CENTRAL DEPOSITORY &
SETTLEMENT CORPORATION
Invested in Progress

CDSC TECHNICAL GUIDELINES FOR CENTRAL DEPOSITORY AGENTS (CDAS)

Acronyms

CDA – Central Depository Agent

CDSC – Central Depository and Settlement Corporation Limited

CDS – Central Depository System

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Pursuant to Section 11 (3) of The Central Depositories (Regulation of Central Depositories) Rules, 2004, the CDSC hereby issues minimum technical guidelines for all CDAs accessing the CDS. The scope of these guidelines is all CDA technology, personnel and processes related to the CDS system and provision of CDSC services. These guidelines are provided as a minimum and should be adopted in line with relevant laws and regulations, guidelines provided in current best practices and international frameworks in Information Security, Data Protection, Business Continuity etc.

2. RESPONSIBILITIES

All CDAs, their Boards, Management and CDS users have the responsibility of protecting the security and integrity of information and equipment used to access and provide CDSC services. The following are the responsibilities of a CDA as far as access to the CDS system and provision of CDSC services is concerned.

1. Protection of all information system resources used for CDSC-related services, such as but not limited to:
    i. Computer systems hardware
    ii. System software
    iii. Data
    iv. CDS documentation (physical and/or electronic)
    v. Ensure only authorized users access the CDS.
2. Application of the highest possible Information Security and Data Protection standards to those information assets used to access the CDS and provide CDSC services.
3. Ensuring that information services that are critical to the access and operation of the CDS are adequately protected and that sensitive information managed by their staff is correctly classified and protected.
4. Ensuring that all the CDA's employees and contractors are aware of their obligation to safeguard CDS Information

3. GENERAL GUIDELINES

3.1. Personnel

a) All CDAs shall ensure that:

   i. They appoint persons duly and exhaustively vetted by themselves as CDS users.

   ii. They provide the necessary continuous IT security awareness training to the employees authorized to access the CDS and/or provide CDSC services.

   iii. They provide the necessary continuous Data Privacy awareness training to the employees authorized to access the CDS and/or provide CDSC services.

   iv. All employees accessing the CDS or providing CDSC services adhere to the CDA's policies and procedures as well as the highest possible standards in Information Security and Confidentiality.

b) Upon changes in employee responsibilities, appropriate measures should be taken to ensure that access controls have been changed to reflect the changes in responsibilities.

c) Upon termination of employment, appropriate measures should be taken to immediately revoke access to the CDS system.

d) The rights and roles assigned to CDA CDS users should be reviewed annually by the CDA to ensure continuous alignment with the role and level of access required for each user.

3.2. Infrastructure

a) The CDSC Technology team together with the CDA's Technology team will be responsible for ensuring that data transmission between CDSC and the CDA is secured and encrypted to the highest possible standard and restricted to authorized personnel only.

b) The CDA shall ensure that all equipment used to access and provide CDSC services is well-secured, patched and updated in line with the latest best practices in Information Security. This shall include but not be limited to network devices, end-user PCs, printers etc. The protections shall address but not be limited to the following: Use of adequate and frequently updated Anti-virus, encryption of end-user devices, and updated operating systems and software components.

3.3. Policies and Procedures

The CDA shall maintain adequate and up-to-date policies and procedures to ensure that all aspects related to the provision and access of all CDSC systems are done in line with the law, company policy and the latest best practice recommendations in Information Security and Data Protection.

3.4. General Access Controls

For access to the CDS system and provision of CDSC services, the CDA shall put measures in place to ensure that:

i. Each CDS user is assigned a unique username ("User ID") to distinguish that user from other users.
ii. Users shall not be created in the CDS without documented authorization.
iii. There is a process to formally approve User IDs and change of rights based on current and documented business needs and roles.
iv. Passwords must remain confidential and should not be shared, posted, or otherwise divulged in any manner.
v. Users will be held accountable for all actions performed under their user ID.
vi. Access to CDS application resources should be restricted to authorized users only.
vii. Access to the CDS system menus should be protected by assigning individual user rights on a need basis.
viii. Where a CDA intends to implement IT tools which may be used to process personal data belonging to CDS users and CDS account holders, CDSC shall require the CDA to conduct a Data Protection Impact Assessment and provide such assessment on request by CDSC before such tools are allowed access or connection to the CDS.

3.5. Change Management

Where changes relate to the CDS system and provision of CDSC services, the CDA shall ensure that:

i. There is adequate pre-planning and internal approval before implementation.
ii. Modifications are reviewed and documented to ensure that they meet the CDA's, requirements as well as current best practices and legal requirements in Information Security and Data Privacy.
iii. Emergency modifications shall be reviewed and documented before implementation.

3.6. Business Continuity

To ensure Business continuity and the recovery of CDSC-related services, the CDA shall ensure that:

i. It participates in all market wide CDSC Disaster Recovery and Business Continuity tests.
ii. They maintain backups of the following but not limited to; system logs, documentation, and software related to the CDS system and provision of CDSC services.
iii. They always maintain access to the CDSC's Disaster Recovery (DR) site.
iv. They maintain arrangements to ensure access to the CDSC's primary and DR sites in the event access to the CDA's primary site is unavailable.
v. They prepare, document, and continuously test and update disaster recovery and business continuity measures in line with current best practices in Information security and Business Continuity standards.

4. REVIEW

These guidelines shall be reviewed every three years or earlier based on evolving business needs, technology, laws, regulations and/or any other factor. Where there are changes to these guidelines, the same will be communicated to CDAs and availed on the CDSC website.