

# Requirement Documentation for Staff Id Module

VERSION 1.0

DATE: OCTOBER 22,2024.

PREPARED BY: PHILIP MANTE ASARE

# TABLE OF CONTENTS

[Requirement Documentation for Staff Id Module 1](#_Toc1270106282)

[TABLE OF CONTENTS 1](#_Toc409775172)

[1 Business Requirements 1](#_Toc1077832952)

[1.1 Overview 2](#_Toc589571681)

[1.2 Business Objectives 2](#_Toc394253480)

[2. Functional Requirements 3](#_Toc598421672)

[2.1 User Roles 3](#_Toc2069168591)

[2.2 Functional Modules 4](#_Toc1179293701)

[2.2.1 Employee Onboarding 4](#_Toc1228779757)

[2.2.2 NIA Integration 5](#_Toc659801642)

[2.2.3 Access Control System Integration 6](#_Toc2104755378)

[2.2.4 Devices Management 8](#_Toc202165691)

[2.2.5 Role Management 9](#_Toc300973087)

[2.2.6 Biometric Authentication 9](#_Toc2136859725)

[2.2.7 Access Anomaly Identification 10](#_Toc1612447694)

[2.2.8 Report Generation 11](#_Toc540254241)

[3. Non-Functional Requirements 12](#_Toc1001340632)

[3.1 Performance Requirements 12](#_Toc1672593921)

[3.2 Availability & Reliability Requirements 12](#_Toc699270171)

[3.3 Scalability Requirements 12](#_Toc224179166)

[3.4 Usability Requirements 13](#_Toc1169325394)

[3.5 Security Requirements 13](#_Toc1631812784)

[3.6 Logging & Audit Requirements 13](#_Toc1622445128)

[3.7 Session Management Requirements 14](#_Toc355042020)

# 1 Business Requirements

## 1.1 Overview

To develop a web-based system that automates employee onboarding and manages building access using Ghana Card and biometric authentication. The system will:

* Integrate with NIA databases to retrieve and verify employee details during onboarding
* Assign employees to roles that determine their default access permissions
* Allow administrators to grant custom (direct) access to specific entrances regardless of role
* Support authentication via Ghana Card or biometrics (facial recognition or fingerprints)
* Integrate with existing entrance access control systems
* Provide real-time reporting on access events, access issues, and employees' last known access points

## 1.2 Business Objectives

**1. Automate Employee Onboarding:**

* Simplify and streamline the onboarding process by capturing employee details via Ghana Card and biometrics, reducing manual data entry and processing time.

**2. Identity Verification:**

* Verify employee identity in real-time by integrating with NIA's API to retrieve and confirm employee details, ensuring authentic employee records.

**3. Flexible Access Management:**

* Assign employees role-based access permissions or grant custom direct access to specific entrances based on business needs.

**4. Secure Access Control:**

* Enable seamless building access using Ghana Card or biometric authentication, eliminating the need for traditional access cards or keys.

**5. Real-time Monitoring and Reporting:**

* Generate comprehensive reports on access events, system issues, and employee last known access points for security and facility management.

**6. Ensure Data Security and Compliance:**

* Comply with data protection laws to secure personal and biometric data, maintaining employee privacy and avoiding regulatory breaches.

# 2. Functional Requirements

## 2.1 User Roles

The system will have different types of users:

**1. Administrator**

* **FR-1:** Must be able to manage system configuration and settings
* **FR-2**: Must be able to create, edit, and delete system users and assign system roles
* **FR-3**: Must be able to create and manage system roles with page-level permissions
* **FR-4**: Must be able to create, edit, and delete building entrances and assign access devices
* **FR-5**: Must be able to create, edit, and manage access control devices for entrances
* **FR-6**: Must be able to onboard, edit, and manage employee records and assign job roles
* **FR-7:** Must be able to create and manage job roles and define entrance access permissions
* **FR-8**: Must be able to assign custom direct access to specific employees for individual entrances
* **FR-9:** Must be able to view, generate, and export all system reports
* **FR-10**: Must be able to assign access anomalies to other users for resolution
* **FR-11**: Must be able to investigate and resolve identified access anomalies.

**2.Users:**

* **FR-12**: Must be able to onboard new employees
* **FR-13:** Must be able to assign job roles to onboarded employees
* **FR-14**: Must be able to generate reports
* **FR-15**: Must be able to view real-time log of access events
* **FR-16:** Must be able to investigate and resolve identified access anomalies

**3. Employees:** Individuals who are being onboarded and assigned job roles for access control

* **FR-17**: Must be able to request access to additional areas
* **FR-18**: Must be able to update personal information

## 2.2 Functional Modules

#### **2.2.1 Employee Onboarding**

* **FR-19** The system must capture the employee's details by taking the Ghana Card number and biometric data (face or fingerprint) and verify the information via NIA API.
* **FR-20** The system must receive and process the NIA API response containing verified employee details.
* **FR-21** The system must auto-populate employee data fields in the onboarding form with verified information from the NIA response.
* **FR-22** The system must allow administrators to assign job roles and employment status to employees and save all information to the database.
* **FR-23** The system must validate the Ghana Card number format before attempting NIA API verification.
* **FR-24** The system must display specific error messages based on verification failure type:

Invalid Ghana Card format

NIA API connection failure

Employee not found in NIA database

Biometric verification failure

* **FR-25** The system must log all failed verification attempts including timestamp, user, Ghana Card number (if valid format), and failure reason for security monitoring.

This provides comprehensive error handling and audit trail capabilities. The logging will help with:

* Security monitoring for potential fraud attempts
* System troubleshooting
* Compliance and audit requirements
* Performance monitoring of the NIA API integration

#### **2.2.2 NIA Integration**

**FR-26**

The system must call the NIA API to retrieve verified employee details (name, date of birth, gender, etc.) based on the Ghana Card number and biometric data.

**FR-27**

The system must display verified employee data from NIA.

**FR-28**

The system must handle NIA API timeouts and connection failures gracefully with appropriate error messages.

**FR-29**

The system must securely transmit Ghana Card number and biometric data to the NIA API using encrypted connections.

**FR-30**

The system must validate the NIA API response format before processing employee data.

**FR-31**

The system must log all NIA API requests and responses (excluding sensitive data) for audit purposes.

#### **2.2.3 Access Control System Integration**

**FR-33**

The system must interface with the building’s access control system to grant authorized employees into a room

**FR-34**

The system must interface with the building’s access control system to deny unauthorized employees into a room.

**FR-35**

The system must keep logs of all entry and exit in building and last access point

**FR-36**

The system must be able to deny and grant access based on role or direct access

**FR-37**

The system must be able to log and notify admins of all access anomalies.

**Authentication Methods:**

* **FR-38**: The system must support Ghana Card NFC authentication at access points
* **FR-39**: The system must support biometric authentication (face or fingerprint) at access points

**Time-based Access:**

* **FR-40**: The system must enforce time-based access restrictions (e.g., business hours, shift times)
* **FR-41**: The system must deny access outside of permitted time windows

**Real-time Communication:**

* **FR-42**: The system must communicate with access control devices in real-time to make instant grant/deny decisions
* **FR-43**: The system must handle offline access scenarios when network connectivity is lost

**Security & Monitoring:**

* **FR-44**: The system must detect and log tailgating attempts (multiple people using one credential)
* **FR-45**: The system must log failed authentication attempts at access points

**System Status:**

* **FR-46**: The system must monitor the status of all connected access control devices
* **FR-47**: The system must alert administrators when access devices go offline

**Emergency Override:**

* **FR-48**: The system must support emergency unlock/lockdown of all entrances by administrators

The system must support three access control modes for each entrance:

**Full Access Mode:**

* **FR-49**: Must grant access based solely on base access permissions (role-based or direct access) without time restrictions

**Lenient Mode:**

* **FR-50**: Must check base access permissions and time range for entry requests
* **FR-51**: Must deny entry if outside permitted time range
* **FR-52**: Must allow exit even if outside time range but log as "out of time range exit"

**Strict Mode:**

* **FR-53**: Must verify base access permissions, time range, and badge-in status before granting exit
* **FR-54**: Must verify base access permissions, time range, and badge-out status before granting entry
* **FR-55**: Must send notification to admin if any person accessing entrance in strict mode fails

#### **2.2.4 Devices Management**

* **FR-56**: Admin must be able to add new access devices and assign entrances with new device (Entry or Exit)
* **FR-57:** Admin must be to view recent access per device access
* **FR-58:** Admin must be able to edit and update existing access device configurations
* **FR-59:** Admin must be able to remove/deactivate access devices from the system.

#### **2.2.5 Role Management**

* **FR-60**: Admin must be able to create new job roles with custom names and descriptions
* **FR-61**: Admin must be able to assign entrances to job roles, defining which areas each role can access
* **FR-62**: Admin must be able to edit existing job roles and modify their entrance permissions
* **FR-63**: Admin must be able to delete job roles (with validation that no active employees are assigned to that role)
* **FR-64**: Admin must be able to view all job roles and their associated entrance permissions
* **FR-65**: Admin must be able to assign time-based access restrictions to job roles (working hours, days of week)
* **FR-67**: Admin must be able to copy/duplicate existing job roles to create similar roles quickly
* **FR-68**: The system must prevent deletion of job roles that are currently assigned to active employees
* **FR-69**: Admin must be able to view which employees are assigned to each job role
* **FR-70**: The system must maintain an audit log of all job role changes (creation, modification, deletion).

#### **2.2.6 Biometric Authentication**

**FR-71**

* Employees should be able to use fingerprints to authenticate themselves at various access points in the building.
* Employees should be able to use facial recognition to authenticate themselves at various access points in the building.
* Access should be granted or denied based on biometric match.

#### **2.2.7 Access Anomaly Identification**

* **FR-72:** The system must detect and flag unauthorized access attempts to restricted areas
* **FR-73**: The system must identify and log multiple failed authentication attempts within a specified time period
* **FR-74**: The system must detect tailgating incidents (multiple people using single credentials)
* **FR-75**: The system must flag access attempts outside of permitted time ranges
* **FR-76**: The system must identify employees accessing areas they don't have permission for
* **FR-77**: The system must detect unusual access patterns (accessing multiple areas in impossible timeframes)
* **FR-76**: The system must flag employees who remain in the building beyond normal hours without authorization
* **FR-77**: The system must detect and alert on device malfunctions or tampering attempts
* **FR-86**: The system must identify badge-in/badge-out mismatches (entering without exiting or vice versa)
* **FR-87**: The system must flag dormant credentials being used after extended periods of inactivity
* **FR-88**: The system must generate real-time alerts to administrators when anomalies are detected
* **FR-89**: The system must categorize anomalies by severity level (Severe, Warning, Info)
* **FR-90**: The system must maintain a detailed log of all identified anomalies with timestamps and evidence.

#### **2.2.8 Report Generation**

* **FR-91**: The system must generate access logs reports showing all entry and exit activities within specified date ranges
* **FR-92**: The system must generate employee access reports showing individual employee access history and patterns
* **FR-93**: The system must generate anomaly reports detailing all detected security incidents and violations
* **FR-94**: The system must generate device status reports showing the operational status and performance of all access control devices
* **FR-95**: The system must generate role-based access reports showing which employees have access to specific areas
* **FR-96**: The system must generate time-based access reports showing access patterns by time of day, week, or month
* **FR-97**: The system must generate occupancy reports showing current building occupancy and last known locations of employees
* **FR-98**: The system must allow administrators to schedule automated report generation and delivery
* **FR-99**: The system must support multiple report formats (PDF, Excel, CSV) for export
* **FR-100**: The system must allow report filtering by employee, role, entrance, time, and anomaly type
* **FR-101**: The system must generate executive summary reports with key metrics and statistics
* **FR-102**: The system must maintain report generation logs showing who generated which reports and when

# 3. Non-Functional Requirements

#### 3.1 Performance Requirements

* **NFR-1**: The NIA API calls must have a response time of less than 60 seconds
* **NFR-2**: Employee authentication (via Ghana Card or biometric data) must complete within 60 seconds at access points
* **NFR-3**: The system must support concurrent access requests from at least 100 users simultaneously
* **NFR-4**: The system must handle peak loads during shift changes without performance degradation
* **NFR-5**: Database queries for reports must execute within 10 seconds for standard date ranges

#### 3.2 Availability & Reliability Requirements

* **NFR-6**: The system must maintain 99.9% uptime with scheduled maintenance downtime not exceeding 2 hours per month
* **NFR-7**: Daily automated backups must be performed with a disaster recovery plan in place
* **NFR-8**: Maximum recovery time objective (RTO) must be 4 hours in case of system failure
* **NFR-9**: Access control decisions must continue functioning during network outages (offline mode)

#### 3.3 Scalability Requirements

* **NFR-10**: The system must be scalable to handle up to 5,000 employees without major architectural changes
* **NFR-11**: The system must support up to 50 access control devices
* **NFR-12**: The database must handle growth of access logs for at least 5 years

#### 3.4 Usability Requirements

* **NFR-13**: The user interface must be intuitive and user-friendly for HR personnel with minimal technical knowledge
* **NFR-14**: The employee onboarding process (Ghana Card scanning and biometric capture) must not exceed 5 minutes per employee
* **NFR-15**: The web interface must be responsive and work on desktop
* **NFR-16**: New administrators must be able to perform basic tasks within 2 hours of training
* **NFR-17**: The system must provide clear error messages and user guidance

#### 3.5 Security Requirements

* **NFR-18**: All data transmission must be encrypted using TLS 1.3 or higher
* **NFR-19**: Biometric data must be encrypted at rest using AES-256 encryption
* **NFR-20**: The system must implement role-based authentication.
* **NFR-21**: Session timeouts must be enforced after 30 minutes of inactivity
* **NFR-22**: The system must comply with Ghana Data Protection Act requirements

#### 3.6 Logging & Audit Requirements

* **NFR-23**: The system must log all user login and logout activities with timestamps and IP addresses
* **NFR-24**: The system must log all administrative actions (user creation, role changes, system configuration) with user identification and timestamps
* **NFR-25**: The system must log all access control events (successful/failed entry attempts, anomalies) with complete audit trails
* **NFR-26**: The system must log all NIA API calls and responses (excluding sensitive personal data) for troubleshooting and compliance
* **NFR-27**: The system must log all system errors, exceptions, and security incidents
* **NFR-28**: Audit logs must be tamper-proof and retained for a minimum of 7 years
* **NFR-29**: The system must support log export functionality for external audit and compliance reporting

#### 3.7 Session Management Requirements

* **NFR-30**: User sessions must automatically expire after 30 minutes of inactivity
* **NFR-31**: The system must force logout and require re-authentication after 8 hours of continuous use
* **NFR-32**: The system must support concurrent session limits (maximum 3 active sessions per user)
* **NFR-33**: The system must immediately invalidate sessions when user accounts are disabled or roles are changed
* **NFR-34**: The system must provide secure logout functionality that completely terminates user sessions
* **NFR-35**: The system must log all session timeout and forced logout events