SOP: Centralized Document Storage and Access Protocols

This SOP details the **centralized document storage and access protocols**, including standardized document organization, secure storage solutions, controlled access permissions, version control, backup procedures, and audit trails. The goal is to ensure efficient document management, enhance data security, enable quick retrieval, and maintain accountability across all departments by implementing consistent and transparent storage and access practices.

1. Purpose

To establish uniform procedures for document storage and access that safeguard data, streamline document retrieval, and support organizational accountability.

2. Scope

This SOP applies to all departments and staff responsible for the creation, storage, management, and retrieval of organizational documents within the centralized storage system.

3. Responsibilities

- **IT Department:** Maintain centralized storage infrastructure, manage user access, perform backups, and monitor system integrity.
- **Department Managers:** Ensure staff compliance with this SOP and report issues to IT.
- **All Staff:** Follow storage and access protocols, maintain document integrity, and report security concerns.

4. Protocols and Procedures

1. **Centralized Storage Solution**
   - All documents must be stored in the designated centralized storage platform (e.g., SharePoint, Google Drive, or internal server).
   - Use only approved and secured organizational document repositories.
2. **Standardized Document Organization**
   - Documents must be organized in a predefined folder hierarchy by department, project, and document type.
   - File naming conventions must be standardized (e.g., YYYY-MM-DD_Department_Title_Version).
   - A directory listing and organization schema must be maintained and updated as necessary.
3. **Controlled Access Permissions**
   - Access to folders and documents is restricted by role and need-to-know basis.
   - User and group access rights must be reviewed quarterly by IT and department managers.
   - All access requests or changes must be documented and authorized.
4. **Version Control**
   - All edits and document versions must be tracked using built-in versioning tools or naming conventions.
   - Obsolete versions may be archived as per retention policy but must not be deleted immediately.
5. **Backup Procedures**
   - Full backups of the storage system must be performed at least weekly; incremental backups daily.
   - Backup logs must be maintained and periodically tested for data restoration integrity.
6. **Audit Trails**
   - All access and modifications must be logged, including user ID, timestamp, and action performed.
   - The IT department will review audit logs monthly and investigate anomalies promptly.

5. Compliance & Monitoring

- Periodic audits will be conducted to ensure adherence to protocols.
- Violations may result in corrective actions and/or revocation of access privileges.
- Staff will receive ongoing training on storage and access protocols as part of organizational security awareness programs.

6. Revision and Review

- This SOP is to be reviewed annually or upon significant changes to storage infrastructure or regulations.

- All updates must be documented and communicated to all relevant personnel.

7. References

- IT Security Policy
- Data Retention Policy
- Access Control Procedures

Document Control

Version	Date	Author	Description of Change
1.0	2024-06-18	[Author Name]	Initial SOP Release