

***Specification for Initial Registration and Authentication in an Investment Management System Report***

***1. Purpose***

*This document aims to establish a comprehensive framework for the registration and authentication processes within the investment management system. This policy outlines the procedures, security measures, and best practices that must be followed to protect user accounts and safeguard sensitive transactions. The system aims to provide all users with a secure and user-friendly experience by implementing these guidelines.*

***2. Scope***

*This document applies to all user registration and authentication aspects within the investment management system. It encompasses the initial user registration process, user login procedures, and reauthentication requirements for sensitive transactions. Additionally, it outlines security measures to prevent unauthorized access, fraud, and confirmation methods during registration and transaction processes. The scope covers technical and procedural aspects, ensuring all components function together to create a secure user environment.*

***3. Overview***

*Registration and authentication are the foundation of user security in any online system. They serve as the first line of defense against unauthorized access and play a critical role in maintaining the integrity and confidentiality of user data and transactions.* *Robust registration and authentication mechanisms are vital in an investment management system where users handle sensitive financial information and transactions. These processes protect the users and help build trust in the system by ensuring that all actions taken within the platform are secure and verified. A well-designed registration and authentication process can prevent unauthorized access, fraud, and other security breaches, making it essential for the system’s overall security strategy.*

***4. Key Use Cases for Registration and Authentication***

*Registration and authentication are foundational processes in securing an investment management system, as they define how users gain access and interact with the platform. By implementing a structured approach to these processes, we can ensure that only legitimate users are granted access while maintaining a seamless and secure experience. This section outlines the critical use cases, from initial registration to reauthentication for sensitive transactions, detailing the essential steps and security measures required at each stage to protect user accounts and sensitive financial data.*

***4.1 Initial User Registration***

***Description:*** *This use case emphasizes secure onboarding by requiring users to submit valid personal information, verify identity, and create strong credentials. The goal is to ensure that only legitimate users can create accounts.*

***User Requirements:***

1. ***Personal Information Submission:*** *Users must provide accurate personal data (full name, email, phone number, etc.).*
2. ***Password Creation:*** *A strong password must adhere to security guidelines (e.g., length, memorable characters, and no dictionary words).*
3. ***Email and Phone Verification:*** *Users verify their email and phone by entering confirmation codes sent to these channels.*
4. ***Document Upload:*** *Users must upload identity verification documents, such as government-issued ID, to meet Know Your Customer (KYC) requirements. The system will authenticate the documents.*

***4.2 Logging into the System***

***Description:*** *The login process ensures only authorized users can access their accounts by requiring correct credentials and multi-factor authentication (MFA).*

***User Requirements:***

1. ***Username and Password Entry:*** *Users enter their registered email (as the username) and password.*
2. ***MFA Completion:*** *To strengthen security, users receive a one-time passcode (OTP) via SMS or an authenticator app, which they must enter to complete the login.*

***4.3 Reauthenticating for Sensitive Transactions***

***Description:*** *Sensitive transactions, such as transfers or account setting changes, require users to reauthenticate to prevent unauthorized actions.*

***User Requirements:***

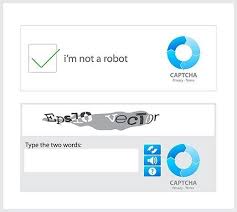
1. ***Password/Biometric Reauthentication:*** *Users must re-enter their password or use biometric verification (e.g., fingerprint or facial recognition).*
2. ***Secondary Confirmation:*** *An OTP or a security question will be required to finalize sensitive actions.*

***4.4 Performing Sensitive Transactions***

***Description:*** *This use case ensures users thoroughly review and authenticate high-risk transactions such as fund transfers.*

***User Requirements:***

1. ***Review Transaction Details:*** *Users must carefully review transaction details (e.g., recipient and amount).*
2. ***CAPTCHA:*** *Users confirm their identity through a CAPTCHA.*



1. ***MFA Confirmation:*** *Another OTP or form of MFA must be entered before proceeding.*
2. ***Final Transaction Review and Confirmation:*** *Users can confirm the details before the transaction is finalized.*

***4.5 Investor Onboarding***

***New Investor Registration:***

*Description: Prospective investors must complete a registration process that includes providing personal information, verifying their accounts, and uploading required documents to comply with KYC regulations.*

***User Requirements:***

1. *Provide Personal Information: During registration, prospective investors enter personal information, including investment goals and risk tolerance.*
2. *System Validation: The system validates the provided information and sends a confirmation email or SMS for account verification.*
3. *Document Upload: The investor uploads required documents (e.g., proof of identity, address, and income) to comply with KYC (Know Your Customer) regulations.*
4. *Document Verification: The system verifies the authenticity and completeness of the uploaded documents.*
5. *Registration Confirmation: The system confirms investor registration once all criteria are met.*

***4.6 Employee Access***

***Description:*** *Employees within the investment firm must log in and perform their tasks based on their roles and permissions.*

***User Requirements:***

1. ***Employee Login:*** *Employees must log in using their credentials (username and password).*
2. ***Role-Based Access:*** *The system grants access to relevant applications and data based on the employee’s role and permissions.*
3. ***Task Execution:*** *Employees can process account changes, generate reports, and manage client communications.*
4. ***Compliance Monitoring:*** *Compliance employees can monitor system activities to ensure adherence to regulatory requirements and internal policies.*

***4.7 Third-Party Integration***

***Description:*** *The system integrates with external platforms, ensuring data synchronization and secure data exchange.*

***User Requirements:***

1. ***API Integration:*** *The system must integrate with external platforms (e.g., trading systems, CRM tools) using secure APIs.*
2. ***Authentication Protocols:*** *Secure authentication protocols, such as OAuth and OpenID Connect, must be used to protect data exchange.*

*A black and white sign with a arrow pointing to the right

Description automatically generated*

1. ***Data Synchronization:*** *Data must be synchronized between the investment management and external systems to maintain consistency and accuracy.*

***4.8 Security and Compliance***

***Description:*** *The system enforces security policies, multi-factor authentication, and compliance measures to protect data and ensure proper access controls.*

***User Requirements:***

1. ***Password Policies:*** *The system enforces vital password requirements, including length, complexity, and regular changes.*
2. ***Multi-Factor Authentication (MFA):*** *MFA must be used, requiring users to provide two verification forms (e.g., password and OTP).*
3. ***Audit Logs:*** *The system must log user activities, including login attempts and actions, for compliance and security purposes.*
4. ***Data Encryption:*** *Sensitive data must be encrypted at rest and in transit to protect against unauthorized access.*
5. ***Access Controls:*** *Role-based access controls must be implemented to ensure users only have access to necessary parts of the system based on their roles.*

***5. Security Features***

*Ensuring robust security measures is essential for safeguarding user data and maintaining the integrity of the investment management system. This section outlines the security features incorporated into the system to protect against unauthorized access, data breaches, and fraudulent activities. By implementing multiple layers of security, from initial registration to real-time notifications, the system aims to provide a secure and reliable experience for all users. The following features detail the mechanisms in place to verify user identity, prevent attacks, and ensure that sensitive transactions are conducted with the highest level of security.*

**5.1. Various Methods of Confirmation for Initial Registration:**

* **Email Confirmation:** Users receive a confirmation email with a link to verify their email address.
* **SMS Verification:** Users receive a confirmation code via SMS to verify their phone number.
* **ID Upload Verification:** Users upload identification documents that the system validates.

A screenshot of a computer

Description automatically generated

**5.2. Reauthenticating for Sensitive Transactions:**

* **Password/Biometric Reauthentication:** Users must re-enter their password or use biometric authentication for high-risk actions.
* **Secondary Confirmation:** An additional confirmation method, such as an OTP or security question, is used to finalize sensitive transactions.

**Multi-Factor Authentication (MFA):**

* **Integration:** MFA is integrated into both registration and login processes.
* **Methods:** MFA methods include SMS codes, authenticator apps, and hardware tokens.

**Preventing Cross-Site Request Forgery (CSRF) and Other Attacks:**

* **Anti-CSRF Tokens:** The system uses CSRF tokens to prevent unauthorized actions from being executed.
* **Additional Confirmation Steps:** Sensitive operations require extra verification steps.

**After-the-Fact Notification:**

* **Email Alerts:** Users receive email notifications of sensitive transactions.
* **Push Notifications:** Users receive push notifications for real-time updates on sensitive activities.

**Human Verification:**

* **CAPTCHA:** CAPTCHA confirms that humans perform transactions, not automated bots

A white rectangular object with black text

Description automatically generated

**Real-World Examples:**

* **Online Merchants:** Implementing multi-factor authentication and real-time alerts for transactions.
* **Banking Systems:** Utilizing strong password policies and secure document upload verification.