SOP Template: Protocols for Document Access Permissions and User Roles

This SOP defines the **protocols for document access permissions and user roles**, ensuring secure and organized management of digital documents. It outlines the classification of user roles, assignment of access levels, procedures for requesting and granting permissions, monitoring and auditing access, and protocols for revoking or updating permissions. The objective is to maintain confidentiality, integrity, and availability of documents by controlling access according to organizational policies and user responsibilities.

1. Purpose

To establish standardized protocols for the assignment, monitoring, updating, and revocation of document access permissions and user roles.

2. Scope

This SOP applies to all employees, contractors, and third-party users who access the organization's digital documents and document management systems.

3. Definitions

- **User Roles:** Categories assigned to users based on their job responsibilities (e.g., Administrator, Editor, Viewer).
- **Access Permission:** The rights assigned to a user role, defining what actions can be performed (e.g., view, edit, delete).
- **Document Owner:** The individual or team responsible for a specific document's management and access control.

4. User Roles and Access Levels

User Role	Access Level	Description
Administrator	Full Access	Can create, view, edit, delete, and assign permissions for all documents.
Editor	Modify Access	Can view, create, and edit documents, but cannot manage permissions or delete documents.
Viewer	Read Only	Can view documents but cannot create, edit, or delete them.
Guest	Limited Access	Access to specific documents on a temporary or restricted basis.

5. Assignment of User Roles

- User roles are assigned by the System Administrator based on job function and data access requirements.
- Access is granted according to the principle of least privilege.
- All assignments must be documented and approved by the Department Head or Document Owner.

6. Requesting and Granting Permissions

1. **Request Submission:** Users submit access requests via an approved access request form or ticketing system.
2. **Review & Approval:** Requests are reviewed by Document Owner and approved by the Department Head or System Administrator.
3. **Assignment:** Upon approval, permissions are assigned and documented.
4. **Notification:** User is notified of granted permissions and effective period.

7. Monitoring and Auditing

- Regular audits are conducted to review user access and compare with user roles.
- All access logs are maintained and reviewed quarterly to detect unauthorized or inappropriate access.
- Incidents of unauthorized access are investigated and remedial action is taken.

8. Updating and Revoking Permissions

- User permissions are updated promptly upon role change, department transfer, or change in job responsibilities.
- Access is revoked immediately upon termination of employment or contract.
- Document Owners and System Administrators are responsible for reviewing user access on a bi-annual basis.

9. Roles and Responsibilities

- **System Administrator:** Manages overall access and ensures compliance with SOP.
- **Document Owner:** Oversees document-specific permissions and approves access requests.
- **End Users:** Use and protect their assigned credentials, follow policies, and report access issues.
- **Department Head:** Approves high-level permissions and resolves access conflicts.

10. References

- Information Security Policy
- Data Classification Guidelines
- IT Acceptable Use Policy

11. Revision History

Date	Version	Description of Change	Author	Approved By
2024-06-01	1.0	Initial SOP Release	Jane Doe	IT Manager