# ThermoTrack Security Overview

**Data Security**

All data sent between the ThermoTrack device, web app and central server is protected.

* Data is encrypted so nobody can read it during transmission.
* Device and servers are authenticated to prevent fake devices from connecting.
* User’s logins on the web application are also protected HTTPS and secure cookies.

**Data Security During Storage**

When data reaches the server, it is stored safely in secured database (MariaDB)

* Sensitive information such as passwords is hashed and salted using algorithms like bcrypt so it cannot be read even if the database is compromised.
* Data backups are encrypted and stored securely to prevent data loss.
* Access to the database is limited to authorized system components only.

All user and sensor data is stored following principle of the least privilege ensuring only required systems can access specific information.

**Application level Security**

* User’s roles determine what each user can view or modify such as Admin or standard users.
* Session management ensures that users are automatically logged out after inactivity to reduce unauthorized access.
* All web forms and API endpoints include server-side validation to ensure the data being sent is valid and secure.

**Device and Hardware Security**

ThermoTrack physical design also contributes to overall system security.

|  |  |  |
| --- | --- | --- |
| Component | Security Function | Description |
| ABS Plastic Project Enclosure | Physical protection | Shields the Raspberry pi and wiring from dust or accidental contact. Prevents direct access to ports and pins |
| Small Sensor Enclosure | Sensor integrity | Protect the PIR and DHT22 sensors from damage or interference, keeping data reliable. |
| Screw Terminal Blocks | Secure wiring | Provides secure, screw-down connection points for all wiring, making maintenance and debugging much safer and easier than temporary connections |
|  |  |  |

Privacy and Data governance

* Only the minimum amount of data necessary for operation is collected.
* Access to personal or sensitive data is logged and reviewed periodically.
* All user actions and systems changes are logged for auditing and accountability.