**System Security Awareness**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | |  |  | | --- | --- | | Risk Description |  | | Risk Rating | Recommendation |
| **1** | Data is stored or transmitted unencrypted, making it vulnerable to theft. | High | Use HTTPS encrypted transmission, and enable encryption for the database and storage |
| 2 | The system has no intrusion protection | High | Strictly verify and escape the input and output, enable the firewall and WAF, and conduct regular penetration tests |
| 3 | no backup and recovery process for the data | Medium | Enable automatic backup of the database and storage, and regularly test the recovery process |
| 4 | Unnecessary ports are open | High | Only open the necessary port (443), close other ports, and regularly check the server port configuration |
| 5 | The rules of the security group are too broad | Medium | Apply the principle of least privilege and only allow access to the necessary IP and port |

**Ethical, Legal, Security and Privacy issues**

**Ethical**

We only collect necessary data related to pollen allergy management, such as the approximate location of users, to make the real-time dashboard more accurate.

Maintain transparency in educational content and do not include hidden data or misleading information.

**Legal**

Comply with Australia's privacy principles (APPs) and give users the right to know what data we have collected and why, for example, to display the allergen situation of the suburb where they are located

Users can opt out of data collection at any time or request us to delete their data.

The content and data processing procedures will comply with relevant regulatory requirements.

**Security**

Only open the necessary ports (HTTPS/443) on AWS and shut down all unnecessary services.

The interfaces of real-time dashboard and educational resources will both be protected by Security Groups

We will regularly check the code and conduct penetration tests

**Privacy**

All data transmission is conducted via HTTPS, and data stored on AWS is also encrypted.

Unnecessary data will not be retained for a long time. Only the parts necessary for the normal operation of the website and dashboard functions will be kept.

**Risk Analysis**

Incorrect or altered educational content

Risk: If there are errors or corrected content in educational resources, users may learn something incorrect.

Possibility: Medium.

Impact: High.

Countermeasures: Only reliable people should be allowed to modify the content. Before release, someone should review it. The content should have version records so that errors can be corrected immediately.

Real-time data is unreliable

Risk: If there is a problem with the pollen/allergen data source or someone maliciously modifies the data, users may see false information.

Possibility: Medium

Impact: High

Countermeasures: Conduct more data verification, compare with other sources, alarm when abnormal values are found, and use cached normal data as a fallback.

User privacy leakage

Risk: If suburb or allergy information is leaked, users will feel that their privacy has been violated.

Likelihood: Low

Impact: High

Countermeasures: Only collect the most basic and necessary information. All data transmissions should be encrypted and stored on AWS as well. Users can apply for data deletion at any time.

The system was attacked (SQL injection/XSS)

Risk: Hackers may write malicious code or queries in the input box, resulting in system control or data leakage.

Likelihood: Low

Impact: High

Countermeasure: Strictly perform input verification at the back end

The Dashboard has been overwhelmed or crashed

Risk: If too many users access it simultaneously, the dashboard may crash.

Possibility: Medium.

Impact: Moderate to high

Countermeasures: Add cache to the interface, limit the number of requests per user, and use AWS WAF to intercept abnormal traffic.