Standard Operating Procedure (SOP)

Role-based Permission and Access Control Management

This SOP defines the processes for **role-based permission and access control management**, detailing how user roles are assigned, permissions are granted, and access to systems and data is controlled. It includes procedures for defining roles, setting access levels, monitoring user activities, and regularly reviewing and updating permissions to ensure security and compliance. The objective is to protect sensitive information and maintain system integrity by implementing structured and auditable access controls based on user responsibilities.

1. Purpose

To establish a robust and auditable process for assigning, managing, and reviewing role-based access controls (RBAC) that protect sensitive systems and data.

2. Scope

This SOP applies to all users, administrators, and information systems within the organization that are subject to access controls.

3. Definitions

- **Role:** A predefined set of permissions associated with job functions.
- **Permission:** Authorization to perform specific operations on systems or data.
- **Access Control:** Mechanism to grant or restrict user access to resources based on role.
- **RBAC:** Role-Based Access Control; a method for restricting system access based on user roles.

4. Responsibilities

Role	Responsibility
System Owner	Defines and approves roles, reviews permissions, enforces compliance.
IT Administrator	Implements, modifies, and revokes permissions; monitors access logs.
Managers	Requests access for team members and validates necessity.
Users	Follows access protocols and maintains credential security.

5. Procedure

1. **Role Definition and Updates**
    - System Owners define roles based on job functions and minimum necessary access.
    - Roles are documented with associated permissions, description, and owner.
    - Roles are reviewed and updated at least annually or as organizational changes occur.
2. **User Access Request and Approval**
    - Managers submit access requests via the designated system or form, specifying required role(s).
    - System Owner or delegated authority reviews and approves/rejects requests based on necessity.
    - All approvals are logged and tracked for audit purposes.
3. **Role Assignment and Permission Granting**
    - IT Administrator assigns the approved role to the user and grants associated permissions.
    - User is informed of granted access and relevant security policies.
4. **Access Modification and Revocation**
    - Managers notify IT of users changing roles or leaving the organization.

    - IT promptly revokes or modifies access based on updated information.
    - Revocations and modifications are logged for auditing.
5. **Monitoring and Review**
    - Access logs are monitored regularly for unauthorized activities.
    - Quarterly reviews are conducted to ensure user access aligns with current roles and responsibilities.
    - Access exceptions or anomalies are investigated and resolved promptly.
6. **Audit and Compliance**
    - All access control changes and reviews are recorded for compliance and audit purposes.
    - Periodic audits are conducted to verify compliance with this SOP and applicable regulations.

6. Documentation and Record Keeping

- Maintain documentation of all access requests, approvals, revocations, and reviews.
- Access logs are retained according to the organization's data retention policy.

7. Review and Revision

- This SOP shall be reviewed annually or as needed to reflect changes in organizational structure, technology, or compliance requirements.
- Revisions are subject to approval by the System Owner.

8. References

- Company Information Security Policy
- Relevant compliance frameworks (e.g., ISO 27001, HIPAA, GDPR)