A secure web interface requires:

1.Default passwords and ideally default usernames to be changed during initial setup

2.Ensuring password recovery mechanisms are robust and do not supply an attacker with information indicating a valid account

3.Ensuring web interface is not susceptible to XSS, SQLi or CSRF

4.Ensuring credentials are not exposed in internal or external network traffic

5.Ensuring weak passwords are not allowed

6.Ensuring account lockout after 3 -5 failed login attempts

Sufficient authentication/authorization requires:

1.Ensuring that the strong passwords are required

2.Ensuring granular access control is in place when necessary

3.Ensuring credentials are properly protected

4.Implement two factor authentication where possible

5.Ensuring that password recovery mechanisms are secure

6.Ensuring re-authentication is required for sensitive features

7.Ensuring options are available for configuring password controls

8.Ensuring credential can be revoked

9.The app authentication is required

10.The device authentication is required

11.The server authentication is required

12.Manage authenticated user id(credential info.) and the user's device id, the user's app id mapping table in the authentication server

13.Ensuring that the authentication token/session key issuing to client is always different

14.Ensuring that the user id, app id, device id is universally unique

Securing network services requires:

1.Ensuring only necessary ports are exposed and available.

2.Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.

3.Ensuring services are not vulnerable to DoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.

4.Ensuring network ports or services are not exposed to the internet via UPnP for example

5.The abnormal service request traffic should be detected and blocked on service gateway layer

Sufficient transport encryption requires:

1.Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks.

2.Ensuring other industry standard encryption techniques are utilized to protect data during transport if SSL or TLS are not available.

3.Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols

4.Ensuring the message payload encryption

5.Ensuring the secure encryption key handshaking

6.Ensuring received data integrity verification

Minimizing privacy concerns requires:

1.Ensuring only data critical to the functionality of the device is collected

2.Ensuring that any data collected is of a less sensitive nature (i.e., try not to collect sensitive data)

3.Ensuring that any data collected is de-identified or anonymized

4.Ensuring any data collected is properly protected with encryption

5.Ensuring the device and all of its components properly protect personal information

6.Ensuring only authorized individuals have access to collected personal information

7.Ensuring that retention limits are set for collected data

8.Ensuring that end-users are provided with "Notice and Choice" if data collected is more than what would be expected from the product

9.Ensuring the role based access control/authorization to the collected data/analyzed data is applied

A secure cloud interface requires:

1.Default passwords and ideally default usernames to be changed during initial setup

2.Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms

3.Ensuring account lockout after 3- 5 failed login attempts

4.Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF

5.Ensuring credentials are not exposed over the internet

6.Implement two factor authentication if possible

7.Detect or block the abnormal requests/attempts

A secure mobile interface requires:

1.Default passwords and ideally default usernames to be changed during initial setup

2.Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms

3.Ensuring account lockout after an 3 - 5 failed login attempts

4.Ensuring credentials are not exposed while connected to wireless networks

5.Implementing two factor authentication if possible

6.Apply mobile app obfuscation technique

7.Implement mobile app anti-tempering mechanism

8.Ensuring the mobile app's memory hacking is possible

9.Restrict the mobile app's execution on tempered OS environment

Sufficient security configurability requires:

1.Ensuring the ability to separate normal users from administrative users

2.Ensuring the ability to encrypt data at rest or in transit

3.Ensuring the ability to force strong password policies

4.Ensuring the ability to enable logging of security events

5.Ensuring the ability to notify end users of security events

Securing software/firmware require:

1.Ensuring the device has the ability to update (very important, need secure update mechanism)

2.Ensuring the update file is encrypted using accepted encryption methods

3.Ensuring the update file is transmitted via an encrypted connection

4.Ensuring the update file does not expose sensitive data

5.Ensuring the update is signed and verified before allowing the update to be uploaded and applied

6.Ensuring the update server is secure

7.Implement the secure boot if possible (chain of trust)

Adequate physical security requires:

1.Ensuring data storage medium can not be easily removed.

2.Ensuring stored data is encrypted at rest.

3.Ensuring USB ports or other external ports can not be used to maliciously access the device.

4.Ensuring device can not be easily disassembled.

5.Ensuring only required external ports such as USB are required for the product to function

6.Ensuring the product has the ability to limit administrative capabilities