Non-Functional Requirements Document (NFRD)

1. Document Purpose

This Non-Functional Requirements Document (NFRD) defines the **quality attributes, constraints, and operational characteristics** of the User Management System (UMS). These requirements describe *how* the system must perform rather than *what* it must do.

This document complements the BRD and FRD and is critical for architectural decisions, system design, and operational readiness.

---

2. Quality Attribute Overview

The User Management System must meet enterprise-grade expectations for: - Security - Performance - Scalability - Availability & Reliability - Maintainability - Observability - Compliance

---

3. Security Requirements

3.1 Data Security

NFR-SEC-01: All data in transit shall be encrypted using industry-standard protocols.

NFR-SEC-02: Sensitive data at rest shall be encrypted.

NFR-SEC-03: Credentials and secrets shall never be stored in plain text.

3.2 Access Security

NFR-SEC-04: The system shall enforce least-privilege access.

NFR-SEC-05: Administrative actions shall require elevated privileges.

NFR-SEC-06: The system shall protect against common security threats (e.g., brute force, credential stuffing).

3.3 Compliance & Standards

NFR-SEC-07: The system shall align with OWASP Top 10 security risks.

NFR-SEC-08: The system shall support compliance with relevant regulatory requirements.

---

4. Performance Requirements

NFR-PER-01: Authentication requests shall complete within defined SLA thresholds under normal load.

NFR-PER-02: Authorization checks shall not introduce noticeable latency to consuming applications.

NFR-PER-03: The system shall support concurrent authentication and authorization requests.

---

5. Scalability Requirements

NFR-SCA-01: The system shall scale horizontally to support growth in users and applications.

NFR-SCA-02: The system shall handle spikes in authentication traffic gracefully.

NFR-SCA-03: The system shall support multi-tenant scalability where applicable.

---

6. Availability & Reliability

NFR-AVL-01: The system shall support high availability deployment.

NFR-AVL-02: The system shall minimize single points of failure.

NFR-AVL-03: The system shall recover gracefully from component failures.

NFR-AVL-04: The system shall support disaster recovery objectives.

---

7. Maintainability & Extensibility

NFR-MNT-01: The system shall support modular design to enable independent evolution of components.

NFR-MNT-02: The system shall allow configuration changes without redeployment where possible.

NFR-MNT-03: The system shall support backward-compatible API evolution.

---

8. Observability & Operations

8.1 Logging

NFR-OBS-01: The system shall produce structured logs.

NFR-OBS-02: Logs shall include correlation identifiers for traceability.

8.2 Monitoring

NFR-OBS-03: The system shall expose health check endpoints.

NFR-OBS-04: The system shall expose metrics for key operational indicators.

8.3 Alerting

NFR-OBS-05: The system shall support alerting for critical failures and anomalies.

---

9. Usability Requirements

NFR-USA-01: Administrative interfaces shall be intuitive and role-appropriate.

NFR-USA-02: Error messages shall be clear and actionable without exposing sensitive data.

---

10. Data Management & Retention

NFR-DAT-01: Audit logs shall be retained according to configurable retention policies.

NFR-DAT-02: User data retention shall align with legal and compliance requirements.

---

11. Interoperability

NFR-INT-01: The system shall support standard identity and access management protocols.

NFR-INT-02: APIs shall be versioned and backward compatible.

---

12. Constraints

- Deployment environment constraints
- Budget and infrastructure limitations
- Organizational security policies

---

13. Risks

- Underestimating peak authentication loads
- Misalignment with evolving compliance standards
- Operational complexity due to integrations

---

14. Acceptance Criteria

- Non-functional requirements are measurable and testable.
- System meets defined SLAs under expected load.
- Security testing passes defined benchmarks.

---

15. Approval

Name	Role	Signature	Date