



OnTime

Powered by ClockedIn



**Time and Attendance
Security and Data**

Time and Attendance Security and Data

Secure transfer of our Time and Attendance data is of the utmost importance to Cube Purple. The data transfer has a number of levels of protection to avoid issues of external data capture.

Data Security Measures

- All the data is encrypted
- To protect our application from external threats, the API & database are encrypted using AES and RSA Cryptographic Algorithms.
- SL Security on Server
- Android Operating System is safer than other operating systems, at the operating system level the Android platform provides the security of the Linux Kernel
- Secure inter-process communication (IPC) facility to enable secure communication between applications running in different processes
- No lottery-themed and similar ADS that have the potential to interrupt and start our using our device.
- The device itself is secured within a kiosk which is locked, this mitigated external threat of accessing ports such as Micro USB
- The operating system is set to run the OnTime app in 'kiosk' mode which means a user cannot navigate to other areas of the operating system. Only users with 'Super Admin Access' can exit out of the OnTime application.
- Wi-Fi network firewall – customer internet policies would apply.

We maintain state-of-the-art technical and organisational measures in order to ensure data security, in particular for the protection of all Personal Data. These measures are updated from time to time in order to remain at the forefront of technology.

A typical user finger scan data string would be double encrypted – Sample below

AwFiFJN4ADAAMAAgACAAIAAgADAAPAC//7//v/+//7//gAAAACCAgc5aUASBAAVHQJV
BFNeGQgoXI0JU349i5EeFgxPHnOREn51Gw9+HKHiXiYjY55MLeSS+dAgUf06sEB9mI5D/

EJThf3Aijj9VIS7/a5OQ3UehpR1Gm+Z6SxuOm00i5IsAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AA
AAAA==

A typical user facial scan data string would be double encrypted – Sample Below

*AID6RAAAAnELpjgq+dpe6PVjhLD2GVzo86t8FvCt0yL3JqgY9cuQ7PeI5zr1GqPQ7IQO0vZv
nQLwk
vKq8uP5nvaUq/rxkHHW8J7JyvNNdIT0Bd0C9jZJuPOVdpz0VxQ69tdEIPIMDJ73Mgzg+W
aoZvNfK
3j2/PKs9/lz2PDgxSD2YXUi8bOKOPTYEjT3AO0S9ngzpPC0jW72tFuy8cmQGvGW2vb2vv
Ay9H1jive6N9Lx44n87zy8LvYaZJr3OScG8hcmuPdtYjj3uMVu9X1m/PH56DjxhKys9nP1B
u33ahj0xj1s9*

These data strings can only be unencrypted by the algorithms created by Cube Purple

Data Size

The below are approximate data sizes of time and attendance events and biometric templates:

Attendance event (1 event) – 2-3Kb

Biometric Facial Template – 20-25Kb

Biometric Finger Template - 20-25Kb