# Security and Privacy of Face Guard

The importance of security and privacy is a fundamental part of the development process of Face Guard. We are aware of the risk associated with handling and collection of user data and we take these concerns seriously. We are committed on building a product with good security and privacy measures to ensure our users are safe from attacks. Here are the details of our security and privacy measures.

## Security and Privacy Measures

* Device security:
  + FaceGuard will be powered using a Raspberry Pi 3. A firewall will be set up with UFW on the Raspberry Pi 3 to allow only necessary communication.
  + Unused services will be disabled on the Raspberry Pi 3.
* Backend and frontend validation:
  + Validation will be done to ensure the integrity and security of user data by preventing unauthorized or malicious input.
  + Input sanitization and validation will be used to protect access against common security vulnerabilities.
* Data encryption:
  + Sensitive data such as user information will be encrypted on the database to ensure the safety of the information.
  + Modern encryption algorithms will be used to prevent data exposure and data transmission between the application and the server will be using HTTPS protocol.
  + Users will be required to authenticate with a username and a strong passwords to login to the FaceGuard app.
* User Authentication:
  + Users will be able to use their usernames and passwords to enter the app which will help secure the details. Users will be required to create strong passwords.
* Data Transfers and Storage:
  + Data will only be stored on the cloud servers hosted on AWS.
  + PubNub will be used for secure data transfer.
* Data Privacy and Consent:
  + The applications privacy practices and the data taken from user will be communicated clearly to users and consent will be taken.
  + Users will be able to review privacy practices before they use the system.
* Data minimization:
  + Only the essential information that are necessary for the functionality of the application is going to be collected from the user. Gathering of excessive or unnecessary data will be avoided.
* Secure Data Storage:
  + User data collected will be stored at a secure cloud storage and it will not be stored locally for security purposes.
* User Education:
  + Users will be able to find all necessary information regarding privacy measures within the application.

References:

<https://gdpr.eu/what-is-gdpr/>

<https://docs.aws.amazon.com/iot/latest/developerguide/connecting-to-existing-device.html>

<https://www.raspberrypi.com/documentation/computers/configuration.html#securing-your-raspberry-pi>

<https://help.ubuntu.com/community/UFW>

https://www.pubnub.com/docs/general/basics/set-up-your-account