# PROJECT CHARTER

PROJECT NAME: STAFF ID MODULE

SUBMITTED BY: PHILIP MANTE ASARE

## Project Purpose

To develop a web-based system that automates employee onboarding and manages a building’s access using Ghana Card and biometric data. The system will pull employee information from the NIA database, assign appropriate roles, and control access to building entrances using Ghana Card or biometric authentication (face or fingerprints).

## Project scope

The scope of this project is to develop a web-based staff identification and access control system that automates the employee onboarding process using the Ghana Card number and biometric data (either facial recognition or fingerprint). The system will integrate with the National Identification Authority (NIA) API to verify the employee's identity and retrieve their details. These details will be used to auto-populate fields in the application during the onboarding process, ensuring that the individual is who they claim to be.

During onboarding, the system will first validate the format of the Ghana Card number, which will serve as the unique employee ID. Once validated, the system will store the employee's details after a successful verification from the NIA API response. The system will utilize the Ghana Card's NFC capabilities or biometric data for physical access control, implementing a multi-factor authentication approach.

A role-based access control (RBAC) system will be implemented to manage access to different entrances. Common areas will be accessible to all roles, while access to specific zones will be determined by employee roles and permissions. This hierarchical structure ensures organized and secure access management across the entire facility. The system will integrate with access readers at doors, connect to the existing building security infrastructure, and maintain real-time access verification and logging.

Security measures will include secure employee data, encrypted data transmission, comprehensive access logs, and role-based administrative controls. This integrated system will provide a seamless, secure, and efficient method for employee identification and access management while maintaining the integrity of sensitive personal data.

## Project Objectives

1. Develop a system that captures an employee's Ghana Card number and biometric data (either facial recognition or fingerprint) during the onboarding process.
2. Validate the format of the Ghana Card number to ensure it adheres to the correct structure and can serve as the employee's unique identifier.
3. Integrate the system with the National Identification Authority (NIA) API to:

* Verify the employee's Ghana Card number and biometric data.
* Confirm the employee's identity by matching the details provided with the NIA database, ensuring the individual is who they claim to be.

1. Automatically populate fields in the web application (e.g., name, date of birth, nationality) using the verified details received from the NIA API.
2. Utilize the Ghana Card's NFC capabilities or person’s biometric data for physical access control. This replaces the need for printed ID cards, leveraging the Ghana Card and biometric data as a means of access.
3. Implement a robust RBAC (Role Based Access Control) system that:

* Manages access to specific zones (e.g., main building, departments, sub-offices, secure areas).
* Assigns access permissions based on employee roles.
* Supports multi-factor authentication by combining Ghana Card and biometric data.

1. Direct access assignment where individual employees can be granted custom access to specific entrances regardless of their role.
2. Ensure secure handling of all data, including biometric and personal information, with encryption and compliance with data protection regulations.
3. Develop an easy-to-use web interface that allows users of the system to onboard employees, verify identities using Ghana Card and biometric data

* Manage role-based access permissions
* Assign direct access to employees.
* View comprehensive Reports
* View Issues that come up during access.
* View Employee Current Location
* Manage access control efficiently.

1. Maintain detailed logs of access control activities, onboarding actions, and system events for auditing and security purposes.

## Deliverables

1. Project Plan
2. Project Flow Diagram
3. Requirement Documents
4. Web-based Access Control System
5. Access Reports
6. Testing and Quality Assurance Reports
7. User Manual
8. Closing Report

## Milestones

1. Project Kickoff
2. Complete Requirements Gathering and Documentation
3. System Architecture and Design Specifications Approval
4. Core functionalities successfully completed
5. Complete system integration testing
6. Conduct User Acceptance Testing with stakeholders to ensure system meets requirements and expectations.
7. Final project review and closure meeting, including the delivery of the closing report and lessons learned.

## Assumptions

1. The NIA API will be available and reliable for data retrieval throughout the project lifecycle.
2. Employees will have access to the necessary technology (e.g., biometric devices, computers) to use the new system.
3. The system will comply with all relevant local laws and regulations regarding data privacy and security.
4. Users will provide timely feedback during testing phases to facilitate necessary adjustments.
5. Key stakeholders will remain committed and engaged throughout the project.
6. All necessary resources (including technical skills, hardware, software, and data access) needed to build the project will be readily available and attainable within the project timeline.

## Risks and Mitigation

1. Difficulty integrating with the NIA API, leading to delays in timeline of project

**Mitigation**: Conduct thorough research on the APIs and perform early integration tests.

1. Potential breaches of sensitive employee data could lead to legal issues and loss of trust.

**Mitigation**: Implement robust data encryption and access controls and ensure compliance with local data protection regulations.

1. Employees may resist using the new system due to changes in process or technology.

**Mitigation**: Provide comprehensive training and clear communication about the benefits of the new system.

1. Lack of engagement or changes in stakeholder requirements could lead to scope creep.

**Mitigation**: Maintain regular communication with stakeholders and conduct frequent system reviews.

|  |  |
| --- | --- |
| (Project Sponsor Name) | Signature |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |