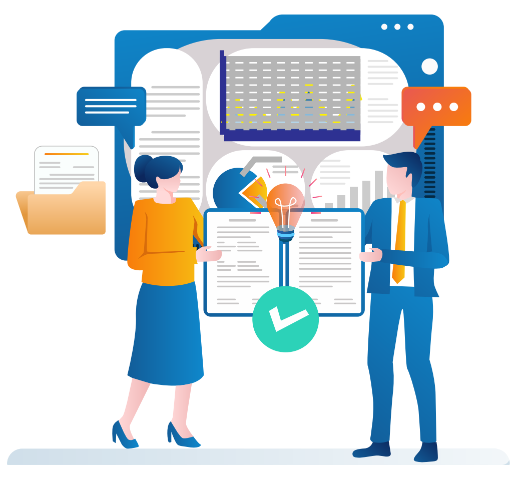
These patterns are common early indicators of data leakage:

- Mass downloads or unusual export activity
- External sharing spikes
- Access outside normal working hours
- Sudden privileged-user behavior changes
- New SaaS integrations or connected apps
- Sensitive data accessed from unmanaged devices

Common DLP Mistakes

Avoid these traps that cause most DLP programs to fail:

- Blocking too much too early
- Treating DLP as "set it and forget it"
- Ignoring SaaS-to-SaaS data movement
- Generating too many alerts without clear workflows
- Assuming DLP replaces backup and recovery



DLP Maturity Snapshot

Where does your program sit today?

Level 1: Basic Protection
Policies + MFA + access control

Level 2: Operationalized DLP
Tuning + monitoring + response workflows

Level 3: Resilient Protection
Automation + incident response + recovery readiness

Recommended Review Cadence

Weekly: review high-severity alerts
Monthly: tune policies and reduce false positives
Quarterly: audit access and privileged roles
Annually: reassess classification model and risk categories

Key Reminder (Prevention vs. Recovery)

DLP reduces exposure risk.
Backup and recovery reduce business impact.
Strong data protection strategies include both.

Want to strengthen your data protection strategy?

Talk to a Data Expert

Sesame Software | Take control of your data.

About Sesame Software

Sesame Software is the Enterprise Data Management leader, delivering data rapidly for enhanced reporting and analytics. Sesame Software's data platform offers superior solutions for data warehousing, integration, as well as backup, and compliance to fit your business needs. Quickly connect to SaaS, on-premise, and cloud applications for accelerated insights. Learn more today!

☎ +1 (408) 550-7999 ✉ info@sesamesoftware.com www.sesamesoftware.com