SOP: Unique User Login and Access Control Protocols

This SOP defines **unique user login and access control protocols** to enhance system security by ensuring that each user has a distinct login credential. It includes procedures for user authentication, password policies, role-based access controls, session management, and monitoring to prevent unauthorized access and protect sensitive information. The objective is to maintain the integrity and confidentiality of system resources through stringent access management practices.

1. Purpose

To establish a standardized protocol for user authentication, access control, and monitoring to safeguard system resources and sensitive information.

2. Scope

This SOP applies to all users, administrators, and systems that require access to the organization's digital resources.

3. Definitions

Term	Definition
Unique User Login	Individualized user credentials that identify and authenticate a single user.
Authentication	The process of verifying the identity of a user.
Role-Based Access Control (RBAC)	Authorization model assigning permissions based on user roles.
Session Management	Controls the creation, maintenance, and termination of user sessions.

4. Responsibilities

- **System Administrators:** Implement and oversee user login and access controls.
- **Users:** Maintain the confidentiality and security of their credentials.
- **IT Security Team:** Monitor access, audit compliance, and respond to security incidents.

5. Procedures

1. **User Account Creation**
   - Each user is assigned a unique username and a temporary password upon account creation.
   - User identity must be verified before account issuance.
2. **User Authentication**
   - Users must authenticate using their unique credentials.
   - Multi-factor authentication is mandatory for all privileged accounts.
3. **Password Policy**
   - Minimum length of 12 characters; must include uppercase, lowercase, number, and symbol.
   - Passwords must be changed every 90 days.
   - Account lockout enabled after 5 failed login attempts.
4. **Role-Based Access Control (RBAC)**
   - Assign permissions based on job function and least privilege principle.
   - Access rights reviewed and updated quarterly or upon role change.
5. **Session Management**
   - Automatic session timeout after 15 minutes of inactivity.
   - Immediate termination of sessions upon logout or account deactivation.
6. **Monitoring and Auditing**
   - All login attempts and access to sensitive data are logged.

    - Security logs reviewed at least monthly for unauthorized access attempts.

7. **Deactivation and Revocation**
    - User accounts are disabled immediately upon termination of employment or contract.
    - Periodic review of active accounts for validity.

6. Compliance and Exceptions

- The procedures above must be followed as stated. Any exceptions must be documented and approved by IT Security.

7. Revision History

Version	Date	Description	Author
1.0	2024-06-01	Initial SOP release	IT Security