**LSEPI and Risk Assessment**

**Legal Considerations**

Data Protection & Privacy

* The dashboard must comply with General Data Protection Regulation (GDPR) if any personal data is processed. While this project primarily involves sensor data, any user authentication data (e.g., login credentials) must be securely stored and handled.

Data Encryption & Security

* All data should be encrypted using modern cryptographic standards.
* Use secure protocols (e.g., HTTPS, TLS) for data transmission.
* Implement role-based access control to restrict access to sensitive settings.

User Authentication & Access Control

* Operators should have access to view temperature data but not modify system settings.
* Managers (admins) should have additional privileges, such as overriding alerts or modifying alert thresholds.
* Implement secure password management, including password hashing and the ability to reset passwords securely.

**Social Considerations**

Impact on Workforce

* Consider training sessions to ensure that all users understand how to interpret dashboard insights.
* **user training materials** or support documentation.

User Experience & Accessibility

* The dashboard must be intuitive for both technical and non-technical users.
* Design should follow responsive web principles, ensuring accessibility on desktops, tablets, and mobile devices.
* Ensure color-coded alerts (traffic-light system) are designed with accessibility in mind (e.g., colourblind-friendly design).

**Ethical Considerations**

Transparency

* Users must understand how temperature alerts are generated.
* Any AI/ML-based decisions should be explainable.
* Provide an explanation interface showing why a particular alert was triggered.
* Allow manual override of ML-based alerts to prevent unnecessary disruptions.

**Professional Considerations**

Industry Standards & Compliance

* Follow best practices
* Ensure compliance with IT security policies and data handling best practices.

Code of Conduct

* Adhere to ethical software development guidelines such as the IEEE/ACM Code of Ethics.
* Maintain clear documentation and version control to track changes in system behaviour.

**GitHub workflow guidelines**

**Risk Assessment & Mitigation**

mitigation strategy for user errors (e.g., accidental setting changes, incorrect data inputs).

Address potential sensor failure risks and how to handle hardware malfunctions.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Likelihood | Impact | Mitigation Strategy |
| Data Breach | Medium | High | Encrypt data, enforce strong authentication, and limit access to authorised data/settings. |
| System Downtime | Low | High | Implement redundancy and have backup recovery strategies. |
| ML Model Inaccuracy | Medium | Medium | Continuously validate the model with real data, allow manual override for alerts. |
| UI/UX Issues | High | Medium | Conduct usability testing and gather feedback early to improve accessibility and navigation. |
| Performance Bottlenecks | Medium | High | Optimize database queries and ensure scalable infrastructure. |

Additional Considerations

* Data Storage: sensor data updates every 30 seconds
* Authentication System: Secure user authentication using hashed passwords.
* Traffic-Light System: Define alert thresholds based on historical data trends to avoid excessive false alarms.
* Display historic data from a data the user inputs
* Statistics in real time