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
