Standard Operating Procedure (SOP)

User Authentication and Request Validation

This SOP details the process of **user authentication and request validation**, covering user identity verification, credential management, session handling, multi-factor authentication implementation, request data validation, input sanitization, error handling, access control enforcement, and logging of authentication events. The goal is to ensure that every user and request is properly authenticated and validated to maintain the security and integrity of the system.

1. User Authentication

1. **User Identity Verification:**
   - Require unique user identifiers (username or email) for login.
   - Verify user existence in the database before proceeding to password check.
2. **Credential Management:**
   - Store passwords using strong one-way cryptographic hashing (e.g., bcrypt, Argon2).
   - Enforce password complexity and rotation policies as needed.
3. **Multi-Factor Authentication (MFA):**
   - Implement MFA for privileged or sensitive accounts, requiring an additional verification factor (e.g., SMS, authenticator app, email OTP).
   - Prompt users for the second factor upon successful primary credential verification.
4. **Session Handling:**
   - Create a new secure session or token upon successful authentication.
   - Ensure session tokens are protected with HTTPOnly, Secure, and SameSite cookie attributes where applicable.
   - Expire sessions after a period of inactivity or upon logout.

2. Request Validation

1. **Request Data Validation:**
   - Validate all incoming request data (query, body, headers, params) using server-side rules.
   - Reject requests with missing, malformed, or unexpected input data.
2. **Input Sanitization:**
   - Sanitize input to mitigate injection attacks (e.g., SQL, XSS).
   - Escape special characters and filter out dangerous content before processing.

3. Error Handling and Access Control

1. **Error Handling:**
   - Return generic error messages to the user to avoid disclosing sensitive system details.
   - Log detailed error information securely on the server for auditing and debugging.
2. **Access Control Enforcement:**
   - Check user roles and permissions before granting access to protected resources or operations.
   - Deny unauthorized access attempts and log such events.

4. Logging and Monitoring

1. **Authentication Event Logging:**
   - Log all authentication attempts, both successful and failed, with timestamps and user identifiers.
   - Implement alerts for repeated failed authentication attempts to detect potential attacks.
2. **Regular Review:**
   - Regularly review authentication logs and access control changes for anomalies.

5. Revision and Approval

1. Review this SOP annually or upon significant system changes.
2. Document changes and obtain necessary approvals from the information security and IT management teams.