**Local Administrator Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |

Table of Contents

**WHO ARE THE LOCAL ADMINISTRATORS? 4**

**WHAT ARE THE FUNCTIONS OF LOCAL ADMINISTRATORS?** **4**

**AREAS TO BE MONITORED 4**

**BREACHES IN SECURITY CONTROLS 5**

**REFERENCES 5**

***ENFORCEMENT 5***

**APPENDIX 1: LOGICAL ACCESS CONTROL 6**

Objective 7

Focus Area 7

Administrator IDs 7

ID Standards 7

IS Maintenance 7

**APPENDIX 2: PHYSICAL SECURITY CONTROL 9**

Objective 10

Focus Area 10

**APPENDIX 3: COMPUTER OPERATIONS 12**

Objective 13

Focus Area 13

**APPENDIX 4: CHANGE AND CONFIGURATION MANAGEMENT 14**

Objective 15

Focus Area 15

**APPENDIX 5: MANAGEMENT OF IDs KEPT UNDER CUSTODY 16**

Introduction 17

Definition of IDs under Custody 17

Who are ID custodians? 17

What are the duties of a custodian? 17

Management of IDs under custody 17

Control of IDs 18

Approval form18

Request for password form 19

1. **WHO ARE THE LOCAL ADMINISTRATORS?**
	1. Local Administrators refer to the security administrators of localized systems
	2. Local Administrators will be authorized persons appointed by the organization e.g. Assistant Branch Manager/ Sales & Service Manager, all Centre Managers (TFC, CAC, LMC, LOC, ZCBC, SSC, Cheque Processing Centre etc. or any future centres to be set up)
	3. He/she may delegates this responsibility to another senior officer but accountability shall still rest with him/her
	4. Local systems refer to all systems not centrally controlled by Organization's Information Systems Division (ISD)
2. **WHAT ARE THE FUNCTIONS OF LOCAL ADMINISTRATORS?**

The Local Administrators will be responsible for: -

* 1. Ensuring that information security requirements are implemented in their respective sites
	2. The administration of logical and physical access controls for computerized information systems and monitoring access violation access reports
	3. Providing guidelines and procedures to achieve consistence practices and complying to the Organization’s security standard
	4. Ensuring audit compliance and security controls are met on an on-going basis.
1. **AREAS TO BE MONITORED**

The security administration of the following areas comes under the jurisdiction of the Local Administrators: -

* 1. **Logical Access Controls (Appendix 1)**

The objective is to enforce segregation of duties by ensuring individuals can only access data and perform processing to which they have been authorized

* 1. **Physical Security Controls (Appendix 2)**

The objective is to prevent unauthorized access to computer related equipment and to ensure that the computer related equipment is adequately protected against natural hazards and malicious damage.

* 1. **Computer Operations (Appendix 3)**

The objective is to ensure that operational procedures are adhered to. These operational procedures are to ensure the continuity of processing, minimizing the risk of disruption to computer services and to ensure that jobs are processed in an authorized manner

* 1. **Change and Configuration Management (Appendix 4)**

# The objective is to ensure a means of identifying and controlling the modification of individual components items that together constitute the local system

* 1. **Management of Ids Kept Under Custody (Appendix 5)**

# The objective is to provide a guideline on those critical Ids to be kept by an appointed custodian (e.g. Branch Manager, Heads of Department and Local Administrator) to ensure back-up for continuity of organizationing operations/services

1. **BREACHES IN SECURITY CONTROLS**

IS Local Administrator is to ensure branch conform to the Organization’s security standard. Any security breach and unsatisfactory audit rating in computer security will be taken into consideration in their performance appraisal.

1. **REFERENCES**

The following documents will be relevant: -

- Logical Access Controls

- Physical Security Controls

- Computer Operations

- Change and Configuration Management

- Management of IDs Kept Under Custody

- Information Systems Security Policy

1. ***ENFORCEMENT***

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
	2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***

Appendix 1

**Logical Access Control**

1. **OBJECTIVE**

To enforce segregation of duties by ensuring individuals can only access data and perform processing to which they have been authorized.

1. **FOCUS AREA**

There are three main areas of focus: -

Administrators Ids

ID Standards

ID Maintenance

* 1. **ADMINISTRATOR IDs**
		1. Administrators privileges will only be given to authorized persons appointed by the organization
		2. The number of IDs with administration privileges must be limited to 2 for each locations
		3. The name of the primary administrator and secondary administrator must be properly documented
		4. Default passwords for Administrator IDs must be changed to be unique and know only to the IS Local Administrators
		5. Under no circumstances shall the administrator share his or her IDs with anyone without proper hand over process
		6. Any modification performed by the Administrator IDs will be deemed done by the administrator unless proven otherwise
	2. **ID STANDARDS**
		1. All IDs issued on IBM mainframe must comply with Organization's ID naming convention, i.e. the MEMO ID naming convention
		2. This is to ensure each staff will only have 1 ID and facilitate the housekeeping process when the staff is transferred, resigned or retired
		3. All IDs issued on non-mainframe platform should be issued according to the standards agreed upon for the system or application
	3. **IS MAINTAINANCE**
		1. **Removal Of Ids**

All means of access (IDs, Password, Magnetic Smart Card) to information kept on the computer systems shall be taken away from every staff who has tendered his/her resignation or whose services has been terminated.

* + 1. **Segregation Of Duties**

Administrators must ensure that IDs given to staff has no conflict or incompatible with their actual duties of the staff, e.g. clerk given ID with manager or officer privileges.

* + 1. **Overlapping Of Functions**

All privileges given to ID must be revoked or review when the owner is assigned new functions. This is to prevent overlapping of function where a staff assigned to JOB B still have special privileges to do JOB A.

* + 1. **Transfer Of IDs**

IDs given are meant for the owner only. Therefore IDs must not be allowed to be passed down from a resigned, transferred or retired staff to an existing staff without first reviewing the access given to the ID and changing the name of the ID's owner.

* + 1. **Sharing Of IDs**

All IDs must have an owner. Under no circumstances should IDs be shared. Even if IDs are required for a certain functions that will be use by a group of people, the group leader will be made owner of the ID. This is to ensure accountability for usage of all IDs issued by Organization.

* + 1. **Development Or Test Ids**

All IDs that were used in the development and the testing of a system must be removed once the exercise in completed. Only IDs that are relevant for the production system are allowed to reside in the production environment.

* + 1. **Matrix For Ids**[[1]](#footnote-1)

All IDs in the system must be given according to the predefined ID matrix. Any changes in ID functions must be updated onto the matrix for IDs. User Access Matrix must be endorsed by management.

* + 1. **User ID Register**

For IDs which user profiles do not contain the name and PF number of the staff, a "User ID Register" must be, maintained. The following particulars must be recorded: -

* + - 1. Name of staff
			2. PF number of staff
			3. Date issued (of ID)
			4. Date receipt (of ID)
			5. Acknowledged receipt by staff
			6. Acknowledged return by staff

***Note:***

*This register is to ensure non-repudiation.*

Appendix 2

**Physical Security Control**

1. **OBJECTIVE**

To prevent unauthorized access to computer related equipment and to ensure that the computer related equipment is adequately protected against natural hazards and malicious damage.

1. **FOCUS AREA**

There are three main areas of focus: -

* 1. **Physical Access To Computer Room**
		1. Each site must have a computer room to store critical computer related equipment, e.g. server, UPS, modems, etc.
		2. Computer room must be locked at all times.
		3. Keys to the computer room must be held by the IS Local Administrator.
		4. The administrator must ensure all staff accessing the computer room must register themselves in "Entry Register Book" before access is given.
		5. Access to the computer room by non-staff must be controlled to ensure that: -
			1. they are bona fide staff of the contractor
			2. they have been authorized by the contractor
			3. they have been approved by the relevant heads of department
			4. they are escorted by a member staff
		6. Entry Register Book" must contain the following: -
			1. Name of visitor
			2. Purpose of visit
			3. In time
			4. Out time
			5. Date
			6. Signature of visitor
	2. **Power Supply**

Administrators must ensure that there is an uninterrupted power supply (UPS) or battery back up for the critical servers.

UPS must be subjected to periodical maintenance and testing.

* 1. **Control Of Storage Media**
		1. Storage media, e.g. diskettes, tapes, etc. must be kept in a secured and preferably fire proof area.
		2. Access to storage media must be controlled and only granted to authorize staff.
		3. Movement of storage media in and out of storage must be logged.
		4. The logged must contain the following information: -
			1. Name of storage device
			2. Date
			3. Purpose of withdrawal
			4. Withdrawal time
			5. Deposit time
			6. Name of staff
			7. Authorized signature

Appendix 3

**Computer Operations**

1. **OBJECTIVE**

The operational procedures are to ensure continuity of processing, minimising the risk of disruption to computer services and to ensure that jobs are processed in an authorised manner.

1. **FOCUS AREA**

There are three areas of focus: -

* 1. **Backup Storage Media Protection**[[2]](#footnote-2)
		1. Copies of backup files must be kept in the storage area once the backup process is completed.
		2. Storage media must be properly labelled to identify the contents.
		3. Centralised inventory listing of all storage media must be maintained by the administrator.
		4. Inventory check must be done annually and tested to ensure it is in working condition.
		5. Monitoring movement of storage media.
	2. **Frequency And Retention Of Backups**
		1. Administrators must ensure that all backups and done regularly at the appropriate intervals.
	3. **Recovery And Restart**
		1. Administrator must be aware of escalation procedure in the event of system failure.
		2. Recovery and restart procedures must be properly understood and documentation stored got easy retrieval.
		3. Administrators must ensure the backup media that would overwrite existing production fact must be obtained from Data Owners.

Appendix 4

**Change and Configuration Management**

1. **OBJECTIVE**

To ensure a means of identifying and controlling the modification of individual components items that together constitute the local system.

1. **FOCUS AREA**

There are four main areas of focus: -

* 1. **Change Management Authorization**
		1. The administrator is to ensure the following information before allowing any changes to be made to their local systems: -
			1. What is to be change
			2. Description of change
			3. Who has authorized the change
			4. Impact of change
	2. **Change Implementation**
		1. The administrator should get the following from the change agent: -
			1. A sign-off from the change agent that the implementation of the change is successful
			2. Problem management procedure in case of complications caused by change
	3. **Change Management For Third Parties**
		1. The administrator should ensure the following: -
			1. The third party formally schedules and communicate all deliveries
			2. Proof that prior acceptance of the change has been approved by Information Systems Division (ISD).
	4. **Configuration Management**
		1. The administrator should ensure: -
			1. No configuration for computer equipment is change without prior approval by ISD
			2. Confirmation if any changes has been made to the configuration of the server after a change exercise.
			3. That documentation for server configuration is up to date.

***Caution:***

*Under no circumstances should the administrator change the configuration of systems without prior approval.*

Appendix 5

**Management of IDs Kept Under Custody**

1. **INTRODUCTION**

This guideline provides a standard on which user IDs under custody should be maintained.

1. **DEFINITION OF IDs UNDER CUSTODY**

IDs kept under custody refer to IDs kept by a trusted person who is known as the custodian. Custody IDs are not used by the custodian but rather held by the custodian for safekeeping.

1. **WHO ARE ID CUSTODIANS?**

Custodians can be anybody who is accountable for IDs given to them for safekeeping. This include Branch Managers, Head of Departments, Local Administrators, etc.

1. **WHAT ARE THE DUTIES OF A CUSTODIAN**

The custodians of IDs must ensure the confidentiality, integrity and availability of the IDs.

* 1. Confidentiality

Password must not be known to anyone except the custodian. Once password is exposed it must be changed immediately.

* 1. Integrity

IDs must be properly labelled and updated to ensure accuracy of its password

* 1. Availability

The custodians must ensure that passwords held by them are available for use as and when needed. Therefore, all custodians should have a backup in case of emergency.

1. **MANAGEMENT OF IDS UNDER CUSTODY**

The following guidelines must be enforced for all IDs under custody:

* 1. Storage of IDs
		+ 1. Passwords of IDs must be stored in a secured area. Secured area is defined as a place where access to the area is controlled.
			2. Password should be stored in compartmentalised method so that exposure of one password will not jeopardise the others. One way of compartmentalising passwords is storing the password in a sealed, signed, labelled and dated envelope.
	2. Divulgence of password
		+ 1. When a password for an ID is required, proper approval must be obtained before divulging such passwords. Approvals must be documented.
			2. All passwords divulged must have issuance date and expiry date recorded. On the expiry date it is the duty of the custodian to revoked the password.
			3. After divulging a password, the administrator must change the password once the ID is returned.
			4. Change of password is documented and updated.
	3. Availability of IDs
		+ 1. The custodian must ensure the availability of IDs at all times. If the custodian is going to absent for a period of time or permanently, controls of the passwords must be handed over to the relieve officer.
			2. Handling over of the custody of IDs must be documented and approved.
			3. For critical systems, the passwords must be available at all time.
1. **CONTROLS OF IDS**

Every time a password is divulged, the following information must be documented:

* + - 1. Name of the requester
			2. PF number of requester
			3. Date issued
			4. Date returned
			5. Acknowledge received by custodian
1. **APPROVAL FORM**

Where possible, approval should be via CHANGE. Where such facilities are not available, the REQUEST FOR PASSWORD form should be used.

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)