**Policy on General Systems Security and**

**Controls on IDs and Password**

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** |
| 1.0 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

**SECURITY PROFILE 3**

**USER ID AND PASSWORD 3**

**POWERFUL ID 5**

**USER ACCESS MATRIX 6**

**USER ID PROFILE 7**

**AUDIT TRAILS 8**

**SYSTEM CONTROL 9**

**ENFORCEMENT 10**

**Description:** This policy is to provide the minimum security requirements for system security and controls on Ids and passwords*.*

1. **SECURITY PROFILE**

For proper security control, the following must be adhered: -

* 1. Access to the system is controlled through assigned user IDs and user controlled passwords.
	2. The set-up of security profile is under control of the Security Administrator for assigning and changing the access capabilities of each user.
	3. Security Administrator is not allowed to assign functions to himself/herself.
	4. Creation of any user security records must be approved at least by the Branch Manager or Department Head before these security records can be activated.
	5. Access control is based on function set-on in security profile.
	6. Each function can be controlled and assigned individually to specific user and terminal.
1. **USER ID AND PASSWORD**

The following is Organization's standard for user IDs and passwords: -

* 1. **Sessions Limit: 1**

Users are not allowed to sign-on to more than one terminal at a time. Users must log-off from one terminal in order to sign-on to another terminal.

* 1. **Duplicate Password Control: Minimum 3 Generations**

Users are not allowed to reuse any passwords that have been previously employed in the last 3 password changes.

* 1. **Maximum Password Expiration Interval: 60 Days**

Password expiry interval must not be more than 60 days.

* 1. **Minimum Password Length: 8**

Password length must be at least 8 characters.

* 1. **Last Sign-on Information Display**

The system must display the last sign-on information after a successful sign-on.

* 1. **Input Field For Password Must Be Blinded**

The input field for password must not be visible while the users type in their passwords.

* 1. **Password Must Not Be Stored In The Clear**

The password stored must be encrypted or masked.

* 1. **First Time Sign-on Password Must Be Forced Changed**

The system must force the users to change their initial password. Security Administrators must instruct their users to change their IDs’ default passwords immediately upon receipt.

* 1. **Passwords Are Strictly Private And Confidential**

No one (including Security Administrators) may know the users’ passwords.

* 1. **Maximum Time-out Interval: 15 Minutes**

User IDs which are inactive for 15 minutes must be logged-off from the system.

* 1. **Maximum Unsuccessful Sign-on Attempts: 3**

Users will be allowed 3 consecutive unsuccessful sign-on attempts after which the IDs should be revoked by the system.

* 1. **Restriction By Specified Date And Time Is Allowed**

Restriction of access using specified date and time is allowed where applicable.

* 1. **Changing Of Passwords Without Assistance**

Users can change passwords as and when required without assistance from Security Administrators. Users must ensure that all passwords are promptly changed if the password or system is suspected of being compromised.

* 1. **Passwords Composition**

Users are not allowed to use easy to guess passwords. Users are encouraged to use mnemonics (first letter of each word in a phrase, poem, song, etc.) when creating a password.

Passwords composition must include at least 1 number, 1 special character, 1 upper and 1 lower case alphabet characters. Security Administrators must not use easy to guess passwords or default passwords when resetting IDs, e.g. default password the same as ID or ‘PASSWORD’. These controls should be system enforced where possible.

* 1. **Passwords and ID Must Not be the Same**

Users are not allowed to use password to be the same as their ID. This rule should also include in the system.

* 1. **Multiple Level Of Access Is Allowed**

User IDs may be assigned different levels of transaction limit or access for overriding purposes.

* 1. **Maximum Dormant Period: 30 Days**

IDs that have been dormant or inactive for 30 days must be revoked.

* 1. **Inactive ID for more than 90 days must be deleted**

IDs that have been dormant or inactive for 90 days must be deleted. Where possible, the feature should be automated in the system else the procedure should be in place to document the process.

* 1. **Powerful (Super) ID usage**

Usage of powerful IDs and passwords must be minimised and properly authorized and must only be made at dedicated terminal located in a physically secured area.

* 1. **Backup powerful (Super) ID**

Backup copies of passwords for powerful IDs must also be logged and kept secured.

**Note:**

Due to operational constraint, the system administrator ID (powerful/super ID) and system ID (with no user login)password will be allowed to have no expiry period. However, the password for powerful/super ID must be changed when the custodian of the ID resigns or is transferred.

* 1. **Standard Naming Convention**

All IDs created should follow mainframe ID naming convention.

1. **POWERFUL ID**
	1. A Powerful ID has the following characteristic: -
		* 1. It has full administration functions to a system, application, database, security system (as defined by IT Security) or network devices.
			2. It comes by default with a system, application, database, security system or network devices.
			3. It is created by design as a powerful ID for a customised system, application, database, security devices or network devices.
			4. It has the ability to over-ride settings made by any other IDs.
	2. Powerful IDs must be under the control of authorized custodians. These custodians can be an individual or an organizational unit that has been endorsed by IT Security.
	3. The Group's standard for custodian of Powerful IDs is as follows: -

|  |  |
| --- | --- |
| Powerful IDs | Custodians |
| Centralised Systems | Decentralised Systems |
| Operating System | Security Administrator | Appointed Executive |
| Database | Security Administrator/ Business Owner/Data Owner | Appointed Executive |
| Application | Security Administrator/ Business Owner/Data Owner | Appointed Executive |
| Security Systems | Security Administrator | Appointed Executive |
| Network Devices | Network Administrator | Appointed Executive |

* 1. In the event where there may be more than one party eligible as the custodian for a Powerful ID, IT Security will be the ultimate decision maker.
	2. Appointment of custodians for Powerful IDs must comply with the following conditions: -
		+ 1. They must not be system engineers, application administrators or database administrators.
			2. They must be endorsed by management and IT Security.
	3. The custodians may be one of the following parties: -
		+ 1. The security administrator of the organisation.
			2. The business owner of the system.
			3. An executive endorsed by management and IT Security.
	4. The custodians are responsible for the administration of Powerful IDs. Proper procedures and process must establish and endorsed by the custodian. This process must be endorsed by management and IT Security.
	5. The procedure for handling of Powerful IDs must cover the following issues: -
		+ 1. Who is the custodian of the Powerful ID?
			2. Who is the backup if the custodian is not available?
			3. Where will the Powerful ID be stored?
			4. When can an administrator request access to a Powerful ID?
			5. How can an administrator request for access to a Powerful ID?
			6. Who shall review the activity logs of Powerful IDs?
			7. How long is the duration for an administrator to have direct access to the Powerful ID?
			8. What is the process of requesting access to a Powerful ID during an emergency?
	6. Powerful IDs must not be used for daily operations. Administrators should be assigned individual IDs with similar access to carry out their operational functions.
1. **USER ACCESS MATRIX**
	1. Access to information, and business processes should be controlled on the basis of business and security requirement based on the “need to know” and “need to do” principle.
	2. Formal procedures must be in place to control the allocation of access rights to information systems and services.
	3. An access matrix is a document that: -
		* 1. Describes relationship between a technical function of a system and a job function of a user.
			2. Creates a relationship between the user identity and the technical function of the system.
			3. Helps ensure segregation of duties when assigning privileges.
	4. An access matrix consists of: -
		* 1. A list of objects;
			2. A list of subjects;
			3. A list of "Access Rights".
	5. A list of objects may be one of the following: -
		* 1. Files, directories, datasets, etc. within an operating system.
			2. Fields, objects, functions, etc. within an application system.
			3. A combination of application and operating system resources.
	6. A list of subjects refers to the list of user groups.
	7. Example: Table 1 shows the access matrix for an application system.
		* 1. The list of subjects is: Manager, Officer and Clerk.
			2. The list of objects is: Address, Telephone Number and Address.
			3. The list of access is: Add, Modify, Delete, View and Approve.

| Subjects | Objects | Access Rights |
| --- | --- | --- |
| A | M | D | V | Ap |
| Manager | Address |  |  |  |  |  |
| Telephone Number |  |  |  |  |  |
| Account Number |  |  |  |  |  |
| Officer | Address |  |  |  |  |  |
| Telephone Number |  |  |  |  |  |
| Account Number |  |  |  |  |  |
| Clerk | Address |  |  |  |  |  |
| Telephone Number |  |  |  |  |  |
| Account Number |  |  |  |  |  |

Table 1: Access Matrix for Customer Profiling Application System

* 1. The access matrix must be maintained and owned by the end users.
	2. At the minimum, management at the departmental level must endorse the access matrix.
	3. The access matrix must be updated to reflect any changes in subjects object and access matrix.
	4. The departmental head must approve changes made to the access matrix. All changes must be communicated to the system engineers. System engineers must comply with the access matrix.
	5. The access matrix should be reviewed at least once every six months or whenever there are changes.
	6. All information technology systems within the Group must have an access matrix. Non-compliance to this requirement may lead to downgrading of audit rating.
1. **USER ID PROFILE**
	1. A user profile refers to the relationship between a user ID to a function within an application or system.
	2. A User ID Profile must at least contain the following information: -
		* 1. User ID
			2. Functions
	3. The functions in the User ID Profile refer to the operation an application or system can perform.
	4. The ID administrator must maintain a list of User ID Profile. The ID administrator must be able to advise and explain to the end users on any access right matters relating to the User ID Profile.
	5. It is the responsibility of the ID administrator to schedule and initiate a review of the User ID Profile at least once a year. This review will be conducted by the end users. The review is to ensure: -
		* 1. IDs of staff that have resigned, transferred or terminated have been removed.
			2. Accesses provided to all staff are according to the access matrix.
			3. There are no differences of access between staff that are performing the same job function.
			4. Any discrepancies in the User ID Profile are reported to the ID administrator and rectified accordingly.
	6. The list of User ID Profile may be stored in the following format: -
		* 1. Hardcopy
			2. Softcopy
			3. Report generated.
	7. If the User ID Profile is in softcopy or report generated, it must be able to be presented in hardcopy format as and when required.
	8. User ID Profile must be made available to the end user as and when requested.
2. **AUDIT TRAILS**

Audit trail of security-sensitive access and actions taken should be logged. All forms of audit logs should be appropriately protected against unauthorized modification or deletion.

Audit logs for system and other security-relevant events should be kept for an agreed time period as it might assist in future investigations and access control monitoring purposes. Procedures on the review of audit log files or exception reports should be formulated for timely remedial action on security violations and management reporting.

All systems related processing clocks should be synchronised with an agreed time source to ensure the accuracy of audit logs.

The relevant information such as date, system date, time, sequence number, user ID, workstation ID, program completion status and transaction / process type should be provided in the following audit logs: -

* 1. **File Activity Log**

Records all activities to any files in the system.

* 1. **User Activity Log**

Records all activities performed by the users.

* 1. **Change Log**

Shows the original and updated information of records that have been changed.

* 1. **System Log**

System audit logs should be adequately activated. System functions such as start-up, shut-down, end-of -day, back-up, recovery, etc. must be recorded.

* 1. **Illegal Access Log**

Records all unsuccessful and unauthorised attempts to gain access to the system.

Should the system be unable to provide the relevant audit logs, then compensating measures should be implemented at application level.

All audit logs must be kept consistently on a fixed retention period to facilitate investigation, later if any at least a year.

1. **SYSTEM CONTROL**

The following controls should be considered for all systems to be implemented or are already running.

* 1. Controls to the loss of data or non-processed data.
	2. Controls to assure the completeness of data such as batch totals and hash totals.
	3. Controls to assure the accuracy of input such as existence check, check digit, format check, reasonableness check, conditional code check, priority check, etc.
	4. Controls to assure transactions are posted to the proper records.
	5. Controls to assure that all transactions have been properly authorised.
	6. All systems related processing clocks are synchronised with an agreed time source to ensure the accuracy of time stamps.
	7. Detection and correction of errors.
	8. Access to a specific record limited to one transaction at a time and prohibition of concurrent updating of a record.
	9. Cryptographic options that help to provide an additional level of security to protect the sensitive financial data.
	10. The operating system should provide security against unauthorised access to the system files, databases and programs.
	11. Auto log-off based on pre-set time period.
	12. Automatic assignment of sequence number for each type of input / transaction.
	13. Controls to assure complete data security and integrity when sending or receiving data.
	14. Networking management facility to monitor links and devices, error reporting, control and capture of statistical data.
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 Company’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 Company 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.