SPECIFICATIONS FOR BIOMETRIC SYSTEM AT OFFICE OF THE PUBLIC SERVICE COMMISSION (OPSC)

Biometric Access Control is a means of control that is used to restrict people, vehicles or any sort of movement into certain areas in a building or an organization by means of blocking them with barriers and granting them access by using different ways of identification.

Biometric Access Control is an important addition to the security system because it is a valuable technique that is used to control who and when people can enter OPSC facilities. Without access control, you risk having your premises and staff exposed to theft, data loss or breach of security.

Understanding the importance of biometric access control has never been more of a necessity to ensure that your staff, assets and services are protected 24/7.

A few benefits of biometric access control include:

- Peace of mind knowing that your staff and building are safe at all times.
- Being able to identify everyone who enters your premises and what time they come and go
- It can be a deterrent for external forces trying to enter your building with malicious intent. Much like alarms and security cameras, access control may discourage burglars or vandalizers from entering your buildings
- You can easily change or block user permissions, making it easy to adjust access when a staff member leaves or changes roles.

Identifying or authenticating a person by set unique points of identification with biological traits such as fingerprints, face or voice which cannot be duplicated or lost, eliminate theft and fraud. This technology is suitable for entrances of office and high-security areas by either using a finger for fingerprint readers, face/voice for face/voice recognition by putting the face next to the face reader or requesting access on one's voice through voice recognition technology or by presenting access cards to the units. The Biometric Technology can either be used for Time Recording or as Access Control.

The following is required by OPSC:

1. Access Control devices

   Virdi, Hikvision, Morpho, Bosch or ZK TECO

2. Main Features
   - Be able to save more than 2 fingers for access
   - Have facial recognition access
   - Have voice recognition access
   - Enroll about 50+ users
   - Enable on device enrolment, terminal configuration and transaction log retrieval
   - Compatible with fingerprint, facial, voice and cards
   - Ability to store users information for a period of 12 months
   - Be able to record users and provide reports on access and exit event
   - Be able to record both access and exit of users
   - Capability to suspend, delete and blacklist users

- Be able to record information during down time

3. Technical Specification
   - Network/Communication
     -Ethernet, RS485, USB and Wi-Fi option
   - Power Supply
     -12V-24V DC
     -Power over Ethernet (POE), compatible with POE+ switches
   - Card reader options
     -Prox Card reader options
     -iClass
     -RFID
   - Use with any Web browser
   - Use with any OS

4. Conclusion
   The system should be of high quality to avoid timeous breakages and be able to provide fake finger detection banned/authorised user list. This will provide peace of mind to OPSC as the end-user.