Druk Green Power Corporation Limited

SOP: Google Workspace Shared Drive Usage

Document Version: 1.0
Effective Date: May 2026
Owner: Information Technology Section

1. Purpose

This SOP establishes standardized procedures for the creation, utilization, and management of Google Workspace Shared Drives to ensure secure, compliant, and efficient collaboration across the organization. Within Shared Drives, ownership of files resides with the organization rather than individual users. Consequently, in the event of an employee's departure and subsequent account deletion by an administrator, all files created or added by the user within Shared Drives remain intact and accessible.

This SOP is aligned with corporate information security requirements and cybersecurity best practices, ensuring the protection of organizational data against unauthorized access, misuse, and potential leakage of sensitive information. Furthermore, it supports the organization's transition toward a paperless working environment by minimizing reliance on physical documentation, printing, and storage infrastructure, thereby enhancing operational efficiency and promoting environmentally sustainable practices.

2. Scope

Applies to all the employees throughout the formation of DGPC. It covers:

- Creation and naming of Shared Drives
- Access management and permissions
- File storage, sharing, and retention
- Security, monitoring, and compliance
- Incident reporting

2.1. Key Principle

- All documents stored on Google Workspace Shared Drives must be shared via document links internally.
- Sending documents as email attachments is strictly prohibited except for third parties.
- This practice ensures everyone accesses the same document repository.
- Eliminates digital waste caused by duplicate files.
- Reduces the risk of unauthorized distribution or leakage.

3. DATA or Information Classification

To promote proper control for safeguarding the confidentiality, integrity and availability of the information available in DGPC's Centralized DMS repository. The classifications assigned are dependent on the sensitivity of information. The following are levels to be classified in Druk Green.

3.1. Confidential Information:

- Confidential information is very important and highly sensitive material. This information is private or otherwise sensitive corporate information and must be restricted to those with a legitimate business need for access. Examples include personnel HR, Board related matters and financial information in the ERP, key financial and contractual information, proprietary information of commercial research, system access passwords and information file encryption keys.

- Unauthorized disclosure of confidential information must require official clearance from the information owner with the approval from DGPC management.

3.2. Internal Information:

- Internal information is intended for unrestricted usage within Druk Green and in some cases within affiliated DHI companies, BEA and RGOB. This information could be distributed

without advance permission from Information Owners. Examples include: contact and directories, internal policies and procedures and most internal emails.

- Any information not under confidential information will fall under this category by default.
- Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

3.3. Public Information:

- Public information has been specifically approved for public release by a designated authority within Druk Green. Examples are marketing brochures, reports, and other materials on the Druk Green internet website.

4. Roles & Responsibilities

Permission	Manager	Content Manager	Contributor	Commenter	Viewer
View files	Yes	Yes	Yes	Yes	Yes
Comment on files	Yes	Yes	Yes	Yes	No
Edit files	Yes	Yes	Yes	No	No
Add/Create files	Yes	Yes	Yes	No	No
Delete files	Yes	No*	No	No	No
Move files to trash	Yes	Yes	No	No	No
Add/Remove Members	Yes	No	No	No	No

Note: Content Managers can move files to the trash, but they cannot permanently delete them or delete the entire shared drive.

5. Shared Drive Creation & Structure

5.1. Creation

- Only authorized personnel (IT or designated functional focal points) shall be permitted to create Shared Drive folders. The designated focal for each function shall be assigned the Content Manager role and will be responsible for sharing folders within their respective teams, assigning access roles based on business requirements. The functional focal shall be accountable for managing user access permissions within their function and overseeing the overall maintenance and governance of the Document Management System (DMS).
- Use standardized naming conventions for organizing documents:
  Level 1: Departments/Governance
  Level 2: Divisions
  Level 3: Sections

Level 4: Units
Example: DGPC_FID/FAD/01_Accounts_Section/2026/

- Avoid personal names or ambiguous titles.

5.2. Structure & Organization

- Organize folders logically inside respective Department/Division/Section/Unit:
  - 01_Administrative
  - 02_Financial
  - 03_Reports
- Include a README document explaining folder structure, content type, and retention.
- Avoid excessive folder nesting (max 4 levels deep) for clarity.

6. Access & Permissions

6.1. Role Definitions

Role	Permissions	Best Practice
Manager	Full access to add/edit/delete files, manage members	Assign only to department/project leads
Contributor	Can add/edit files but cannot delete drive	Standard operational role
Commenter	Can view and comment, not edit	For external reviewers or auditors
Viewer	Read-only access	For general awareness or compliance monitoring

6.2. Assignment

- Apply the least privilege principle: only assign the minimum required permissions.
- Avoid giving Manager access to temporary staff or external users unless strictly necessary.
- Conduct access reviews every 3 months or when team changes occur.

6.3. Sharing

- Do not use "Anyone with the link" sharing unless approved by the competent authority.
- Never share sensitive corporate information to external parties and if need be, legal clearance be sought before sharing. In such a case, sharing must use Google Workspace controls with expiration dates.

7. File Management & Collaboration

Only final signed copies of documents, which are currently maintained offline for record-keeping purposes, shall be uploaded to the shared drive.

7.1. File Naming

- Use standardized, descriptive names:
  ProjectName_FileDescription
  Example: RISEwithSAP_CostBreakdown
- Avoid spaces, special characters, or personal identifiers.

7.2. Version Control

- Maintain document versions; enable **Google Docs/Sheets/Slides version history**.
- Avoid overwriting critical files; use _v1, _v2 suffixes.

7.3. Retention & Deletion

- Follow corporate document retention policies.
- Archive or delete obsolete files after verification and backup.

8. Security & Compliance

8.1. Data Protection

- Enable 2-Step Verification for all users.
- Do not download files to personal devices unless genuinely required.
- Google Workspace provides encryption in transit and at rest.

8.2. Prohibited Content

- Classified and confidential data (sensitive corporate documents) must not be stored in Shared Drives.
- Sensitive information may only reside in secure storage.

8.3. Monitoring & Auditing

- IT shall monitor Shared Drives via Admin Console.
- File Managers report suspicious activity immediately.
- Conduct quarterly audits of permissions, folder structures, and external sharing.

8.4. Incident Handling

- Report any suspected data breach or unauthorized access to the IT Section immediately.
- Temporarily suspend access to compromised drives until investigation is complete.

9. Review & Updates

- Review annually or when Google Workspace features or corporate policies change.
- Changes require approval from the IT Section.