

<b>Document Name</b>	<b>CSE Information Technology Policy</b>
<b>Document Creation Date</b>	<b>08/06/2022</b>
<b>Document Created By</b>	<b>CISO-CSE</b>
<b>Version Control History</b>	<b>1.4</b>
<b>Document Reviewed Date</b>	<b>05/12/2024</b>
<b>Document Reviewed By</b>	<b>CISO-CSE &amp; CRO-CSE</b>
<b>Document Approved By</b>	<b>Standing Committee on Technology</b>

## **CSE Information Technology Policy**

### **Overview**

IT is an integral part of any modern organization especially Stock Exchanges. Maintaining a fruitful and effective IT Policy is utmost important for the sanctity, effectiveness, durability and trustworthiness of The Exchange. Any Cyber-attacks and threats on IT infrastructure to compromise the Confidentiality, Integrity and Availability of the computer systems, networks and databases, this Information Technology Policy is a formal set of rules by which those people who are given access to The Calcutta Stock Exchange Ltd (CSE) technology and information assets must abide.

### **Purpose**

The IT Policy serves several purposes. The main purposes are:

- i. Inform employees, vendors and other authorized users of their obligatory requirement to protect the technology & information assets of the CSE.
- ii. Set the guidelines for expected behavior by users, system administrators, management, and security personnel to achieve the above objective.
- iii. Deploy & authorize Security Personnel to monitor, probe, investigate and take remedial measures, whenever required.
- iv. Define the consequences of violation.
- v. Help minimize risk.
- vi. Help achieve security compliance as per guidelines of the relevant regulators like SEBI etc. is to inform users, employees, vendors and other authorized users of their obligatory requirements for protecting the technology and information assets of The Calcutta Stock Exchange Ltd.

### **Scope**

The scope of this policy includes all those people who are given access to The Calcutta Stock Exchange Ltd (CSE) systems and its wholly owned subsidiary CSE Capital Markets Private limited (CCMPL) to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the CSE are made up of the following components:

1. Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
2. System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
3. Application Software: used for trading purpose by the various departments.
4. Communications Network hardware and software including: routers, routing tables, hubs, modems, switches, firewalls, private lines, and associated network management software and tools.

## Policy

1. As per the information technology policy, the following process to identify, assess, and manage IT risk associated with processes, information, networks and systems.
  - a. 'Identify' critical IT assets and risks associated with such assets,
  - b. 'Protect' assets by deploying suitable controls, tools and measures,
  - c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes,
  - d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,
  - e. 'Recover' from incident through incident management, disaster recovery and business continuity framework.
2. The HOD of ITD, a senior level responsible officer will act as Chief Information Officer (CIO), whose function would be to assess, identify and secure IT infrastructure, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Information Technology Policy approved by the Board of the CSE.
3. The Standing Committee on Technology of the CSE will review IT policy on annual basis and its implementation. The policy will be approved by the Boards, and such review should include review of their current IT capabilities, set goals for a target level of IT compliance, and establish a plan to improve and strengthen IT service
4. A reporting procedure has to be established to facilitate communication of unusual activities and events to CIO or to the senior management in a timely manner.
5. The aforementioned committee and the senior management, including the CIO, will periodically review instances of IT non-compliance or incident, if any, domestically and globally, and take steps to strengthen CSE IT framework.
6. Responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use systems / networks of CSE, towards ensuring the goal of IT framework should be defined.
7. A senior level IT officer like HOD of ITD or Network Security, will act as Chief Information Security Officer (CISO), whose function would be to assess, identify and secure IT Security, respond to incidents/attacks, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the CSE.

## Identify

Critical IT assets based on their sensitivity and criticality for business operations, services and data management has to be identified. To this end, an up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows have to be maintained.

Cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality have also to be identified.

## **Protection Access Controls**

No person by virtue of rank or position will have any intrinsic right to access confidential data, applications, system resources or facilities.

Any access to CSE's systems, applications, networks, databases, etc., will be for a defined purpose and for a defined period. Access be granted to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access will be for the period when the access is required and has to be authorized using strong authentication mechanisms.

- a. **Password Control:** Strong password controls have to be implemented for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length (8 currently, alpha numeric and a special character) and history, password complexity as well as maximum validity period (15 days) and the user credential data has to be stored using strong and latest hashing algorithms as per the password policy of the Exchange.
- b. **User Access Policy:** User Access are uniquely identified and logged in system for audit and review purposes. Such logs have to be maintained and stored for a period not less than 2 years.
- c. **Additional controls and security measures:** Additional controls and security measures have to be deployed to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures will inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
- d. **Account Access Lock Policy:** An account access lock policies after failure attempts have to be implemented for all accounts. Its 3 attempts currently implemented.
- e. **Physical Access:** Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, will be subject to stringent supervision, monitoring and access restrictions of ITD.
- f. **Internet Access:** An Internet access policy has been governed by the Network Access Policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.
- g. Proper 'end of life' mechanism has to be adopted to deactivate access privileges of users who are leaving the organization or who access privileges have been withdrawn.

## Physical Security

Physical access to the critical IT systems should be restricted to minimum. Physical access of outsourced staff / visitors should be properly supervised by ensuring at the minimum that outsourced staff / visitors are accompanied at all times by authorized employees.

Physical access to the critical IT systems should be restricted/stopped immediately if the same is no longer required.

It has to be ensured that the perimeter of the critical equipment's room are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

## IT Asset Management

CSE follows a general purchase policy as a whole for the Exchange.

- a. **Procurement:** The IT procurement is also governed by it. However relaxation is made whenever a special IT product is procured superseding the overall procurement policy of the Exchange as special cases.
- b. **Asset Register:** The proper asset register is maintained by the accounts department after procurement and is also taken note after its disposal and end of life condition.
- c. **Disposing rejected/EOL IT Assets:** CSE doesn't follow any strict IT asset disposal policy as such. Whenever a considerable amount of unused and EOL products is generated then it is being disposed-off by accounts department under the supervision of General Administrative department. The disposed-off assets are removed from IT asset lists as maintained by the Accounts department.

## Critical IT Asset Management

To mitigate General IT risk and Cyber security risk in time of any incident occurs which can affect the trading system at large, CSE follows a policy of identifying and managing Critical IT Assets at its premise.

- a. **Identification:** The Critical IT Asset would be such IT equipment/hardware/software, which can affect critically important trading system. For main Trading Engine when TANDEM system was present, whole TANDEM mainframe servers were identified as critical asset. Likewise Servers used in Section-13 arrangement trading are identified as critical asset too. The network system connecting all the servers are equally critical here along with the security devices like firewalls etc. are also identified as critical IT assets.
- b. **Critical IT Asset Register:** The whole TANDEM mainframe servers, Servers used in Section-13 arrangement for trading in NSE & BSE, Total Network devices like core switches, Server farm switches, Some

important Desktops which runs critical operations and DP Servers used in CCML, Firewall devices are identified and booked in the Critical IT Register for easy and handy management of them to mitigate IT and Cyber security risk most importantly in case of any exigency or incident occurs.

Earlier when TANDEM system was present TCS Ltd. used to maintain and monitor regular critical asset register. Network and Firewall were also maintained by them. Section-13 assets were additionally maintained by them only.

- c. **SOP for incident management:** A clear cut SOP for managing IT incidents and exigencies have been led down in a detailed SOP for Incident Management as a policy. Identification of incident, its immediate actions to be taken and immediate reporting and long term solution and its testing and auditing (internal or external on case to case basis) has been led down in the SOP.
- d. **Disposal of Critical IT Assets:** Disposing of critical IT asset doesn't require any special treatment, it would follow General IT asset disposal policy only.

## Network Management

Baseline standards has to be used to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. Regular enforcement checks has to be conducted to ensure that the baseline standards are applied uniformly.

Network and network security devices, such as Switches, Core switches, firewalls as well as intrusion detection and prevention process has to be installed to protect its IT infrastructure from security exposures originating from internal and external sources.

Anti-virus software should be installed on servers and other computer systems. Updation of Anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

## Data Management

Measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity should be implemented. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

Only authorized data storage devices should be allowed through appropriate validation processes.

Data is stored in local disks daily backed up and kept in separate external hard disks which are kept in safe custody of respective departmental heads. IT data is kept in ITD

department under lock and key and used whenever required for testing/restoring or data extraction purposes only.

For CCMPD DP services related data of NSDL and CDSL and its own back office systems, the backed up data is stored locally as well as a set remotely also and handled by the DP employees only.

### **Hardening of Hardware and Software**

Only a hardened and vetted hardware / software should be deployed. During the hardening process, default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipment / software.

All open ports, which are not in use or can potentially be used for exploitation of data, should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

### **Application Security and Testing**

Regression testing like uncovering software bugs, enhancements, patches and new configuration should be undertaken before implementation. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

### **Change Management**

The IT Policy should define what constitutes a change in IT infrastructure. CSE has its complete change management policy in place. CSE has implemented processes for generating, evaluating, granting, approving, testing and responding to IT change requirements.

Proper Forms are designed and followed with authenticated documentation and kept in respective departmental heads.

Regarding changes in Section-13 arrangement like change in Multi Exchange trading software like ODIN etc. is maintained by the OEM and tested according to the rules of the respective exchanges like NSE or BSE and then implemented in the system.

For CSTAR CSE follows the rules set as per the policy.

### **Patch Management**

The patch management procedures should be established to include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

Rigorous testing of security patches should be performed before deployment into the production environment so as to ensure that the applications of patches do not impact other systems.

## **Incident Management**

The IT Policy should define what constitutes an incident. CSE has its incident management policy in place. CSE has implemented processes for preventing, detecting, analyzing and responding to IT exigency incidents as well as any information security incidents like virus/ransomware attacks etc.

The CISO is immediately informed and for cyber security incidents the appropriate authorities like Exchanges, Depositories, SEBI and CERT-In is informed complying fully with the SEBI circular. The Board is also informed in cases as per its veracity.

## **Data Centre Operations**

The main Data Centre is located at the Mezzanine Floor of the Exchange at 7, Lyons Range, Kolkata 700001. This data center hold Servers and Network backbone equipment. CSE Trading Engine, named as CSTAR is hosted on the TANDEM System which is located here. The HP switches and all the Network core switches and the Servers related to Section-13 Arrangements are also located in this Data Centre.

As it is a critically important place, adequate safety arrangements has been taken like physical access control, logical access control through biometric access control etc. Fire prevention arrangement is also maintained and monitored by the Administrative department of The Exchange and ensure proper fire safety.

## **Operating Systems and Database Management**

The CSTAR is developed in Tandem and run in Tandem hardware having proprietary Operating System (Guardian D45 onward). Other systems like earlier settlement and clearing house system used to use HP Unix based system and Oracle and currently database is kept using Linux 6 and Oracle. The Section-13 Servers are Intel based servers using only Windows Operating Systems and SQL Server as databases.

Proper Password management protocols, Patch management protocols, user access management protocols and security management and antivirus management protocols are followed to secure these systems.

The OEMs and Software vendors are given request based permission to access the systems whenever required. TCS has the full access as they resides at the same premise for maintaining and monitoring CSTAR application, hardware and currently maintaining all the CSE LAN infrastructure.

## **Database security**

The Database security is maintained as per the requirement of OEM/Software vendor as well as complying with the SEBI guideline relating to database security. Proper authentication method is followed for SQL Server databases and Oracle as well.

ITD securely maintains the database password as given monthly by TCS for Tandem and CSTAR application (when it was operational) and the database of ODIN and CLASS back office is predominantly maintained by the software vendors (63 Moons Technologies Ltd. for ODIN and BSE IT Ltd. for CLASS) as they maintain with fees. The Database passwords are shared with CSE ITD as well.

## **Application Security**

The security of the Application is responsibility of the vendor but those systems resides in CSE premise is under the purview of CSE IT security. The ITD and its HOD is predominantly responsible for securing Application and its successful running. Tandem and CSTAR application security is managed by TCS Ltd. till it was operational and the Section-13 applications like ODIN and CLASS BO software are managed by their respective Vendors who are mainly responsible for Application security.

## **Password Security**

CSE has a defined and detailed Password policy in place which is rigorously followed considering the ever increasing vulnerabilities and cyber threats.

HOD of any department using IT systems for their own requirement is predominantly responsible for securing the security of the passwords of the servers and critical systems. While the users and staffs are sole responsible for their Desktop password protection and security. Any lapse/breach of password security is punishable offence as far as data security is concerned.

## **Monitoring and Detection**

CSE should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, suitable mechanism has to be implemented to monitor capacity utilization of its critical systems and networks.

Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

## **Vulnerability Assessment and Penetration Testing (VAPT)**

Vulnerability assessment should be carried out twice a year to detect security vulnerabilities in the IT environment. Periodic penetration tests should also be done, twice a year too, in order to conduct an in-depth evaluation of the security posture of the IT systems through simulations of actual attacks on its systems and networks.

Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

In addition, perform vulnerability scanning and conduct penetration testing to be done prior to the commissioning of a new system, which offers Internet accessibility and open network interfaces.

## **Backup and Recovery**

CSE has a detailed backup and recovery policy in place. Backups are taken daily basis and kept in separate media on weekly basis. The response and recovery plan should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan should be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by SEBI.

The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of any system crash or cyber-attacks or breach of cyber security mechanism.

Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

CSE conducts suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

## **Sharing of information**

Quarterly reports containing information on cyber-attacks and threats experienced by CSE and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful to other Exchanges, should be submitted to SEBI. Such details as are felt useful for sharing with other Exchanges in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

## **Training**

Periodic training programs will have to be conducted to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT policy and standards. Special

focus should be given to build awareness levels and skills of staff from non-technical disciplines especially related to Cyber Security and use of IT infrastructure.

The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

### **Periodic Audit**

The Terms of Reference for the System Audit of CSE specified vide circular SEBI/HO/MRD1/MRD1\_DTCS/P/CIR/2022/58 May 02, 2022 accordingly modified to include audit of implementation of the aforementioned areas.

Also as a part of statutory audit procedure CSE audits the iBOS system every year.

CSE and CCMPL also conducts Cyber Security and Resilience Audit for NSE & BSE based trading systems and NSDL & CDSL DP operations every year as per SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019.

## Version Control History

**Version Change Date:** 04/11/2022

**Version Number:** 1.2

### Changes:

1. Purpose has been defined more elaborately as follows:
  - Inform employees, vendors and other authorized users of their obligatory requirement to protect the technology & information assets of the CSE.
  - Set the guidelines for expected behavior by users, system administrators, management, and security personnel to achieve the above objective.
  - Deploy & authorize Security Personnel to monitor, probe, investigate and take remedial measures, whenever required.
  - Define the consequences of violation.
  - Help minimize risk.
  - Help achieve security compliance as per guidelines of the relevant regulators like SEBI etc. et the guidelines for expected behavior by users, system administrators, management, and security personnel to achieve the above objective.
2. 'Account Access Lock Policy' under the topic 'Protection Access Controls' the '6 attempts, mentioned is replaced by '3 attempts'.
3. Some typos are rectified.

**Version Change Date:** 17/05/2023

**Version Number:** 1.3

### Changes:

1. **Scope** has been extended to CCMPPL also
2. **The Critical IT Asset Management** section has been added for CSE as well as CCMPPL.
3. The **Data Management** section has been updated with 'For CCMPPL DP services related data of NSDL and CDSL and its own back office systems, the backed up data is stored locally as well as a set remotely also and handled by the DP employees only'.
4. The last paragraph of the Periodic Audit has been added as 'CSE and CCMPPL also conducts Cyber Security and Resilience Audit for NSE & BSE based trading systems and NSDL & CDSL DP operations every year as per SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019'.

**Version Change Date:** 05/12/2024

**Version Number:** 1.4

### Changes:

1. **SOP for Incident Management** and its effect on critical IT assets has been added.
2. CRO-CSE has been added as reviewer of policy