Document Storage and Sharing

- Removing Metadata from Word Documents & PDFs
- Using Tresorit for file storage and editing
- Best Practices for Safely Sharing Google Docs
- Best Practices for Preventing Unauthorized Document Capture and Access
- Secure Document Sharing & Retention Framework

Removing Metadata from Word Documents & PDFs

What Metadata Is and Why It Matters

Metadata is hidden information stored within files — like author names, document history, comments, tracked changes, revision dates, and even location data. It can reveal sensitive details unintentionally and should always be removed before sharing documents externally.

Common Metadata Found in Files Microsoft Word Documents (.docx)

- Author and company names
- Hidden comments and tracked changes
- Document revisions, timestamps, and file path
- Custom properties or template information

PDF Files:

- Author, creation date, and software used
- Hidden text layers and annotations
- Embedded links or tags from original source files
- GPS or image EXIF data (if the PDF includes photos)

How to Remove Metadata in Microsoft Word

Option 1: Use the Document Inspector (Windows desktop version)

1. Open the document in Word.
2. Click File → Info.
3. In the right-hand panel, click Check for Issues → Inspect Document.
4. In the Document Inspector window, check all the boxes (especially Comments, Revisions, Versions, and Annotations).
5. Click Inspect.
6. Review the results, then click Remove All next to each category you want to delete.
7. Click Close, then Save As to create a clean version for sharing.

Option 2: For Word on Mac

1. Open your document.
2. From the Tools menu, select Protect Document.

3. Check the box labeled Remove personal information from this file on save.
4. Save the document. This strips identifying metadata automatically.

Option 3: Manual Cleanup (All Versions)

- Accept or reject all tracked changes.
- Delete all comments (Review → Delete → Delete All Comments in Document).
- Ensure “Author” and “Company” fields in File → Info → Properties → Advanced Properties → Summary are blank.
- Save the cleaned file as a new copy.

How to Remove Metadata from PDFs Using Adobe Acrobat

1. Open the PDF.
2. Go to File → Properties → Description and clear all fields.
3. Then go to Tools → Redact → Remove Hidden Information.
4. Check all boxes (comments, metadata, file attachments, etc.) and click Remove.
5. Save the sanitized version under a new file name.

Removing Metadata from Google Docs (Before Downloading as Word Files)

When downloaded as Word (.docx) files, Google Docs can retain:

- Document owner name and email address
- Revision and comment history
- “Last edited by” details
- Internal sharing permissions

Best Practices Before Downloading Option 1: Create a Clean Copy

1. Click File → Make a copy in Google Docs.
2. In the new copy: o Delete all comments and suggestions (Tools → Review suggested edits → Accept all). o Remove all collaborators (Share → Remove access). o Ensure your name/email are removed from the document title and content.
3. Download as Microsoft Word (.docx).
4. Open the file in Word and run the Document Inspector (see Section 3 above).

Option 2: Export as PDF

1. Click File → Download → PDF Document (.pdf).
2. Most collaborative metadata will be stripped automatically.
3. Use Adobe Acrobat’s “Remove Hidden Information” or BleachBit/ExifTool for a final clean.

For Highly Sensitive Documents

- Avoid personal names or internal links in content or comments.

- Use a neutral, non-personal account (e.g., admin@organization.org) as the file owner.
- Rename files generically before sharing (e.g., Policy_Guidelines_CLEAN.docx).
- After download, recheck metadata in Word before distribution.

Automation for Google Workspace Admins

- Disable “Show editors” in version history for shared links.
- Set default link-sharing to “Restricted” or “Anyone with the link (Viewer).”
- Use Google Workspace DLP rules to flag documents with personal data before export.

Organizational Best Practices

- Always inspect documents before sharing. Make this part of your publication or communication workflow.
- Never rely on “print to PDF” alone. Some metadata can survive that process.
- Store original versions securely on encrypted storage like Tresorit, not in email threads or shared folders.
- Train all staff on why metadata matters as part of regular cybersecurity and privacy awareness.

When in Doubt

If a file contains sensitive content (e.g., internal strategy, donor data, or legal documents), sanitize it twice — once in its native format and again after conversion to PDF. For highly sensitive reports, share only through encrypted channels like Tresorit or Signal.

Using Tresorit for file storage and editing

For organizations handling highly sensitive information where security outweighs convenience concerns, Tresorit provides privacy and security that mainstream providers cannot match. However, teams requiring extensive real-time collaboration may need to supplement with other tools or accept Tresorit's limitations, developing a policy dictating when to store data on Tresorit rather than on other systems, i.e. Google Drive.

What is Tresorit?

Tresorit is a secure cloud storage service based in Switzerland that uses end-to-end encryption and zero-knowledge authentication to ensure a very high level of security. As a Swiss company, Tresorit cannot be compelled to participate in mass surveillance by US or EU intelligence agencies.

How It Works

End-to-End Encryption: Your files are encrypted on your device and never decrypted until they reach your intended recipient - only you and anyone you authorize can decrypt the files. Tresorit uses AES-256, one of the most secure symmetric encryption standards available.

Zero-Knowledge: Tresorit doesn't store passwords or have access to unencrypted data. This means that even if Tresorit gets hacked or authorities demand your information, there's nothing to find on their servers.

Data Storage & Jurisdiction

- Primary Location: By default, data is encrypted and stored in data centers in Ireland and the Netherlands
- Legal Protection: Tresorit is subject to Switzerland's strong data protection laws

Key Differences from Google Drive

Feature	Google Drive	Tresorit
Encryption	Data on servers is not end-to-end encrypted, Google can decrypt	End-to-end encryption - files never decrypted on servers, only users can decrypt

Access by Provider	Google can access file content for various business purposes or to respond to a law enforcement request	Zero-knowledge - Tresorit cannot access your data
Government Requests	Must comply with U.S. government data requests, often with gag orders	Swiss jurisdiction protects against mass surveillance requests
Real-time Collaboration	Built-in document editing and collaboration	Primarily secure storage and sharing. But users can edit shared documents using Tresorit Drive on their local machines, with documents set to read-only while others are editing.

Tresorit Sharing & Collaboration Features for Teams

Secure Link Sharing

- Link Controls: Set expiry dates, download limits, and passwords on shared links
- Access Tracking: Enable access logs to track browsers, IP addresses, and email addresses that accessed your content
- Email Verification: Require recipients to verify their email before accessing shared content

Advanced Security Features

- Cooperative Links: Two-way collaboration allowing external partners to share, receive, and edit files through a single encrypted link without needing Tresorit accounts
- Watermarking: Add watermarks to shared videos and documents to prevent unauthorized re-sharing
- Download Control: Disable downloads on shared links while allowing preview

Team Collaboration

- Permission Levels: Three permission levels - Managers (read, change, re-share), Editors (read, modify), Viewers (read-only)
- File Access: Users can use Tresorit Drive to access files locally on their machines, or access cloud files directly from the Web.
- Folder Sharing: Direct collaboration in shared encrypted folders with granular access controls

Implementation Recommendations

Desktop Collaboration Strategy

1. Use Tresorit Drive for teams that prefer working in local documents rather than web interfaces

2. Implement Folder Structure with clear permission hierarchies for different materials
3. Leverage Cooperative Links for external collaboration without requiring accounts
4. Determine Storage Policies for sensitive documents that need to be stored and shared in Tresorit, rather than in Google Drive

Link Security Best Practices

- Always set expiration dates on shared links, especially for time-sensitive campaigns
- Use download limits (e.g., 5-10 opens) for highly sensitive documents
- Enable access logs for all external shares to monitor who accessed materials
- Implement password protection with separate communication channels for passwords

Best Practices for Safely Sharing Google Docs

These guidelines help you use Google Drive strategically, balancing collaboration needs with data protection and security awareness. Adapt these practices based on your organization's risk level, document sensitivity, and compliance requirements.

Before You Share: Document Classification

Ask yourself first:

- Who needs access to this document?
- What's the worst case if this document becomes public?
- Does it contain sensitive information (donor data, strategy, personal details)?
- How long will external parties need access?

Document Sensitivity Levels:

- **Public:** Annual reports, press releases, published research (share freely)
- **Internal:** Staff communications, draft materials (organization-only)
- **Confidential:** Strategy documents, donor lists, financial data (restricted sharing)
- **Highly Sensitive:** Legal materials, info that compromises sources (use Tresorit, not Google)

Sharing Permission Levels: Choose Wisely

Google Docs offers three permission levels: viewer, commenter, and editor. Use the most restrictive option that still allows necessary work:

Viewer (Read-only)

- Best for: Sharing final documents, board reports, public materials
- Recipients can: View and download (but not edit)
- Use when: You want to share information without risk of changes

Commenter

- Best for: Review processes, feedback gathering
- Recipients can: View, download, and add comments
- Use when: You need input but want to control actual edits

Editor (Full Access)

- Best for: Active collaboration with trusted colleagues
- Recipients can: View, download, edit, and share with others
- **Warning:** Editors can also re-share your document with anyone

The "Anyone with the Link" Trap

Never use "Anyone with the link" for sensitive documents. This setting makes your document accessible to anyone who obtains the URL—through forwarded emails, shared screenshots, or accidental posting.

Instead:

- Use **"Restricted"** access (specific people only)
- Manually add each person's email address
- Review the access list before sharing

Exception: Public documents like published reports can use "Anyone with the link" with "Viewer" permissions.

Access Audits: Regular Maintenance

Set a recurring calendar reminder to review document access:

Quarterly Reviews:

1. Open important documents
2. Click "Share" button
3. Review the list of people with access
4. Remove anyone who no longer needs access (former staff, completed projects, external consultants)

Immediate Removal When:

- Staff members leave the organization
- External consultants complete their work

- Board members rotate off
- Partnership agreements end

Advanced Security Settings (for owners of documents)

Enable "Prevent viewers from downloading":

- Click Share → Settings (gear icon)
- Under "People who can download, copy, and print," uncheck "Editors" and "Commenters and Viewers"
- Note: This deters but doesn't fully prevent determined users from capturing content

Restrict sharing abilities:

- Click Share → Settings (gear icon)
- Uncheck "Allow editors to change permissions and share"
- This prevents editors from adding new people

Link expiration (for Google Workspace users):

- Share → Advanced → Set expiration date
- Useful for time-limited external collaboration

Secure Sharing Workflow

For External Partners:

1. Create a "clean" version with sensitive details removed
2. Share with "Commenter" access initially
3. Set calendar reminder to revoke access when project ends
4. If extensive collaboration needed, consider other platforms (see "Alternatives" below)

For Internal Teams:

1. Create shared folders with appropriate team permissions
2. Store sensitive documents in restricted folders
3. Use clear naming conventions indicating sensitivity level
4. Document your organization's folder structure

Communication Security

Don't share sensitive documents via:

- Unsecured email with "Anyone with the link" settings
- Public Slack channels
- Social media messages

Instead:

- Send direct emails to specific individuals
- Use "Restricted" sharing with email addresses
- For highly sensitive materials, switch to Signal and use Tresorit links

What Google Can Access

Important Reality Check:

Google can access the content of your documents. While Google Drive offers encryption "at rest" and "in transit," it is not end-to-end encrypted. This means:

- Google can read your documents (for business purposes and legal compliance)
- Documents can be subject to legal requests and subpoenas
- Google scans content for security threats and policy violations
- Documents are vulnerable if Google's systems are compromised

For truly sensitive materials (legal strategy, whistleblower information, highly confidential donor data), use end-to-end encrypted platforms like Tresorit instead of Google Docs.

When NOT to Use Google Docs

Switch to more secure alternatives when:

- Documents contain personally identifiable information (PII) at scale
- Legal or financial information that could be subpoenaed
- Information about vulnerable individuals
- Strategic plans you cannot afford to have leaked
- Partnership with organizations requiring higher security standards

Secure Alternatives:

- **Tresorit:** End-to-end encrypted storage (Swiss-based, zero-knowledge)

- **Cryptpad:** Encrypted collaborative documents (less user-friendly)

Red Flags: Signs of Compromised Documents

Watch for:

- Unexpected editors added to documents
- Unfamiliar names in version history
- Documents you don't recognize in your "Shared with me" folder
- Notifications of sharing activity you didn't initiate

If you suspect compromise:

1. Immediately revoke all sharing
2. Change your Google account password
3. Enable 2-factor authentication if not already active
4. Review recent account activity (myaccount.google.com/security)
5. Contact K'lal or your IT support for incident response guidance

Best Practices for Preventing Unauthorized Document Capture and Access

The Reality

Unfortunately, there's no foolproof technical solution to prevent screenshots. If someone can view a document on their screen, they can potentially capture it through:

- Screenshots
- Phone cameras
- Screen recording software

Practical Limitations

Prevention Through Access Control Rather than trying to block screenshots, focus on:

1. **Minimize Exposure**: Don't share sensitive documents digitally unless absolutely necessary
2. **Control Who Has Access**: Use role-based permissions (Managers, Editors, Viewers)
3. **Create Audit Trails**: Enable access logs so you know who viewed what and when
4. **Use Secure Platforms**: Store highly sensitive documents in end-to-end encrypted services like Tresorit rather than general cloud drives
5. **Implement Data Classification**: Classify documents by sensitivity level and apply appropriate security measures

Detection Over Prevention Since you can't fully prevent screenshots, focus on detection:

- Watermark documents with recipient-specific identifiers
- Maintain detailed access logs
- Use platforms that track viewer IP addresses and email verification
- Create clear policies about acceptable use

Technical Controls

Document Watermarking

- Add watermarks to sensitive documents for leak detection
- Tresorit offers watermarking features for shared videos and documents to prevent unauthorized re-sharing

Access Controls & Monitoring

- Use platforms like Tresorit that provide access logs to track who viewed documents
- Enable download tracking to monitor document access
- Implement time-limited access with expiration dates on shared links
- Use download limits (e.g., 5-10 opens) for highly sensitive documents

Secure Document Sharing & Retention Framework

This framework provides actionable guidance for managing document sharing, permissions, and offboarding in Google Workspace and Microsoft 365 environments.

Part 1: Core Principles

Least Privilege Access

Give users the minimum permissions needed to do their work. Default to restrictive permissions and grant additional access only when justified.

Regular Permission Audits

Access requirements change as projects evolve and staff transitions occur. Quarterly reviews prevent permission creep and orphaned access.

Clear Ownership

Every shared resource needs a designated owner responsible for managing access and ensuring appropriate use.

Data Classification

Not all information requires the same protection. Classify data by sensitivity (Low, Medium, High) to apply appropriate controls.

Retention by Purpose

Keep data only as long as it serves organizational needs or legal requirements. Unnecessary data creates liability.

Part 2: Data Classification Framework

Public Information

Definition: Already published or intended for public consumption
Examples: Press releases, published reports, public event information
Sharing: Can be shared widely with "anyone with the link"
Storage: Standard organizational drives
Retention: Permanent archive appropriate

Internal Information

Definition: Not sensitive but intended only for organizational use
Examples: General staff communications, non-confidential meeting notes, internal newsletters
Sharing: Organization-only; no external sharing
Storage: Organizational shared drives
Retention: 3-7 years typical

Confidential Information

Definition: Sensitive information requiring protection
Examples: Strategic plans, donor information, financial records, personnel files, legal documents
Sharing: Named individuals only; explicit approval for external sharing
Storage: Restricted folders with audit logging
Retention: Varies by type; often 7+ years

Highly Sensitive Information

Definition: Information that could cause significant harm if disclosed
Examples: Legal strategy, sensitive external communications, information about vulnerable individuals
Sharing: Extremely limited; requires executive approval for any sharing
Storage: Encrypted cloud storage (Tresorit) or encrypted local storage
Retention: Minimum necessary; destroy when no longer required

---

Part 3: Permission Management

Google Workspace Permission Levels

Viewer

- Can view and download files
- Cannot edit or share
- **Use for:** External partners needing read-only access, staff viewing reference materials

Commenter

- Can view and add comments
- Cannot edit content directly
- **Use for:** Review processes, feedback collection without editing rights

Editor

- Can edit content and share with others
- Cannot change ownership
- **Use for:** Active collaborators on shared documents

Owner (Google-specific)

- Full control including deletion and ownership transfer
- Only role that can permanently delete from shared drives
- **Use for:** Primary document steward

Microsoft 365 Permission Levels

Read

- Can view and download
- Cannot edit or share
- **Use for:** Reference materials, read-only external access

Edit

- Can modify content
- May or may not be able to share (configurable)
- **Use for:** Active collaborators

Full Control (SharePoint)

- Complete administrative control
- Can change permissions and settings
- **Use for:** Site administrators only

Permission Best Practices

Default to "Specific People" Never use "anyone with the link" for anything beyond public information. Even for internal documents, explicitly name users or groups.

Consider Using Groups, Not Individual Accounts Create groups for recurring access needs:

- Communications Team
- Finance Staff
- Board Members
- Program Directors

This simplifies management when people join or leave roles.

Time-Limited Access for External Collaborators When granting access to external partners:

- Set expiration dates where possible
- Use "commenter" or "viewer" rather than "editor" unless editing is essential
- Document why access was granted
- Review after 90 days

Avoid Editor Rights to External Parties External collaborators should rarely need editing rights. Use comment access and have internal staff make approved changes.

Regular Permission Audits Quarterly, review:

- Who has access to confidential folders
- External shares across the organization
- Shared drives with "anyone with the link" settings
- Users with ownership rights

Part 4: Sharing Workflows

Internal Sharing (Google Workspace)

For Individual Documents:

1. Open sharing settings
2. Select "Restricted" (not "Anyone with the link")
3. Add specific people or groups
4. Choose appropriate permission level
5. Uncheck "Notify people" if you'll inform them separately
6. Document the share in your records if sharing confidential information

For Shared Drives:

1. Use Shared Drives (not "My Drive") for team collaboration
2. Assign team members to the Shared Drive with appropriate roles
3. Set default permissions at the drive level
4. Individual files inherit drive permissions unless specifically overridden

For Folders:

1. Share the folder, not individual files when possible
2. Use consistent permission structure
3. Name folders clearly to indicate sensitivity level
4. Include a README file explaining the folder's purpose and access requirements

Internal Sharing (Microsoft 365)

For SharePoint Sites:

1. Use SharePoint sites for department/project collaboration
2. Assign users to appropriate SharePoint groups (Members, Visitors, Owners)
3. Site-level permissions cascade to libraries and files
4. Use sensitivity labels to enforce encryption on confidential content

For OneDrive:

1. Use OneDrive for personal working files, not organizational documents
2. Move files to SharePoint when they need team access
3. Avoid long-term storage of organizational content in personal OneDrive

For Teams:

1. Each Team has an underlying SharePoint site
2. Files shared in Teams channels are stored in SharePoint
3. Team owners manage member access
4. External guest access requires explicit enablement

External Sharing

Risk Assessment First Before sharing anything externally:

- What information does this contain?
- What's the minimum access level needed?
- How long should access last?
- Who would benefit from gaining access to this information?

Google Workspace External Sharing:

1. Prefer "Commenter" or "Viewer" access
2. Monitor access through activity logs
3. Revoke access when collaboration ends

Microsoft 365 External Sharing:

1. Use sensitivity labels to control what can be shared externally
2. Require expiration for guest access
3. Use "Anyone" links only for truly public information
4. Set organizational policies blocking external sharing of confidential content

Alternative: Secure Sharing Platforms For highly sensitive materials, consider:

- Tresorit Send for encrypted file transfer
- Tresorit to host and share documents
- Password-protected, time-limited links
- Watermarked documents for leak detection

Part 5: Offboarding Procedures

30 Days Before Departure (If Possible)

Document Ownership Transfer

- Identify all documents owned by departing staff
- Determine new owners for each document/folder
- Transfer ownership to permanent employees, not other departing staff
- Create a spreadsheet to document the transfers

Knowledge Transfer

- Create list of key files and their locations
- Document any unique sharing arrangements
- Identify external parties with whom staff member shared documents

Day of Departure

Immediate Actions:

Google Workspace:

1. Transfer ownership of critical documents immediately

2. Remove from all organizational groups
3. Convert account to suspended (not deleted yet)
4. Review and revoke external shares made by user
5. Set email forwarding to appropriate staff member (if approved)
6. Document the account status

Microsoft 365:

1. Transfer ownership of critical SharePoint content
2. Remove from all Microsoft 365 groups and Teams
3. Revoke active sessions
4. Block user sign-in (don't delete yet)
5. Set email forwarding (if approved)
6. Convert mailbox to shared mailbox if retention needed
7. Document account status