STANDARD OPERATING PROCEDURE		
User Domain Access Control SOP		Page 1 of 9
Document No: 009	Version:1.0	Relevant area: IT and all other departments

Author:

Written/Revised by: (Name, Position)	Signature:	Date:
Kennedy Malembo		18/01/2024

Approval cycle:

Reviewed by: (Name, Position)	Signature:	Date:
Alfred Kilamile		18/1/2024
Martin Ringia		10.1.2024

Authorized by: (Name, Position)	Signature:	Date:
Paul Kasanga (IBA Head)		18/01/2024
IBA Head		

Authorized by: (Name, Position)	Signature:	Date:
Rehema Ngamilo (COO)		18/1/2024

Document Change Control

Version	Changes	Name	effective date
1.0	New SOP	Kennedy Malembo	2024
1.1	Revised SOP		
1.2	Revised SOP		

1. Introduction

CCBRT as non-government institution, describe standards of operations when it comes to access of network infrastructures on its premises. The quality and security of information technology infrastructure is effective if access is limited and granted based on user privileges based on user roles.

The production information systems infrastructure is usually spread over several servers and include complex production chains with processing on all nodes, where access should be well managed to support efficacy of operations. It is thus, important to derive these standard operating procedures in aligning the qualities of domain access and services at CCBRT.

However, the same basic infrastructure is made available for both types of information systems, as described hereafter.

2. Purpose

The purpose of this SOP is to specify the steps that are required for obtaining domain/network access, user Identification (ID) and password maintenance, termination, and use.

3. Scope

This Procedure covers the unique user identification and password, emergency access, automatic log off, encryption and decryption, firewall, remote and wireless access procedures that will apply to new and/or existing computer systems/networks used within **CCBRT** to assure that such systems are accessed only by those persons or software programs that have been granted access rights under the CCBRT's Security Policy Information Access Management.

4. Requesting User Access

a. Obtain a User Creation, Deletion and Modification form from Information Technology (IT) office.

b. Fill in the information requested on the form.

c. Obtain designated Head of Department approval signature.

5. Receipts of Requests for User Access

Information Technology Officer

1. On receipt of the User Creation, Deletion and Modification form, review the document for acceptable completion, and process as follows:
   a. If all required fields are completed, sign and write the date received in the designated spaces on the form. Proceed to step 6.
   b. If required fields are not complete, notify the user requesting for access to refill the form, else discard the form and give the user a fresh form for filling.

6. Responsibility Action

Information Technology Officer

2. Determine the course of action for making requested changes as follows:
   c. If the request is for Termination of Access, proceed as directed in the "Termination of User Access" section of this SOP and complete the change immediately.
   d. If the request is for Change in Access, proceed as directed in "Granting/Changing User Access" section of this SOP.
   e. If the request is for New Access, proceed as directed in the "Granting/Changing User Access" section of this SOP.

7. Granting/Changing User Access

3. Determine a permanently unique User ID and check as follows:

Information Technology Officer

a. Check the User ID against the network Master ID Log.
   i. If the User ID is assigned to the individual and is on the Active Directory, continue to step 8(b).
   ii. If the individual is on the Active Directory, but with a different User ID, contact the Information Technology Manager immediately for investigation.
   iii. If the requested User ID is not unique, create a User ID according to the User ID Guidelines and document the new User ID

8. Information Technology Officer

iv. If the individual is not on the Active Directory, add the individual to the Active Directory.

v. If the request is for a name change, record the name change in the Active Directory.

b. Check the User ID against the application/network access log to determine if the User ID has access to the application/network.

i. If the User ID does not have access to the application/network, do the following and continue with step 8(c):

- Create the new user.
- Assign a temporary password.

ii. If the user ID does have access, do the following and continue with step

- Assign a temporary password
- Assign the access level listed on the Request Form

9. Information Technology Officer

c. Inform the User of the temporary password.

d. Control use of the temporary password as follows:

i. If the system is capable, require the password to be changed at first login.

ii. If the system is not capable of forced password changes, notify the User that the password must be changed within 2 business days of receipt of the temporary password and that passwords must adhere to Password Guidelines.

4. Notify the User that access has been granted.
5. Sign and date the Request form as completed.
6. File the request form.

10. Maintenance of access

User

7. Change the password every 90 days and adhere to Password Guidelines
8. The IT security team will have to check security logs every week based on the changes and execution performed by other super user on relevant areas of domain access and other critical systems based on agreed security tool. **Appendix i**

10.1.Information Technology Officer

9. Ensure system/network security as follows.

a) Disable access to users with expired passwords.

b) If the system has the capability, cause the system to lock the User ID after three (3) unsuccessful login attempts. The User ID may be unlocked after a few minutes or manually by the IT officer.

User

c) If the system has the capability, have the system do the following:

i. Request password changes every 90 days.

ii. Enforce password restrictions.

iii. Check for password reuse.

d) Ensure the User ID may not be logged onto two or more workstations simultaneously.

e) Complete access terminations immediately upon receipt of request.

10.2.User, User's Head of Department, or Designate

10. Complete a Request for Computer Access form and send it to Information Technology within three (3) business days of employee status change to change one or more of the following:

a) Access termination of a User that no longer needs access to a system or systems

b) User name change – Request a change in access and describe the reason for change.

10.3.Termination of User Access

10.3.1. System/Network Administrator or Designate

11. Eliminate the User's access from the system(s) identified on the User Creation, Deletion

Note: **Do NOT** remove the User information from the Active Directory.

12. Sign and date the Request form as completed.
13. File the request form.
14. Send an E-mail verification to the User's head of department that the requested access termination has been completed.

11. User ID Guidelines

User IDs shall be created according to the following Guidelines:

a. Format: User IDs shall be the User's first name dot followed by the User's last name. Example: Damas Aron user name should be **damas.aron.**

b. Permanently Unique, an acceptable User ID must be unique from any other User ID at CCBRT.

- Tie Breaker(s). Should two users have the same first letter and last name, User IDs shall be created using the first name, last name, and two (2) digit number sequences. Example: John.Doe, John.Doe01, John.Doe02

1. Network ID used. When granting access to a system or application, the user's network ID (User ID) will be used.

12. Password Guidelines

1. Passwords shall be established according to the following guidelines:
   a. Minimum Length: An acceptable password must have at least six (8) characters.
   b. Unique Characters: An acceptable password must have at least five (5) different characters.
   c. Character Repeat: An acceptable password must not repeat the same character more than twice consecutively.
   d. Character Types: An acceptable password must have characters from at least two (2) different character types – upper case, lower case, digits, etc.
   e. Password Content: An acceptable password shall NOT contain the first or last name of the User.
   f. Change Frequency: Passwords must be changed on a 90-day cycle.

13. Usage Guidelines

1. Passwords shall be used according to the following guidelines:
   a. Accountability: The user, to which the login and password are assigned, is responsible for all activity under that login and password.
   b. Password Confidentiality: Passwords should not be written down, transmitted to, shared with, or divulged to others Passwords may be given to the system/network administrator if deemed necessary and should be changed immediately after resolution.
   c. Electronic Signatures: Login and password combinations are equivalent to the user's hand written signature.

Revision Tracking

Ver. No.	SOP number and Title	Effective Date	Reviewed by	Reason for Revision
1.0	User Domain Access Control	2024	IT Department	Original version
1.1				
1.2				

SOP Acknowledgement log

By signing below, I acknowledge that I have received, read and intend to follow this SOP					
		Received		Read	
Name	Role:	Signature	Date	Signature	Date

Appendix i

System Name:				
Period: From Date:		**To Date:**		
IT Officer Name:		**Date:**		
#	**Admin Activity Log Audit**	**Y/N**	**Comments**	
1	Was there any new account created?			
2	If account was created, was the proper process followed?			
3	Any disabled/suspended account?			
4	If account was disabled/revoked, was proper revocation process followed?			
5	Was there password reset for user account?			
6	If account was reset, provide *Helpdesk Ticket*			
7	Any other admin activity observed. *Specify*			

	Name	**Signature**
Checked by (IT Officer):		
Reviewed by (Team Lead):		
Approved by (HoD)		