Central Depository & Settlement Co. Ltd

IT Security Policy

Version Control	
Document Title:	IT Security Policy
Version Number:	15.0
Approved by:	Audit Committee – 05/05/06 Board of Directors - 05/06/06
Document Review Date:	31/05/22
Document Expiry Date:	30/11/22
Confidentiality:	Low
Integrity:	Medium
Availability:	Medium

Authorised Signature:

Name: Vipin Mahabirsingh **Position:** Managing Director

Signature: **Date:** 31/05/2022

Document History

Version No.	Date	Description of the change	Author	Approved by:
1.0	03/04/06	Initial Document	MS/VM	Audit Committee/ Board Members
2.0	01/10/07	Change of appellation of the following document: Software and Systems Change Management Procedure	MS	VM
3.0	30/04/08	Section 11 (e) - Access Control	MS	VM
4.0	15/02/09	Check-List of security controls (based on ISO 27001) implemented at SEM/CDS	MS	VM
5.0	16/03/09	File Encryption	MS	VM
6.0	31/12/09	Acceptable Internet Use Policy Desktop Security Policy Data Protection	MS	VM
7.0	28/02/11	Backup of PCs – External Hard Disk included	MS	VM
8.0	31/12/11	Document Classification	MS	VM
9.0	30/06/12	New Documents: Scope of ISMS and Business Contingency Planning Policy	MS	VM
10.0	29/03/13	Physical Access Monitoring :CCTV and Door Access Control Device	MS	VM
11.0	15/04/14	Use of Email Policy	MS	VM
12.0	30/06/14	Centralized Backup of PCs and File Encryption	MS	VM
13.0	10/04/15	Wireless Internet Connection	MS	VM
14.0	07/06/16	IT security policy realigned to the new ISO 27001:2013 standard	MS	VM
15.0	31/05/22	Work From Home Policy	MS	VM

1. Information Security Policies

This document defines the responsibilities relating to the management of the Information Technology (IT) systems of the Central Depository & Settlement Co. Ltd (CDS) and the procedures to be followed by employees of the Central Depository & Settlement Co. Ltd as well as by remote users (investment dealers, custodian banks, Financial Services Commission, Bank of Mauritius and registries) when using the IT systems of the company. It is the responsibility of each employee or the remote user to ensure the integrity and confidentiality of data that the employee or the remote user processes or has access to, using the IT systems of the CDS.

An employee who violates any of the procedures contained in this document may be subject to disciplinary action. The CDS may suspend access of an employee or a remote user to its IT systems at any time for technical reasons, violations of security procedures, or other concerns. The IT Security Policy has been realigned to the new ISO 27001:2013 standard and a user guideline has been prepared to facilitate end users in abiding the IT Security Policy.

This document has been approved by the Audit Committee and Board of Directors on 5th May 2006 and 5th June 2006 respectively. The IT Security Policy shall to be reviewed every six months or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

2. Organization of Information Security

The Systems Manager is responsible for the management of the IT systems of the Central Depository & Settlement Co. Ltd (CDS). The Systems Manager is also responsible for the IT function of the Stock Exchange of Mauritius Ltd (SEM) which includes the technical management of the Automated Trading System (ATS). SEM and CDS have signed an IT Outsourcing Agreement where the service provided by CDS is clearly defined.

Investment dealers, Custodian Banks, the Financial Services Commission, the Bank of Mauritius and Company Registries use the same network and telecommunications lines to access the ATS and CDS systems. The engine of the Automated Trading System (ATS) runs on separate servers on the same network.

SEM and CDS have a common Disaster Recovery Plan (DRP) to cater for various possible scenarios.

A policy and supporting security measures has been adopted to manage the risks introduced by using mobiles devices such as laptop and mobile phone pertaining to the company in unprotected environments. When using mobile devices, special care should be taken to ensure that business information is not compromised.

Systems Management and Documentation

The following set of technical documents relating to the IT systems of the CDS should be maintained by the Systems Manager:

- Scope of ISMS for SEM/CDS
- Description of the IT Environment
- Business Contingency Planning Policy
- Disaster Recovery Plan (including backup strategy for CDS system)
- Implementation Procedures for IT Security Policy
- Guideline to facilitate end users in abiding the IT Security Policy
- System/Security Routine Task and Verifications
- Check-List of security controls (based on ISO 27001) implemented at SEM/CDS
- IT Incident Management Policy
- Asset Classification, Risk Assessment and Business Impact Analysis
- CDS Systems Administration Procedures
- Application Software and Systems Change Management Procedure
- Disk Mapping
- Backup and Recovery of Accounting System
- UPS, Electrical, Data and Telephone Cabling and Installation
- Fire Detection and Extinguisher

The set of technical documents may be common to both CDS and SEM since both the ATS and CDS systems run on the same network and share most resources.

The management of the different components of the systems should be done in accordance with the above documents and this should be verified by external auditors on a regular basis.

The responsibilities of the Systems Department of CDS in relation to the security of the IT systems of the SEM are covered in the IT Security Policy of the SEM.

Employees of the CDS should address any request for technical support to the Systems Manager.

3. Human Resource Security

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics. All employees shall read the IT Security Policy of the company and agree to abide by it.

All employees of CDS as well as Investment Dealers, Custodian Banks and Company Registries shall receive appropriate awareness education and training and regular updates on the policies and procedures.

4. Asset Management

All assets are inventoried and the inventory is frequently updated. Information such as type and details of asset, vendor details, and maintenance contract may be found.

All information assets of CDS have a designated owner. Information owners are responsible for classification of asset, authorizing access to that information asset, and specifying and implementing (where possible) security requirements needed to protect the asset.

The critical level gives direction about the control procedures to be implemented for appropriate level of security for that asset. The criticality level also helps in focusing attention on the more critical assets for more stringent security, monitoring and budgeting.

Information asset owners use the following matrix to classify information asset

Class	Description
Highly Critical	Information of the highest sensitivity, which if mishandled or disrupted may cause substantial damage to CDS.
Moderate Critical	Information of the highest sensitivity, which if mishandled or disrupted may cause moderate damage to CDS.
Low Critical	Information of the highest sensitivity, which if mishandled or disrupted may not cause any damage to CDS.

Information assets are clearly labelled where appropriate.

Recovery Time Objective (RTO) is the period of time that the business can sustain without the asset being available. The business will start suffering major losses after this period. RTO helps in framing the Recovery architecture, finalizing the list of assets to be recovered with priority and budgeting.

Risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk.

Document Classification

The valuation and classification of information in a document shall take into account the Confidentiality, Integrity and Availability requirements of the company and its processes whether they are used. These following requirements shall define the criticality of the documents for the business and its processes and be used in defining the business resumption plan and / or disaster recovery plans:

Confidentiality of information refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing organization security to the disclosure of private data of employees. The table below provides guideline to determine Confidentiality requirements:

Confidentiality Requirements	Explanation
Low	Non-sensitive information available for public disclosure. The impact of unauthorized disclosure of such information shall not harm the organization anyway.
Medium	Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a limited harm to the organization.
High	Information which is very sensitive or private, of highest value to the organization and intended to use by named individuals only. The unauthorized disclosure of such information can cause severe harm.

Integrity refers to the completeness and accuracy of Information. Integrity is lost if unauthorized changes are made to information in the documents by either intentional or accidental acts. If integrity of information is not restored back, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions. Integrity criteria of information can be determined with guideline established in the following table:

Integrity Requirements	Explanation
Low	There is minimal impact on business if the accuracy and completeness of information/data is degraded.
Medium	There is significant impact on business if the asset if the accuracy and completeness of information/data is degraded.
High	The Integrity degradation is unacceptable.

Availability indicates how soon the information is required, in case the same is lost. If critical information is unavailable to its end users, the organization's mission may be affected. Following Table provides guideline to determine availability criteria of information assets.

Availability Requirements	Explanation
Low	There is minimal impact on business if the asset/information is not available for up to 7 days
Medium	There is significant impact on business if the asset / information is not available for up to 48 hours
High	The Asset / information is required on 24x7 basis

Disposal of Media

All items of equipment containing storage media should be verified by the Systems Department to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

5. Access Control

The following procedures regarding access control must be followed:

a) Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times. User rights shall be determined by the Managing Director.

b) Users requiring access to the IT systems must make a written application on the forms provided by the Systems Department. The application must be approved by the Managing Director of the CDS prior to submission to the Systems Department.

c) Access to the network/servers and systems will be by individual username and password.

d) Usernames and passwords must not be shared by users.

e) Usernames and passwords should not be written down, except for the system administrator. Network/server/database administrator passwords will be known only to the Systems Manager and the two IT Officers. These passwords will be stored in a sealed envelope in a secure location in the Systems Department and will be accessed by the Managing Director or an authorised person only in case of an emergency or disaster or when the passwords are changed.

f) All users will have an alphanumeric password of at least 8 characters.

g) Users must change their passwords every 30 business days and must be unique. System administrator passwords must be changed at least 3 times a year.

h) The Finance and Administration Manager must inform the Systems Manager of any employee leaving the organisation's employment. The Systems Department will then remove the employee's access to all systems.

i) The Managers of stock broking companies, custodian banks, FSC, Bank of Mauritius and registries must inform the Systems Manager of any user leaving their organisation. The Systems Manager will reset the password of the relevant organisation and the latter will then change the password again.

j) Default passwords on systems such as Oracle must be changed immediately after installation.

6. Cryptography

Files such as Entitlement Schedule and Allotment Schedule are exchanged between the CDS and Company Registries on a regular basis via email or diskette. These files contain confidential data. In order to ensure the security of these data, all files that are exchanged between the CDS and Company Registries should be encrypted.

Furthermore, McAfee DLP Endpoint will be enabled on all PCs and laptops at SEM and CDS. This feature will allow only approved external storage devices to be connected to these PCs and laptops. Furthermore data on these approved external storage devices will be encrypted.

7. Physical and Environmental Security

Access to the data center should be strictly restricted to the Systems Manager, IT Officers and the Managing Director of CDS. Any intervention by suppliers should be made in the presence of at least one of the above persons. The intervention should be logged into an Intervention Form. Other persons may have access to the data center if they are duly authorised by the Managing Director of CDS and accompanied by at least one of the above persons. Note that access to the data center is monitored and logged by CCTV and door access control device respectively.

An employee should not allow other employees to use his/her PC unless authorised by his/her immediate supervisor to do so. Other persons are strictly prohibited from using the IT

systems of the CDS, except stock broking companies, custodian banks, FSC, Bank of Mauritius and registries for operations relating to the CDS.

Stock broking companies, custodian banks, FSC, Bank of Mauritius and registries should not allow unauthorised persons to have access to the computers and network equipment that are connected to the CDS/SEM network.

8. Operations Security

Procedures

Access and use of the CDS system by employees of CDS and by stock broking companies, custodian banks, registries, the Financial Services Commission (FSC) and the Bank of Mauritius should be in accordance with the CDS Rules and Procedures.

Change Management

CDS has also implemented and follow an Application Software and Systems Change Management Procedure to cater the following:

1. Requests for enhancement or new requirements
2. Change in CDS Procedures
3. Bugs encountered while operating the system

Backup

Backup of important documents and data on all PCs of the CDS should be performed automatically on a weekly basis (daily where necessary) and a copy of the backup should be kept offsite. SEM/CDS uses a centralized backup mechanism (Veritas Desktop and Laptop Option (DLO)) to automatically backup domain users working files. This tool will be scheduled on a weekly basis (daily where necessary) to automatically encrypt the folders "My Documents" on each PCs and laptops and then send the encrypted backup file to the Domain Server of SEM and CDS. The encrypted backup files for each user of SEM and CDS will be centrally backup on tapes and will be kept offsite. Note that the password of the encrypted backup file will be known by the corresponding user ONLY. SEM/CDS uses Microsoft O365 for emails and emails are backup on cloud.

Technical Vulnerability Management

Vulnerability assessments are performed by the IT team using scanning tools on a quarterly basis and appropriate actions are taken accordingly. A network monitoring tool has also been implemented to further strengthen the current preventive controls in place as it will help in the early identification and remediation of vulnerabilities.

9. Use of CDS system

Access and use of the CDS system by employees of CDS and by stock broking companies, custodian banks, registries, the Financial Services Commission (FSC) and the Bank of Mauritius should be in accordance with the CDS Rules and Procedures.

Remote users namely, stock broking companies, custodian banks, registries, the Financial Services Commission (FSC) and the Bank of Mauritius, are responsible for taking appropriate and diligent security measures concerning their own personnel, physical access to computers and other equipment connected to the CDS and the confidentiality of usernames and passwords used to access the CDS computer system.

Remote users must implement the following measures regarding their connection to the CDS/ATS network:

- The network running the CDS/SEM application at remote sites should be separated from any other networks. If there is a need to connect a PC running the CDS/SEM application to any other network, then the PC and the network should be protected by a Firewall.
- Prevent remote access facilities to network equipment
- Change network equipment password (routers, firewall.) after each intervention by suppliers
- Users are not permitted to alter network hardware and configurations in any way
- Remote users must not install a router, switch, hub, or wireless access point to the CDS/SEM without the approval of SEM/CDS.
- Routers should be protected with Access Control List and Firewall where necessary

10. Purpose and Use

The CDS offers access to its IT systems to employees and remote users for business purpose only. Employees should seek the prior approval of the Managing Director for any exceptional use of the IT systems of the company.

The CDS may suspend access to employees and remote users at any time for technical reasons, Policy violations, or other concerns.

11. Banned Activities

The following activities violate the CDS's IT Security Policy:

(A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.

(B) Revealing personal information, such as the home address, telephone number, or identity number of another person or the employee himself/herself.

(C) Making ethnic, sexual-preference, or gender-related slurs or jokes.

(D) Engaging in illegal activities or encouraging others to do so. Examples:

1. Accessing, transmitting, receiving, or seeking unauthorized, confidential information about clients or colleagues.
2. Conducting unauthorized business.
3. Viewing, transmitting, downloading, or searching for obscene, pornographic, or

illegal materials.

4. Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others.
5. Downloading or transmitting the organization's confidential information or trade secrets.

(E) Causing harm or damaging others' property. Examples:

1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the IT systems or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws-unless explicit permission to use the materials is granted.
2. Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the IT systems or Internet.
3. Uploading a virus, harmful component, or corrupted data.
4. Vandalizing the IT systems.
5. Using software that is not licensed or approved by the Company.

(F) Jeopardizing the security of access, the IT systems, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.

(G) Accessing or attempting to access controversial or offensive materials. IT systems and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites.

(J) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

12. Acceptable Internet Use Policy

Use of the internet by employees of SEM/CDS is permitted and encouraged where such use supports the goals and objectives of the business. However, SEM/CDS has a policy for the use of the internet whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet

Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic, violence, illegal drugs, weapons or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas

- publishing defamatory and/or knowingly false material about the company, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- undertaking deliberate activities such as social networking, chat, audio and video streaming , peer-to–peer downloads, dating, gaming and gambling that waste staff effort or networked resources
- introducing any form of malicious software or spam into the corporate network

Monitoring

SEM/CDS accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the SEM/CDS maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Wireless Internet Connection

Limited (time based) and controlled (Sophos) access to Wireless Internet Connection in the Board Room and Meeting Room of SEM/CDS will be granted to guests or SEM/CDS staffs upon request. Username(s) and password(s) as well as Internet access will be automatically deactivated after the prescribed time period. All requests for wireless Internet connection will be recorded in a log book by the System Department.

13. Use of Email

a) The CDS allows email access primarily for business purposes. Employees may use the CDS's email system for personal use only in accordance with this policy. Employees are prohibited from using personal email software (Hotmail, etc.) for business or personal communications at the office.

b) Employees are prohibited from using email to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

c) Employees are prohibited from using email to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

d) Employees are prohibited from using email to:

- Send, receive, solicit, print, copy, or reply to text or images that disparage others based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
- Send, receive, solicit, print, copy, or reply to jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, veteran status, ancestry, or disability.
- Send, receive, solicit, print, copy, or reply to messages that are disparaging or