

Document Name	CSE VPN Access Policy
Document Creation Date	22/01/2015
Document Created By	Executive – ITD
Version Control History	1.4
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO-CSE
Document Approved By	Standing Committee on Technology

CSE VPN ACCESS POLICY

Purpose:

The purpose of this policy is to define requirements for connecting to The Calcutta Stock Exchange Ltd.'s (CSE) network (or any network managed by CSE) from an outside entity. These requirements are designed to minimize the potential exposure of CSE from damages which may result from unauthorized use of CSE resources. Damages include the loss of sensitive or confidential information, damage to public image and damage to critical CSE internal systems. CSE intent to offer SSL VPN access for those Members/departments/users that need specific access to services where a smooth level of user access control and/or application control is necessary. In particular, the SSL is intended to provide authenticated/encrypted access to restricted resources like CSTAR, ODIN, CLASS applications, and/or systems that house sensitive information. The resources should not be available from the general Internet and need to be clearly identified.

Definition:

The SSL VPN offers remote access using a web browser over SSL (Secure Socket Layer) and does not require client side software (unless full traditional VPN-like access is required, in which case the Network Connect client is required). An additional benefit to the implementation of SSL VPNs is the ability to grant access to specific resources based on group membership as defined by the CSE ITD.

Scope

This policy applies to authorized users of CSE intending to access internal servers or applications hosted in CSE for Trading, remote administration or secure access to Intranet applications. This policy applies to VPN connections provided through centralized VPN devices. This policy also applies to all CSE employees, contractors, vendors and agents with a CSE-owned or personally-owned computer used to connect to the CSE network including CSE's own subsidiary CC MPL for DP operation. This policy applies to remote access connections used to perform work on behalf of CSE including reading or sending email and viewing intranet web resources.

Policy

- 1) VPN connection is provided to only registered users and is available through the URL link <https://trade.connect2cse.com>.
- 2) VPN connection is provided to user for accessing the Applications hosted in CSE for trading or to access Intranet applications hosted in CSE.
- 3) VPN connection is provided to authorise Member Brokers, CSE Employees & Third party Vendors.
- 4) The following process will be used for VPN Users activation.
 - Users applies for VPN connectivity through a filled VPN application form with copy of Internet & address proof to ITD.
 - After Verification of the application and documents and a user activation request is forwarded to CSE VPN Support Team by ITD.
 - VPN Support Team creates the VPN User ID & Password and a password reset enforcement is applied at the time of first login and then replies back to ITD.
 - ITD informs the user the VPN login portal, User ID & password through email.
 - The Verification of the users shall be done by the authorised representative from the concerned department.
- 5) The following process will be used for VPN Users deactivation.
 - User surrenders by a written letter / email.
 - ITD requests VPN support team for ID deletion form VPN devices.
 - Support Team performs the same and informs users.
- 6) VPN access will only be provided to servers hosted in CSE and behind firewall.
- 7) Once connected to CSE VPN, all traffic between the user's PC and CSE will be through SSL VPN tunnel and user will have access to only the servers opted in the application form.
- 8) Each VPN user ID & Password will be verified at the VPN Equipment level and will only be permitted with the matched policy already defined against it.
- 9) Password reset of VPN ID is entertained only by written request / email.
- 10) Users has to make sure that the system used for VPN connection is regularly scanned and updated with latest OS patches and anti-virus software .
- 11) The VPN connection will be automatically disconnected after a predefined time interval due to inactivity (idle timeout). The user has to login again.
- 12) It is the responsibility of Users /Members/ Employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.

- 13) SSL VPN use is to be controlled using a User ID & password authentication through a dedicated secured URL and a SSL tunnel.
- 14) VPN gateways will be set up and managed by network operational groups.
- 15) Pings or other artificial network processes are not to be used to keep the connection open.
- 16) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of CSE's network, and as such are subject to the same rules and regulations that apply to -owned equipment.
- 17) Exceptions on the already defined service access restrictions should be duly authorized by an appropriate authority after carrying out a Risk Assessment.
- 18) Deny access logs on remote access service should be monitored by Network/Security Operations staff for taking appropriate preventive actions.
- 19) Adequate care should be taken by mobile users when mobile computing facilities are used in public places, meeting rooms and other unprotected areas as defined in VPN Access Guidelines.
- 20) Laptop users using VPN connectivity to access CSE resources should additionally follow the below mentioned guidelines:
 - While not in use, laptop is to be securely placed in its docking station, a locked cabinet or locked to the desk in your office.
 - Users should refrain from sharing laptops with someone else for business use or non-business use.
 - While on travel, laptop should be kept under constant surveillance. Laptop is to be protected with screen saver password.
 - Ensure every connected laptop has the latest virus signature files.

Responsibility

The Members, Users, Network Administrator and all CSE Employees shall follow the policy.

Enforcement

The policy has to be enforced by VPN administrators, network administrator and CSE ITD.

Version Control History

Version Change Date: 04/11/2022

Version Number: 1.3

Changes:

1. Some grammatical and typo errors rectified under topic '**Purpose**', '**Scope**', '**Policy**'
2. Point 11 under the topic '**Policy**' is rephrased as 'The VPN connection will be automatically disconnected after a predefined time interval due to inactivity (idle timeout). The user has to login again.'
3. The following points have been added under the topic '**Policy**' after Point no. 16:
 - a) Exceptions on the already defined service access restrictions should be duly authorized by an appropriate authority after carrying out a Risk Assessment.
 - b) Deny access logs on remote access service should be monitored by Network/Security Operations staff for taking appropriate preventive actions.
 - c) Adequate care should be taken by mobile users when mobile computing facilities are used in public places, meeting rooms and other unprotected areas as defined in VPN Access Guidelines.
 - d) Laptop users using VPN connectivity to access CSE resources should additionally follow the below mentioned guidelines:
 - While not in use, laptop is to be securely placed in its docking station, a locked cabinet or locked to the desk in your office.
 - Users should refrain from sharing laptops with someone else for business use or non-business use.
 - While on travel, laptop should be kept under constant surveillance. Laptop is to be protected with screen saver password.
 - Ensure every connected laptop has the latest virus signature files.

Version Change Date: 17/05/2023

Version Number: 1.4

Changes:

1. In the RESPONSIBILITY section 'all CSE Employees shall follow the policy 'has been updated.
2. In the Scope section 'including CSE's own subsidiary CC MPL for DP operation 'has been added.