Standard Operating Procedure (SOP)

User Access Control and Authorization Protocols

This SOP defines **user access control and authorization protocols**, including user identification and authentication processes, role-based access management, permission assignment and review, multi-factor authentication implementation, access monitoring and logging, password policies and management, and procedures for access revocation and privilege escalation prevention. The objective is to secure system resources by ensuring only authorized users gain appropriate access according to their roles and responsibilities, thereby protecting sensitive data and maintaining compliance with security policies.

1. Scope

This SOP applies to all personnel, contractors, and third-party users accessing organizational systems and sensitive data.

2. Responsibilities

Role	Responsibilities
System Administrators	Configure, grant, revoke access; monitor compliance.
Managers	Approve access requests; initiate access reviews.
Users	Comply with access and password policies.
IT Security	Oversee access control mechanisms, perform audits.

3. User Identification & Authentication

- Each user is assigned a unique user ID.
- Authentication requires passwords adhering to policy (see Section 7) and may include multi-factor authentication (MFA).
- Default accounts must be disabled or assigned strong credentials.

4. Role-Based Access Management

- Roles are defined according to job functions and responsibilities.
- Access rights are assigned strictly by role and business necessity (principle of least privilege).
- Segregation of duties is enforced to prevent unauthorized activity.

5. Permission Assignment & Review

- Access requests are documented and require managerial approval.
- Permission changes (granting, altering, revoking) are logged.
- Periodic reviews (at least quarterly) are conducted to validate permissions.

6. Multi-Factor Authentication (MFA)

- MFA is enabled for all systems containing sensitive or critical data.
- Accepted factors: password plus hardware token, app-generated code, or biometric.
- MFA enrollment, recovery, and usage are documented and monitored.

7. Password Policies and Management

- Minimum password length: 12 characters (unless system limitations apply).
- Password complexity: mix of uppercase, lowercase, numbers, and symbols.
- Password changes: mandatory every 90 days or upon suspicion of compromise.

- Password history: last 5 passwords cannot be reused.
- Password storage: store only in approved encrypted password vaults.

8. Access Monitoring and Logging

- All access attempts (successful and failed) are logged with user, timestamp, and activity details.
- Critical system logs are monitored daily; anomalies are escalated to IT Security.
- Logs are retained for at least 1 year in accordance with compliance requirements.

9. Access Revocation & Privilege Escalation Prevention

- Immediate revocation of access for terminated users or those transferred from their role.
- Privilege escalation requests are carefully reviewed and require dual approval.
- Periodic audits ensure no unauthorized or orphaned accounts exist.

10. Exceptions

Any exceptions to this SOP require formal approval from the IT Security team and must be documented, including risk assessment and mitigation plan.

11. Review and Revision

This SOP shall be reviewed annually or upon any significant system or regulatory change. Revisions must be documented in the version history below.

12. Version History

Date	Version	Description	Editor
2024-06-20	1.0	Initial creation	Your Name