Dual Document & Data Storage System Checklist

Google Workspace for low-sensitivity work, Tresorit for medium- and high-sensitivity data. This checklist walks through classification, setup, migration, and the policy decisions that make the split actually hold up in practice.

1. Classify Your Data Before You Touch Either Platform

This has to happen first. Without it, staff default to whatever's easiest, usually Google, and the system doesn't work.

- ☐ Define your organization's sensitivity tiers (we recommend 2 or 3, not more; a 5-tier system won't get used):
  - ☐ Low: general programmatic work, public-facing drafts, routine admin, scheduling
  - ☐ Medium: legal or HR files, strategic plans, internal memos
  - ☐ High: donor and beneficiary PII, incident response records, anything with legal discovery exposure
- ☐ Identify and document your organization's low-, medium-, and high-risk categories

2. Set Up Google Workspace (Low-Sensitivity Tier)

Admin console configuration

- ☐ Set default link-sharing to "Restricted" org-wide (not "Anyone with the link")
- ☐ Disable external sharing by default; allow it per-domain or per-request only
- ☐ Enforce 2-factor authentication for all accounts (security key, passkey, or authenticator app, not SMS)
- ☐ Advanced: Turn on Google Workspace DLP rules to flag exports/shares containing SSNs, financial account numbers, or other PII patterns
- ☐ Disable "Show editors" in version history for shared links
- ☐ Set a data retention / auto-delete policy for Drive trash and shared drive versions

Structure

- [ ] Create Shared Drives (not "My Drive" folders) for team-owned content so access survives staff turnover
- [ ] Build a folder structure that mirrors your data tiers, so "where does this go" has an obvious answer
- [ ] Name shared drives and top-level folders consistently (e.g., by program, not by person)

Access

- [ ] Audit current sharing permissions; remove former external collaborators and "Anyone with the link" shares
- [ ] Set quarterly permission review as a recurring calendar item, not a one-time cleanup

3. Set Up Tresorit (Medium/High-Sensitivity Tier)

Account & structure

- [ ] Provision Tresorit accounts for staff who will handle medium/high-sensitivity data
- [ ] Build a Tresorit folder structure with clear permission hierarchies (mirror the Workspace structure where useful)
- [ ] Set permission levels deliberately: Managers (read/change/re-share) only for those who need to grant access; most staff should be Editors or Viewers

Collaboration approach

- [ ] Decide your desktop vs. web policy: Tresorit Drive for staff who prefer local file editing, web interface for occasional access
- [ ] Tresorit is not built for the kind of real-time multi-editor collaboration Google Docs offers; plan workflows accordingly (e.g., check-out/check-in norms, or draft in Google at low sensitivity and move final sensitive versions to Tresorit)

Sharing controls

- [ ] Set expiration dates as default practice on all shared links
- [ ] Use download limits (i.e., 5–10 opens) for highly sensitive one-off shares
- [ ] Enable access logs (browser, IP, email) on shared links for anything above medium sensitivity
- [ ] Require email verification before link access for high-sensitivity shares
- [ ] Apply watermarking on shared documents/videos where leak-tracing matters

☐ Send link passwords through a separate channel from the link itself (e.g., Signal, not the same email)

4. Write the Policy That Ties Both Together

☐ Draft a one-page "where does this go" policy: tier definitions, examples, and the platform each maps to

☐ Name a specific person or role responsible for policy questions and edge cases

☐ Decide how you'll handle documents that start low-sensitivity and become sensitive (e.g., a draft becomes a legal matter): who moves it, and when

☐ Set a policy on AI tool use with each tier: flag that most AI platforms retain and can be compelled to produce data, similar to standard cloud storage, so high-sensitivity documents shouldn't be pasted into AI tools by default

☐ Circulate the policy in writing (not just verbally in a meeting) and store it somewhere staff will actually find it again

5. Migrate Existing Data

☐ Inventory what's currently in Google Drive that should be reclassified as medium/high sensitivity

☐ Move those files to Tresorit; don't leave duplicate copies behind in Google Drive

☐ Remove metadata from sensitive documents before they're moved or shared (Document Inspector in Word/Google Docs, or ExifTool/BleachBit for a final pass)

☐ Check for sensitive data sitting in email threads or chat history that should be relocated to structured storage

Quick Reference: What Goes Where

Category	Detail
Low sensitivity	General programmatic drafts, public-facing content, routine scheduling and admin, non-sensitive internal comms
Medium/high sensitivity	Donor & beneficiary PII, legal and HR files, strategic/campaign plans, incident response records, anything with litigation discovery exposure
Platform	Google Workspace (low) → Tresorit (medium/high)
AI tools	Treat like cloud storage for discovery purposes; don't paste high-sensitivity content into AI platforms by default

Revision #2
Created 2 July 2026 03:25:43 by Josh

Updated 2 July 2026 03:26:45 by Josh