

Document Name	CSTAR User Authorization Procedure
Document Creation Date	25/03/2014
Document Created By	DGM-ITD
Version Control History	1.4
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO-CSE
Document Approved By	Standing Committee on Technology

CSTAR User Authorization Procedure

Overview

Users of CSTAR computing infrastructure viz. Members (including users authorized by them to use CSTAR resources on the member's behalf), Exchange employees and personnel deployed by the vendors of the Exchange are allowed access to only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the Exchange.

Access Classification

The following table summarizes the key references for access authorization in CSTAR.

<u>Sl</u>	<u>User</u>	<u>Role</u>	<u>Area</u>	<u>Controller</u>	<u>Pre-processor</u>	<u>Approver</u>
1	Member (incl trader)	Trading	TWS/SS	MOP	Membership	MD&CEO
2	Exchange employee	Monitoring	TWS/SS	MOP	Deptt In Charge	MD&CEO
3	MOP user	MOP	MOP	MOP	Deptt In Charge	MD&CEO
4	SURV user	SURV	SURV	MOP	Deptt In Charge	MD&CEO
5	Ex. Vendor person	Maintenance	CSTAR All	MOP	Vendor's Project Manager	CFO/AM-IT
6	Ex. Vendor person	Role based	Operating System	ITD	Vendor's Project Manager	CFO/AM-IT
7	Ex. Vendor person	Role based	Database	ITD	Vendor's Project Manager	CFO/AM-IT

Procedure

1. For Activation & Revision of access privileges to CSTAR (other than Sl no 1 above) the user will submit 2 (two) copies of the duly filled up Access Request Form from the Controller Department and submit the same to the designated pre-processor.
2. Each set of forms (both copies) should be filled up for required privileges by the pre-processor after evaluation of the need for the same before seeking authorization from the Approver with recommendation.
3. The approved application (both copies) to be forwarded to Controller department for processing of Account. The official at Controller Department would sign at "Processed by" box of the Form after entering the details in the manual register for all the User-Id details with Serial No. given by them.

4. One copy of the form will remain with Controller Department and the other is to be sent to MOP/SURV/ITD. Department for assignment of privileges by the Module SUPER USER as per approval contained in the form.
5. On completion of the privilege assignment, the form, duly signed by SUPER USER, will be returned to the pre-processor for records. In case of OS & Database access accounts, this copy would be retained with the System / Data Base administrator as applicable.
6. In case of activation, controller department will immediately set the User Password to default password and then it is the User's responsibility to change the same as per the CSE Password Policy.
7. It is User Department's responsibility to initiate de-activation process of the User account at the time of any transfer/ termination of the User using the prescribed form.
8. Each User Department / pre-processor would review the privileges assigned to all active users under their supervision, along with the Controller, at least once in a year. ITD would intimate all concerned before stipulated date of review.
9. SUPER Users form should be approved by MD&CEO and reviewed at least once in a year. ITD would intimate all concerned before stipulated date of review.



The Calcutta Stock Exchange Association Limited
7, Lyons Range, Kolkata-700 001.

C-STAR (MOP / SURVEILLANCE) ACCESS REQUEST FORM

Serial No. : _____

Date: _____

USER:

USER-ID: _____

Activate / Deactivate / Revise

Module (MOP/SURV.):

With Effect From

 (dd/mm/yyyy)

User's Acceptance

 Signature: _____

 Designation & Dept.: _____

MAKER <input type="checkbox"/>		/ CHECKER <input type="checkbox"/>		SUPER USER <input type="checkbox"/>	
MOP ACCESS					
	All	View	None		All
					View
					None
SESSION				SETTLEMENT	
COMPANY				INDEX	
MEMBER				INDEX SCRIP	
USER				ACCESS CONTROL	
SCRIP				SESSION (AUCTION)	
NEWS ENTRY				CLOSE RATE	
DIVIDEND				NO DELIVERY	
SCRIP GROUP				BANK	
CUSTODIAN					
SURVEILLANCE ACCESS					
General	All	View	None	Suspension	All
ONLINE MARGIN				SCRIP	
MESSAGE				COMPANY	
MARKET HALT				TRADER	
ADMIN				MEMBER	
NEWS				Surveillance	
FUNDSPAY				SCRIP	
GELMARGIN				SCRIP GROUP	
Daily Margin				CKT FLT LIMIT	
SCRIP					
SCRIP GROUP					
Privileges Updated by : _____			Signature : _____		

Recommended by HOD

Approved By MD&CEO

Processed By

 (MOP Department)

Note: A) Procedure for Activation/ De-activation/ Revise of C-STAR MOP/ SURV. USER-ID and
 B) CSE Password policy are given overleaf.

A. Procedure for Activation/ De-activation/ Revise of C-STAR MOP/ SURV. USER-ID

1. For Activation/ De-activation/ Revised of a MOP/ SURV. User-Id, the user department will collect 2 (two) copies of the USER-ID Access Form from the MOP Department.
2. The new forms then to be duly filled up in duplicate along with the User's Acceptance details & signed by the User.
3. The forms is to be approved by the MD&CEO/ Executive Director on recommendation of Head of the Department.
4. The approved application to be forwarded to MOP department for process of User-Id Account.
5. MOP/SURV. Department's SUPER USER will assign the privileges as approved.
6. The forms then will come back to MOP department with duly signed by SUPER USER.
7. Then MOP official has to duly sign at "Processed by" box of the Form and will maintain a manual register for all the User-Id details with Serial No. given by them. 1 copy of the form will remain with MOP and 1 copy of the form will go back to User Department
8. In case of Activation, MOP department will immediately set the User Password to default password and then it is User's responsibility to change the same as per the Password Policy of the C-STAR.
9. It is User Department's responsibility to initiate de-activation process of the User-Id at the time of any transfer/ termination of the User using the same form.

B. CSTAR Password Policy

1. Password should contain at least one small letter and one capital letter of the alphabet and should also contain a special character. User Id and User name should not be used as a part of the password. Three previous passwords cannot be used as the new password.
2. The Password length will be a minimum of 8 characters and a maximum of 16 characters.
3. On successful modification of the password the "Password Modification" window will close automatically after an interval of 2 or 3 seconds.
4. Password will have a validity period and the password will expire unless changed within this period and the User will fail to logon. The current validity period is 15 calendar days.
5. Attempts to obtain User Access with incorrect Password via the Logon Box will be restricted to 3 (Three) successive retries. In case the User fails to login after 3 (Three) consecutive unsuccessful attempts, his account will expire until further action is taken from MOP.
6. Password should not be shared with any one and should never written down or stored on-line.
7. All Passwords are to be treated as sensitive, confidential CSE information.
8. All passwords should be stored in the system in an encrypted form.



Ref No.:

**THE CALCUTTA STOCK EXCHANGE LIMITED
INFORMATION TECHNOLOGY DIVISION**

Immediate Computer System Access Suspension/Revoke Form

First Name _____ Middle Name _____ Last Name _____

User Name _____ Home Directory _____

Status Level

- Fully revoke
 Fully suspended
 Partial revoke
 Partial suspended

Need justification for suspension/Revoke of user name _____

If partially revoked / suspended (provide with necessary details bellow)

1. Permanent Temporary
2. system administration Database administration Network Administration Security Administration System Maintenance
- Application Developer System Operators

DETAILS

#	<u>Roles</u>	<u>Privileges</u>

Access Denied In Server

- SUN (Main Trading server)
 MOON (Online Data Backup server)
 BRUNO (Settlement processing server)

Recommended by (signature) **Name** **Designation**

System administrators please de-activate/partially de-activate this account and report.

GM (ITD)/DGM (ITD)/AM (ITD)



Ref No.:

**THE CALCUTTA STOCK EXCHANGE LIMITED
INFORMATION TECHNOLOGY DIVISION**

Computer System Access Request Form

First Name _____ Middle Name _____ Last Name _____

User Name _____ Home Directory _____

Creation Date ____/____/____

Status Level

Expert Intermediate Beginner

Signature _____ Date _____

Access Type

- 1. Permanent Temporary (Date upto _____)
- 2. system administration Database administration Network Administration Security Administration System Maintenance
- Application Developer System Operators

DETAILS

#	Roles	Privileges

Access Required In Server

- SUN(Main Trading server) MOON(Online Data Backup server) BRUNO(Settlement processing server)

Recommended by (signature) _____ Name _____ Designation _____

System administrators please activate this account and report.

GM (ITD)/DGM (ITD)/AM (ITD)

Version Control History

Version Change Date: 20/10/2022

Version Number: 1.4

- Changes:**
- Point No. 4 In case the Controller department is MOP/SURV, copy of the form should be marked to ITD.
 - Point No. 8 ITD would intimate all concerned before stipulated date of review.
 - Point No. 9 ITD would intimate all concerned before stipulated date of review.

 - B Point No.1 Password Policy Password should contain at least one small letter and one capital letter of the alphabet and should also contain a special character.
User Id and User name should not be used as a part of the password. Three previous passwords cannot be used as the new password.
 - B Point No.2 Length of Passwords should be at least 8 characters and Maximum 16.
 - B Point No.4 The current validity period pf password is 15 calendar days.
 - B Point No.5 Attempts to obtain User Access with incorrect Password via the Logon Box will be restricted to 3 (three) successive retries
 - B Point No.8 All passwords should be stored in the system in an encrypted form.