User Manual for Emergency Device Management System

Introduction

Welcome to the EDMS User Manual. This guide will help you install, deploy, and effectively use the application. This application will display device information, as well as features to add, delete, and update device records. Users will be able to search for specific devices, and the system will differentiate between user and admin accounts to control access to certain functions. Automated notifications will be sent to alert users of upcoming device expirations and required maintenance.

System requirements

1. Web Browser: A modern, standards-compliant browser such as:
   - Google Chrome (latest version)
   - Mozilla Firefox (latest version)
   - Safari (latest version for macOS)
   - Microsoft Edge (latest version)
2. Operating System: Generally, any operating system that supports modern web browsers:
   - Windows 10 or later
   - macOS Mojave or later
   - Linux (Ubuntu 18.04 or later recommended)
3. Internet Connection: Minimum 5 Mbps for optimal performance (varies with application size).
4. Device: Desktop, laptop, tablet, or smartphone with minimum 2 GB RAM (more recommended for complex apps).

Installation

This application is packaged as a Docker container, making it easy to deploy in various environments, whether on-premise or in the cloud (e.g., Azure, AWS, or Google Cloud). Ensure your deployment environment supports Docker and has access to a PostgreSQL-compatible database. Configure the necessary environment variables (e.g., database credentials, JWT secret) as needed.

Deployment details may vary based on your specific environment and infrastructure requirements.

Using the Application

- **Authentication**: The "Authentication" component is responsible for verifying user credentials to ensure that only authorized individuals can access the system. It manages the login, registration, and password recovery processes.
    - Login: Validates user credentials against stored data. If correct, access to the system is granted.
    - Registration: Saves new user details in the database, creates a new user account, and displays a success message.
    - Forgot Password: Sends a password reset email to the provided address and displays a success message.

- **Dashboard**: The "Dashboard" component is responsible for the management of emergency devices across locations. Admins can create, read, update, and delete device records (regular users can only read), Devices can be filtered by building using an interactive map, while additional filtering and searching are available through a search box and dropdown menus.
    - User Actions: Create, read, update, and delete operations for Admins; read operations for regular users.
    - Device Data: Includes Device ID, Device Type, Room, Serial Number, Status, Manufacture Date, Description, Size, and Last Inspection Date.
    - Search and Filter Inputs: Search box input and dropdown selections for filtering by device type, status, or location.

- **Admin**: The “Admin” component is used to manage location and user information in the system, like locations (Sites, Buildings, Rooms), users, and device types. It allows admins to add, view, update, and delete records for these categories.
    - Add, view, update, and delete Locations (Sites, Buildings, Rooms)
    - View, update, and delete Users and their roles.
    - Add, view, update, and delete Device Types
- **Inspect**: The "Inspection" component is responsible for creating and viewing inspections for fire extinguishers. It enables viewing past inspection details for a fire extinguisher and creating new inspections for fire extinguishers by Admin users.
    - Admins can create new inspection records for fire extinguishers.
    - Admins can view existing inspection records which include Inspection date, inspector's name, and device condition.
- **Notification**: The “Notification” component is responsible for notifying users about devices that are nearing their expiry or have an upcoming inspection due date (within the next 30 days). Notifications are displayed in a bell icon dropdown on the dashboard after the user logs in.
    - After a successful login, the system checks device records for expiry and inspection dates.
    - Generates notifications for devices with upcoming expiry or inspections due within the next 30 days.
    - Displays these notifications in the dropdown menu associated with the bell icon on the dashboard.