


STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 1 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

Background

1. General Statement of Purpose

The purpose of this document is to provide CCBRT's Staff with documented and formalized procedures to be adhered with access control policies that are to be utilized throughout CCBRT at all times when using RFID key cards.

The included protocols help ensure that sensitive critical state facilities, protected areas, personally identifiable information (PII) and all other regulated and controlled facilities is secured in accordance with applicable agreements and regulations defined by CCBRT Security and Access control procedures.

2. Scope

- 2.1. This document applies to the CCBRT Data Center and network hubs located at maternity wing, standard wing and private polyclinic wing .

3. Discipline


- 3.1. Administrative Standards

4. Terms and Definitions

- 4.1. Guest – An individual accessing an area for which their Identification card does not allow them access through any electronic doors.
- 4.2. Visitor – An individual without an CCBRT identification card to access secured facilities.
- 4.3. Custodian – A member of CCBRT granted with access to specified accesses secured facilities

5. Instructions

- 5.1. CCBRT has implemented a Security Access Card Control and Identification System. This system includes the physical access control card keys, Closed Circuit Television cameras and physical barriers that require specific authorization based on the security access required by the CCBRT regulations and access control procedures.
- 5.2. These access controls also include guest and visitor access to facilities, in compliance with the Information Security Policy and Procedures that all occupants must have a

STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 2 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

visible identification access key card and all visitors must be escorted by CCBRT authorized personnel and sign visitors form upon temporary access granting to facilities.

5.3. Access to Electronic key card systems

The access control system is securely installed on the production servers, at the secured data center for secured facility areas within CCBRT. Only the systems administrator is able to login to the computers and their databases using special credentials and manage the electronic card access systems and CCTV cameras.

5.4. Electronic key card registration on the access control systems


The key cards are registered on secured databases hosted in two modes.

5.4.1. **Secured Web URL registration:** The systems administrator enters the secured link on CCBRT network to access the secured database, then the administrator username and password on secured link are entered, from there the system administrator will be able to do the settings that include, registering new cards, modify the existing cards, freezing or disabling the user electronic card online.

5.4.2. **Secured CCTV Cameras registration:** The systems administrator may login using admin user name and password onto secured database for electronic IP camera (s) or remote connect the DVR database server for monitoring tasks. With administrative access the administrator may access the security portal where he or she can register the new card, delete, freeze and modify the electronic key card with the computer connected to access card device using ethernet cable.

5.5. Electronic Key Card agreement on handling to user

5.5.1. The user who needs access on secured premises, must first liaise with his or her department head to get approval for the need and then the request is forwarded to IT team for registration by the line manager, after confirmation, the secured facilities will be analyzed by IT team for

STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 3 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

electronic key card generation, then user details like name, card no, facility name, access time and role will be registered onto the Access control systems and set as per the user privilege or level of access defined.

5.5.2. Before handling the electronic key card, the user will need to sign the agreement form of handling key card registered under his or her name. On the form the user will prove his details on empty fields and sign to adhere with the defined access control policies of CCBRT listed on the form.

5.5.3. If the electronic key card after handling gets lost, the user must immediately report to his or her line manager or program coordinator that the IT team may temporarily lock the ID from accessing the restricted areas or facilities as defined by CCBRT access control policies.

5.5.4. If the user resigns or leaves his or her position, the electronic key card should be returned to IT office to unsubscribe the user from the system once confirmation has been done. Again, the user will have to sign the agreement of handling key card on returning, to unbind himself or herself from the contract. Then the systems administrator will work to freeze user account and disable the access to all secured areas.


5.6. Building Access

5.6.1. Employees with CCBRT access key card are given access within the building based on their working title and defined working areas.

5.6.2. Visitors and guests to the building are only granted pass under special supervision of the CCBRT staff after signing the visitation form, defining the purpose of visit where CCBRT's Officer and must check-in be using CCBRT's visitor procedures. Refer to the Visitors section of this document.

5.7. Employee Electronic Key Card Controls

5.7.1. Each employee who has privilege to access the controlled areas, will have

STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 4 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

approved access key card (Electronic ID) registered under his or her name at all times while on duty, will also have the following obligations:


- Appropriately store the electronic key card at office premises or while at home when not in use. The access key card badge should not be lent or given to any other unauthorized person for any means including to allow unspecified person to use it.
- Immediately report lost or stolen electronic key card to the Management and IT help desk, that the IT team may suspend the specified key cards from accessing the facilities.
- Surrender your electronic key cards immediately to your supervisor upon leaving agency employment.

The hiring supervisor must ensure the following after appropriate confirmation of identity:

- New employees have initial registration contract issued at induction /orientation upon completion of new hire paperwork and signing the special access form as defined on the working area responsibilities.
- Replacement of key cards are issued when the original is damaged or lost with strictly description notes from the respective staff who lost the card.
- Appointments may be made to issue new or replacement access cards upon internal agreements as defined in **CCBRT Access Key Form**

5.8. Access Reviews


5.8.1. The IT Support team will conduct physical security access reviews every six months. These reviews will occur in January and July each year. Reports will be kept to CCBRT IT department for the current employees and their access roles, access logs and upgrades. IT team will review the access levels and approve or make changes if so needed. If changes to access need to be made, an access change request must be completed. The IT

STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 5 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

Support team will keep a log of each review and its activity and provide the log to the IT manager.

5.8.1.1. The visitor must be a known and identified. A valid Organization-issued photo ID includes a driver's license, a state-issued photo ID or a passport may be included for further references before entering to facility under surveillance or control.

5.8.2. All visitors to the CCBRT critical areas must sign in using the Sign-In system form. They must enter their first and last name, their company and whom they are here to see including the visit date and purpose of visit, time in and out and kept to receptionist bench. Again, the visitors must sign out before leaving the building.

STANDARD OPERATING PROCEDURE		
Facility Physical Security and Access Control		
		Page 6 of 8
Document No: 006	Version:1.0	Relevant area: Academy, Facility, HEC, IT, Lab, MW and Security

COMPREHENSIVE COMMUNITY BASED AND REHABILITATION IN TANZANIA

P.O. Box 23310

Dar es Salaam – Tanzania

Tel: +225-699 990 002

Email: communication@ccbrt.org

Agreement Of Handing Key Card

Smart Key Card No: _____ **Handed Over to:** _____

User Department: _____

- 1. The recipient is responsible for this key**
- 2. It's not permitted to bring anybody without authorization (from line manager) to the secured facility locations**
- 3. The handover of the key to any other person is strictly prohibited.**
- 4. Displace or loss must be reported immediately to the line manager or program coordinator.**

User Signature: _____ **Date:** ____ / ____ / **20**

Line manager Name: **Signature:** _____

CCBRT Office Use only

Returned back by: _____ **Date:** _____

Received by: _____ **Date:** _____

Key Disabled: Yes / No

.....

