# Introduction:

Provide an overview of the purpose and scope of the requirements document.

# Background:

Include any relevant information about the business, project, or problem being addressed.

# Stakeholder Requirements:

List the needs and expectations of all stakeholders involved in the project.

# Business Objectives:

Identify the specific goals and outcomes that the project is expected to achieve.

# Functional Requirements:

Describe the specific functions and features that the solution must have in order to meet the business objectives.

User Login: The solution must allow users to log in with a unique username and password.

"The system must provide a secure login feature that allows registered users to access the platform by entering their username and password. In case of a failed login, the system must display an error message indicating the reason for the failure (e.g. incorrect username or password) and prompt the user to try again. To prevent unauthorized access, the system must limit the number of consecutive failed login attempts and lock the account after a specified number of attempts. The user must be able to reset their password if they have forgotten it."

Title: User Login

Primary Actor: Registered User

Goal: To allow a registered user to access the platform and retrieve information.

Preconditions:

The user has a registered account with a valid username and password.

Flow of Events:

The user launches the platform and is prompted to enter their username and password.

The user enters their username and password.

The system validates the login credentials. a. If the username and password are correct, the system grants access to the platform. b. If the username and password are incorrect, the system displays an error message and prompts the user to try again.

If the user makes multiple consecutive failed login attempts, the system locks the account.

If the user has forgotten their password, they can initiate a password reset process.

Postconditions:

The user is able to access the platform and retrieve information.

The system protects the user's information and limits the number of consecutive failed login attempts.

The user is able to reset their password if necessary.

As a registered user, I want to be able to log into the platform, So that I can access my information and perform tasks.

Acceptance Criteria:

The user can enter their username and password to log in.

The system displays an error message if the username or password is incorrect.

The system limits the number of consecutive failed login attempts.

The user can initiate a password reset process if they have forgotten their password.

Better Examples

Two-Factor Authentication (2FA): Requiring users to provide two forms of identification, such as a password and a one-time code sent to their phone, to log in.

Multi-Factor Authentication (MFA): Requiring users to provide multiple forms of identification, such as a password, a fingerprint, and a one-time code sent to their phone, to log in.

Risk-Based Authentication: Dynamically adjusting the authentication requirements based on the level of risk associated with the login attempt, for example, requiring stronger authentication for high-risk logins from unfamiliar devices or locations.

Device Trust: Allowing users to mark a device as trusted, so that they can log in with fewer authentication steps from that device in the future.

Geolocation Verification: Verifying the user's location before allowing them to log in, to prevent unauthorized logins from outside the organization.

Passwordless Authentication: Allowing users to log in using an alternative method, such as a biometric scan or a one-time code sent to their phone, instead of a password.

Data Management: The solution must allow users to create, edit, and delete records in the database.

Report Generation: The solution must generate reports based on specified criteria and allow users to export them in different formats (PDF, Excel, etc.).

Alerts and Notifications: The solution must send email or SMS notifications to users based on specific events or triggers.

Mobile Access: The solution must be accessible from mobile devices and provide a similar user experience as on desktop devices.

Data Import/Export: The solution must allow users to import and export data from/to external systems in a specific format.

User Permissions: The solution must allow administrators to assign different levels of access and permissions to users based on their role.

Workflow Management: The solution must support customizable workflow processes to automate business processes.

Search Functionality: The solution must provide a search function that allows users to quickly find and retrieve relevant information.

Dashboards: The solution must display real-time information and analytics through customizable dashboards.

Integration with Other Systems: The solution must integrate with other systems, such as CRM, accounting, or HR, to exchange data and avoid duplicated data entry.

Document Management: The solution must support the management of documents and attachments, including version control, access control, and search.

Task Management: The solution must support the creation, tracking, and completion of tasks, with the ability to assign tasks to specific users and set deadlines.

Multilingual Support: The solution must support multiple languages and allow users to switch between languages dynamically.

E-commerce: For e-commerce projects, the solution must support secure transactions, product catalog management, order management, and payment processing.

Customer Support: The solution must provide a customer support module, including a ticketing system, live chat, and knowledge base.

# Non-Functional Requirements:

Outline the constraints and requirements for performance, security, usability, and other non-functional aspects of the solution.

Performance: The solution must respond to user requests within 2 seconds, even during peak times.

Response Time: The solution must respond to user requests within 2 seconds, even during peak times.

Throughput: The solution must be able to process a minimum of 100 transactions per second.

Latency: The solution must have a latency of less than 100 milliseconds.

Resource Utilization: The solution must use limited resources, such as memory and storage, to ensure optimal performance.

Load Testing: The solution must be able to handle a maximum load of 1000 concurrent users without any degradation in performance.

Availability: The solution must have an availability of 99.9% or higher.

Scalability: The solution must be able to handle an increasing number of users and data over time, without affecting performance.

Scalability: The solution must be able to handle an increasing number of users and data over time.

Security: The solution must protect sensitive data and comply with industry-standard security protocols, such as SSL and encryption.

Usability: The solution must be user-friendly and accessible to users with disabilities, with clear navigation and simple, intuitive interfaces.

Interoperability: The solution must be compatible with other systems and platforms, allowing for easy integration and exchange of data.

Reliability: The solution must be available 24/7 and have a high level of reliability, with minimal downtime for maintenance.

Maintainability: The solution must be maintainable, with clear documentation and the ability to make updates and changes easily.

Compliance: The solution must comply with relevant regulations and standards, such as GDPR and HIPAA.

# Assumptions and Dependencies:

Identify any assumptions made about the project and list any dependencies that need to be taken into account.

# Acceptance Criteria:

Define the criteria that will be used to determine if the solution meets the requirements and expectations.

# Appendices:

Provide any additional information or supporting material, such as diagrams, data samples, or references to related documents.