

Petrozone Pulse - User Authentication Specification

1. Purpose

This document delineates the authentication mechanisms, credential management processes, access control policies, and recovery procedures for the Petrozone Pulse system. It ensures that internal users can only access the data and functions that are in line with their roles.

2. Authentication Mechanisms

2.1 Login Method

- Authentication Type: Username + Password (no MFA)
- Session Management: Token-based sessions
- Web-hosted access enforced via HTTPS

3. Credential Management Processes

3.1 Account Creation

- Account creation is performed only by Developer, Higher Management, POC Supervisor, or Junior Supervisor.
- Role assignment: Defined by Developer, Higher Management, POC Supervisor, or Junior Supervisor during creation
- Temporary password issued: Yes, has to be changed at first login

3.2 Password Policy

- Minimum length: 8 characters
- Character requirements: Uppercase + Lowercase + Number
- Password expiration policy: None
- Password reuse restriction: None

3.3 Credential Storage

- Passwords stored using secure hashing (bcrypt/Argon2 recommended)
- Plaintext password storage is prohibited
- All login and password transmissions occur over HTTPS

3.4 Account Lockout

- Maximum failed login attempts: 5
- Lockout duration: 15 minutes
- Manual unlock: Developer, Higher Management, POC Supervisor, or Junior Supervisor can unlock
- Failed login attempts are logged in the audit trail

4. Authorization & Permission Model

- Role-Based Access Control (RBAC) is implemented as per FR-2 & NFR-05
- Access to functions and data is limited according to internal role definitions
- Existing role permissions matrix governs access
- Principle of Least Privilege enforced: Users access only what is necessary for their role

5. Account Recovery Procedures

5.1 Password Change

- All authenticated users may change their own password from their profile settings
- Current password must be entered before changing
- New password must follow defined password policy
- Password change events are logged in the audit trail

5.2 Password Reset Process

- If a user forgets their password or account is locked, reset is handled by Developer, Higher Management, POC Supervisor, or Junior Supervisor.
- Temporary password issued; must be changed upon next login
- All reset events are logged in audit trail

5.3 Account Recovery

- Identity verification handled by Developer, Higher Management, POC Supervisor, or Junior Supervisor
- Manual override available for locked accounts

6. Audit Logging & Monitoring

- Login attempts logged: Yes
- Failed login attempts logged: Yes

- Log retention: Retention according to internal policy

7. Developer Responsibilities

- Implement secure password hashing (bcrypt / Argon2)
- Enforce backend password validation and account lockout
- Apply role-based middleware
- Enforce HTTPS for all authentication and data transmission
- Implement secure token/session handling
- Maintain audit logs for login, reset, and administrative actions
- Perform security testing

8. User Roles & Permissions

- Refer to:  [5BYTE x SPM] Sprint Masterfile for roles and permissions matrix