DPDP Compliance Software Overview

Objective: To design and implement a webpage compliant with the Digital Personal Data Protection (DPDP) Act 2023. The webpage is intended to manage different types of users, specifically admin, employee, and company, ensuring secure handling and processing of personal data.

Goals:

- **Compliance**: Ensure the webpage complies with all regulations stipulated in the DPDP Act 2023.
- **User Management**: Implement a robust user management system to handle different user roles (admin, employee, company).
- **Data Security**: Implement stringent data security measures to protect personal data.
- **Transparency**: Provide clear documentation and user interfaces to ensure transparency in data handling processes.

Usage

The DPDP compliance software will be used by various stakeholders within an organization to ensure compliance with the DPDP Act 2023. The main users include Compliance Officers, IT Administrators, Data Protection Officers (DPO), Legal Teams, Senior Management, and Employees. They will use the software to set up compliance controls, upload and manage evidence, monitor compliance status, conduct audits, receive and respond to alerts, and generate reports.

Who Will Use/How Will They Use

Compliance Officers:

- **Role**: Ensure adherence to the DPDP Act.
- **Usage**: Monitor compliance actions, upload evidence, generate reports, set up controls, receive alerts.

IT Administrators:

- **Role**: Maintain technical aspects of compliance.
- **Usage**: Configure security settings, integrate software with IT infrastructure, ensure data integrity.

Data Protection Officers (DPO):

- **Role**: Oversee data protection strategies.

- **Usage**: Review/manage data processing, conduct audits, guide compliance requirements.

Legal Teams:

- **Role**: Provide legal oversight.
- **Usage**: Interpret DPDP requirements, review reports/evidence, advise on legal risks.

Senior Management:

- **Role**: Oversee compliance and risk management.
- **Usage**: Review compliance status/reports, make strategic decisions.

Employees:

- **Role**: Follow compliance protocols.
- **Usage**: Adhere to data protection policies, report breaches, participate in training.

Functions

1. **User Management**
    - Register, login, and manage user accounts with role-based access control.
2. **Company Management**
    - Register companies, define IT assets and scopes, manage control data.
3. **Control Family Management**
    - Define control families and assign controls for compliance.
4. **Compliance Scoring**
    - Score companies based on completed actions and required compliance measures.
5. **Evidence Uploading Portal**
    - Upload and manage evidence, maintain audit logs and records.
6. **Security & Compliance**
    - Data encryption, secure authentication, authorization, and logging/monitoring controls.
7. **Testing & QA**
    - Unit testing, integration testing, user acceptance testing, security testing.
8. **Deployment & Maintenance**
    - Use Azure for cloud, implement CI/CD pipeline for updates.

Features

1. **User Management**
    - Registration, login, password management, role-based access.
2. **Company Management**
    - Company registration, IT asset definition, control data management.

3. **Control Family Management**
   - Define control families, assign compliance controls.
4. **Compliance Scoring**
   - Algorithm to score companies based on compliance actions.
5. **Evidence Management**
   - Portal for uploading evidence, audit data storage.
6. **Security Features**
   - Data encryption, secure authentication, authorization, logging/monitoring.
7. **Testing & QA**
   - Comprehensive testing to ensure reliability and security.
8. **Deployment & Maintenance**
   - Cloud deployment on Azure, CI/CD pipeline for smooth updates.

System Design Information

Technology Stack:

- **Front-End**: React.js, Redux, React Router
- **Back-End**: Node.js, Express.js
- **Database**: MongoDB, Mongoose

Architecture:

- **Presentation Layer (Front-End)**: React.js for UI, Redux for state management, React Router for routing.
- **Application Layer (Back-End)**: Node.js and Express.js for server-side logic, middleware for various functions.
- **Data Layer**: MongoDB for data storage, Mongoose for ODM.

Core Code Information

Front-End:

- Located in `frontend/src`
- Main components: `App.js`, `Dashboard.js`, `Login.js`, etc.
- CSS for styling components: `ActionTable.css`, `Login.css`, etc.

Back-End:

- Located in `backend`
- Main files: `app.js`, `index.js`
- Controllers for handling various functionalities: `authController.js`, `user.controller.js`, etc.
- Models for data structure: `User.js`, `action.js`, `asset.model.js`, etc.

- Middleware for authentication and authorization: `auth.js`, `adminAuth.js`
- Configuration and database connection: `db.js`

Database Schema

MongoDB Schema:

- **User Collection**: Stores user information such as username, password, role, etc.
- **Admin Collection**: Manages admin-specific data.
- **Employee Collection**: Manages employee-specific data.
- **Company Collection**: Stores company-specific information and associated data.
- **Other Collections**: Manage IT assets, controls, actions, evidence, etc.

Conclusion

This detailed overview provides a comprehensive understanding of the DPDP compliance software, including its usage, user roles, functions, features, system design, and core code information. The system is designed to ensure compliance with the DPDP Act 2023, offering robust data protection, user management, and compliance monitoring capabilities.

1.