

|                                |   |
|--------------------------------|---|
| <b>Document Name</b>           | <b>Patch Management Policy for CSE &amp; CCMP</b> |
| <b>Document Creation Date</b>  | <b>01/06/2022</b>                                 |
| <b>Document Created By</b>     | <b>CISO-CSE</b>                                   |
| <b>Version Control History</b> | <b>1.2</b>  |
| <b>Document Reviewed Date</b>  | <b>05/12/2024</b>                                 |
| <b>Document Reviewed By</b>    | <b>CISO-CSE</b>                                   |
| <b>Document Approved By</b>    | <b>Standing Committee on Technology</b>           |

## **Patch Management Policy for CSE & CC MPL**

### **Introduction**

This document forms The Calcutta Stock Exchange Ltd. termed as CSE & CSE Capital markets Pvt. Ltd. termed as CC MPL here and their Patch Management Policy which supports the Information Security Policy and Cyber Security policy. It details requirements for maintaining up-to-date software version levels and operating system security patches on all IT equipment used in CSE & CC MPL.

Compliance with this policy will help ensure that consistent controls are applied across CSE & CC MPL to minimize exposure to 'known' vulnerabilities. Where possible, all CSE & CC MPL IT systems shall be updated to the latest patch/security releases.

### **Purpose**

To ensure that security patches and systems and application updates, hotfixes and patches are properly identified, tested and applied and tracked in a consistent manner.

The purpose of this policy is to ensure that all CSE & CC MPL owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform the broking community about the change in end-point computing, if any.

### **Definitions**

#### **IT Systems include:**

- Computers
- Software (platforms, applications, databases, security products etc.)
- Networks (switches, routers etc.)
- Servers (physical and virtual)

### **Scope**

This policy applies to all IT systems at CSE and CC MPL which includes Servers (hardware and software/virtual), Application software, Security devices and its OS etc. The scope and purview of it is also included in the scope in System Audit and Cyber Security Audit as per SEBI guidelines.

## **Roles & Responsibilities**

|                      |  |
|----------------------|--|
| <b>IT Department</b> | Patch centrally managed systems<br>Record unpatched systems<br>Remove/quarantine non-compliant systems as appropriate<br>Responsible for routinely assessing compliance with the patching policy and providing guidance to all stakeholder groups in relation to issues of security and patch management |
| <b>IT Committee</b>  | Exceptional situation approval if any which is out of written down IT policy<br>Record Information on exceptions and exigency non-compliance if any  |
| <b>Business Unit</b> | Each business unit is responsible for devices and systems under their control<br>Business unit directors must ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list or by direct notification from the vendor/ITD                      |
| <b>End User</b>      | Responsible for adhering to policy and reporting any issues to the ITD   |

## **Policy and Procedure for Patch Management**

- All IT systems shall be manufacturer supported and have up-to-date and security patched operating systems and application software.
- Security patches must be installed to protect assets from known vulnerabilities.
- All recommended patches should be controlled through change management procedure and follow the guidelines mentioned therein as far as CSE's own trading system CSTAR is concerned.
- Patches rated 'Critical' or 'High' by the vendor must be installed within 7 days/1 week of release from the operating system or application vendor unless prevented by CSE & CC MPL's change control procedures.
- Patches rated 'High' or 'Medium/Moderate' by the vendor must be installed within 14 days/2 weeks of release from the operating system or application vendor unless prevented by CSE & CC MPL's change control procedures.
- Patches rated 'Low' by the vendor must be installed within 28 days/1 month of release from the vendor, unless mitigating controls are in place to prevent the exploit being realised, in which case it may be deferred to the nearest maintenance window.
- CSTAR software vendor team should track all advisories from OEMs of various System devices as well as network devices and other forums regarding OS and application patches evaluate the same in terms of exposure to such vulnerabilities to systems and devices

(Servers, desktops, laptops, mobile devices etc.) And apply the relevant patches to manage the technical vulnerabilities in OS of Tandem (if used) and all network devices and servers used in CSE network.

- CSE-ITD personnel should be deployed to update patches in Section-13 Intel based Servers at least quarterly. Same rule applicable for CC MPL DP, CSE Listing and other departmental servers under CSE as well.
- All the systems should have OS patches based on proper assessment and testing and confirmation from relevant application vendors and proper records of the same should be maintained.
- For CSE & CC MPL central Antivirus server arrangement, it is automatically updated as far as security and signature patches and DAT files are concerned. Any software version update is controlled separately with consultation and testing with CSE IT department and OEM vendor concerned.
- No approval is required for standard patch deployment on desktops and laptops. However, the patch should be tested on a test system before mass deployment of patches.
- Fallback option should be studied thoroughly before applying any update/patch & necessary steps to be taken to recover from any undesirable effect after update.
- For critical systems, the patches will be applied manually after proper test in the Test system created for testing the server OS patches.
- All patches from application vendors in production servers and critical systems should be first tested on a separate test system and only once working fine, it should be applied to the production systems/servers.
- Testing needs to be done in the test environment and only after the test is successful should be patches be applied in case of in house or customized software/application only. For global software (Microsoft/Oracle products etc.) separate testing need not be done as they are presumed to be well tested before global release.
- Rollback plan has to be formulated, reviewed and approved before implementing patches. Backups should be taken before and after any major change/critical patch.
- All client software installed in PCs should be kept up-to-date with the latest security patches as available from the concerned vendors & after proper testing.
- For emergency patches, this should be discussed with CISO with a proper analysis of risk and impact of the patches.
- Patch management records and complete history of patch management for critical systems and all other systems should be maintained by the IT department.

## **Monitoring and Reporting**

Reporting metrics that summarize the outcome of each patching cycle shall be compiled and maintained by IT Department. These shall be used to evaluate patching levels and assess current levels of risk.

## **Exceptions**

There are some systems that cannot be patched. For example systems that are end of life or that require a precise version of software to operate. Exceptions must be risk assessed, have formal documented approval and be recorded by CTO/CIO. Compensating controls will be applied, as necessary, and may be considered as sufficient mitigation.

## **Non-Compliance**

A device that poses an unacceptable level of risk may be disabled or removed from the production environment. They will only be reconnected once it is proven that they have been brought up to date and are secure.

## **Period**

Patch management update in servers including critical servers should be done at least quarterly where automatic windows update is not configured. Otherwise it should be done as per criticality. The table is as follows:

| <b>Sl. No.</b> | <b>Criticality</b> | <b>Timeline</b> |
|----------------|--------------------|-----------------|
| 1              | High               | 1 Week          |
| 2              | Moderate           | 2 Weeks         |
| 3              | Low                | 1 Month         |

## **Related policies, procedures, guidelines & regulations**

- Information Security Policy.
- Information Risk Management Policy

## **Policies superseded by this policy**

SOP: Patch Management v1.0

## Version Control History

**Version Change Date:** 03/11/2022

**Version Number:** 1.1

**Changes:**

The following points have been added under the topic “**Procedure for Patch Management**”

1. All recommended patches should be controlled through change management procedure and follow the guidelines mentioned therein.
2. Fallback option should be studied thoroughly before applying any update/patch & necessary steps to be taken to recover from any undesirable effect after update.
3. Rollback plan has to be formulated, reviewed and approved before implementing patches. Backups should be taken before and after any major change/critical patch.
4. All client software installed in PCs should be kept up-to-date with the latest security patches as available from the concerned vendors & after proper testing.

**Version Change Date:** 09/02/2024

**Version Number:** 1.2

**Changes:**

The main change being the name of the policy from ‘SOP: Patch Management’ to ‘Patch Management Policy of CSE & CC MPL’

The following points have been added under the policy

1. Added the Introduction section
2. Added the Purpose section
3. Added the Definition section
4. Modified the Scope section
5. Modified the Policy and Procedure section as well at large
6. Also Modified the period section with addition of criticality table
7. Added the sections like ‘Monitoring and reporting’, ‘Exception’ and ‘Non-Compliance’ and also the Related policies section and Policy Superseding section also.