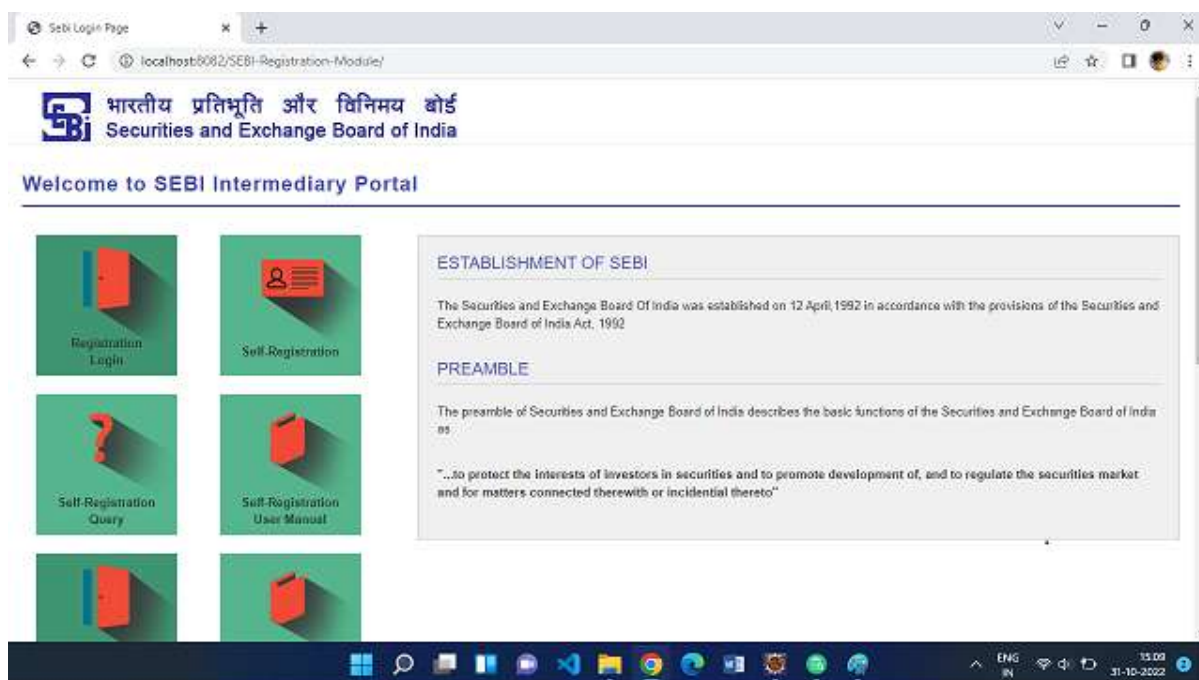


Incident Reporting Portal- User Manual

1. Steps for Self-Registration

Step 1.1. Go to SEBI Intermediary Portal by visiting the URL:
<https://siportal.sebi.gov.in/intermediary/index.html>



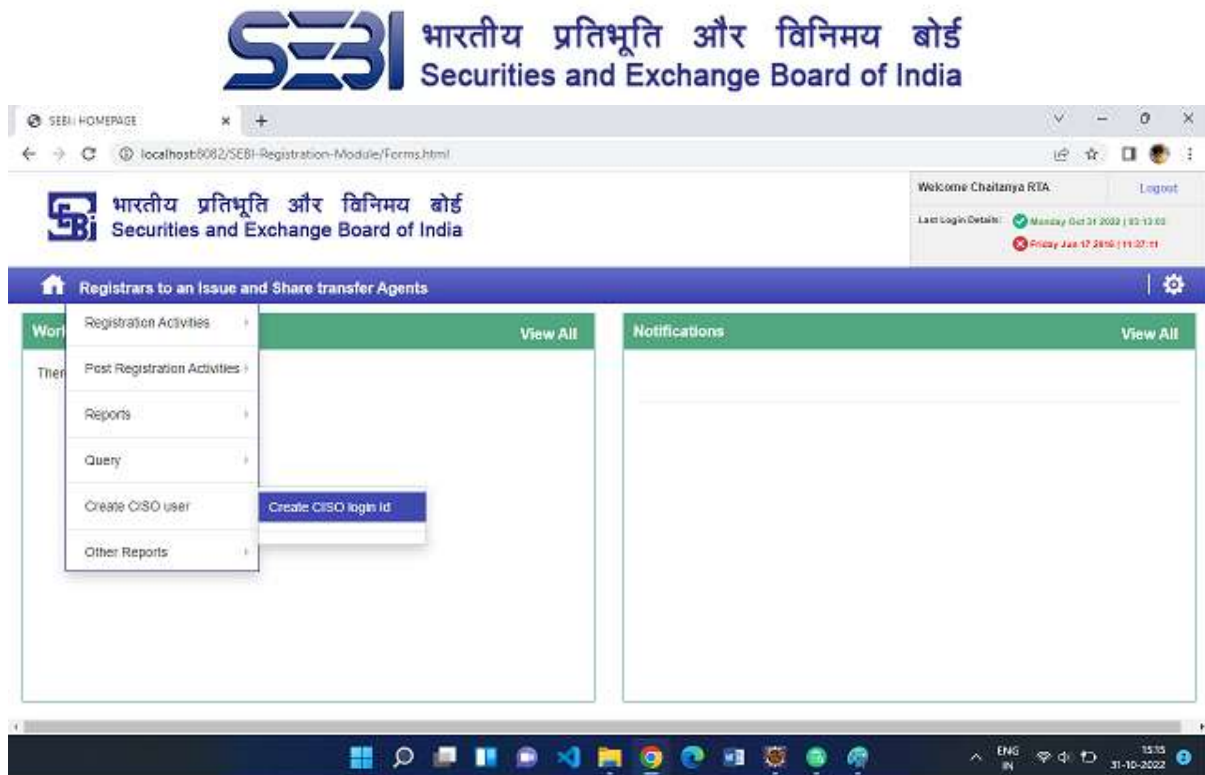
Step 1.2. Click on Registration Login and Enter your credentials to login to the SI Portal.



Step 1.3. Enter OTP and click on Validate OTP



Step 1.4. Go to Create CISO User -> Create CISO Login Id

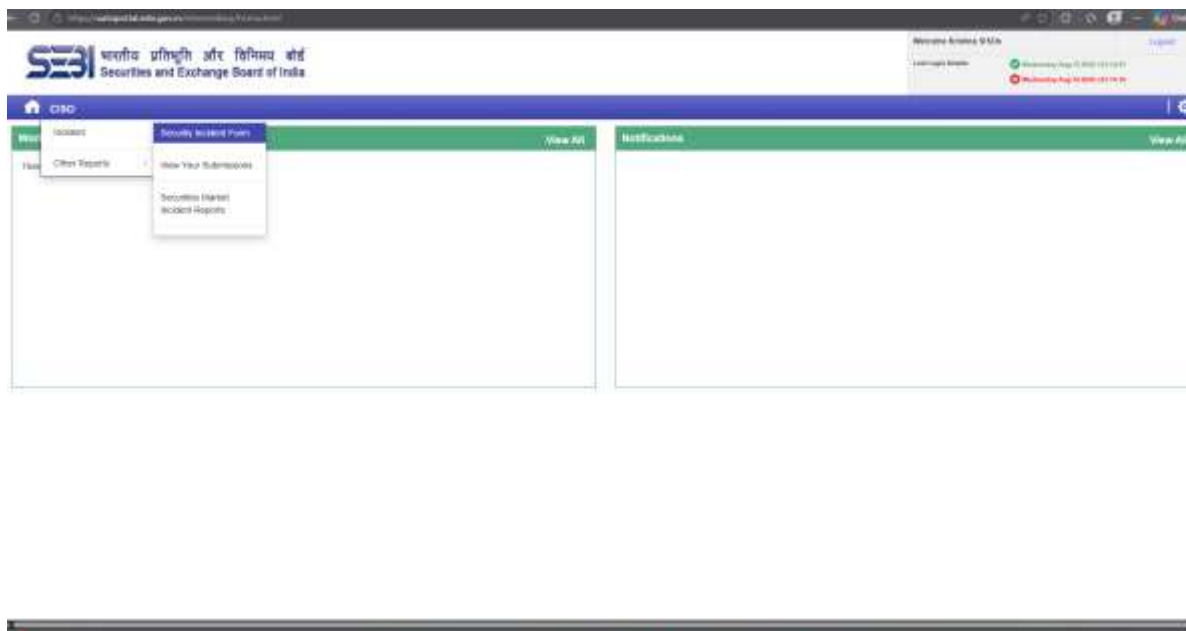


Step 1.5. Fill the form and click on submit button.

Your request to create CISO Role would be successfully submitted to SEBI. Once approved by SEBI, you will receive activation email on the email id mentioned above to activate the email.

2. Steps to Report Security Incident: -

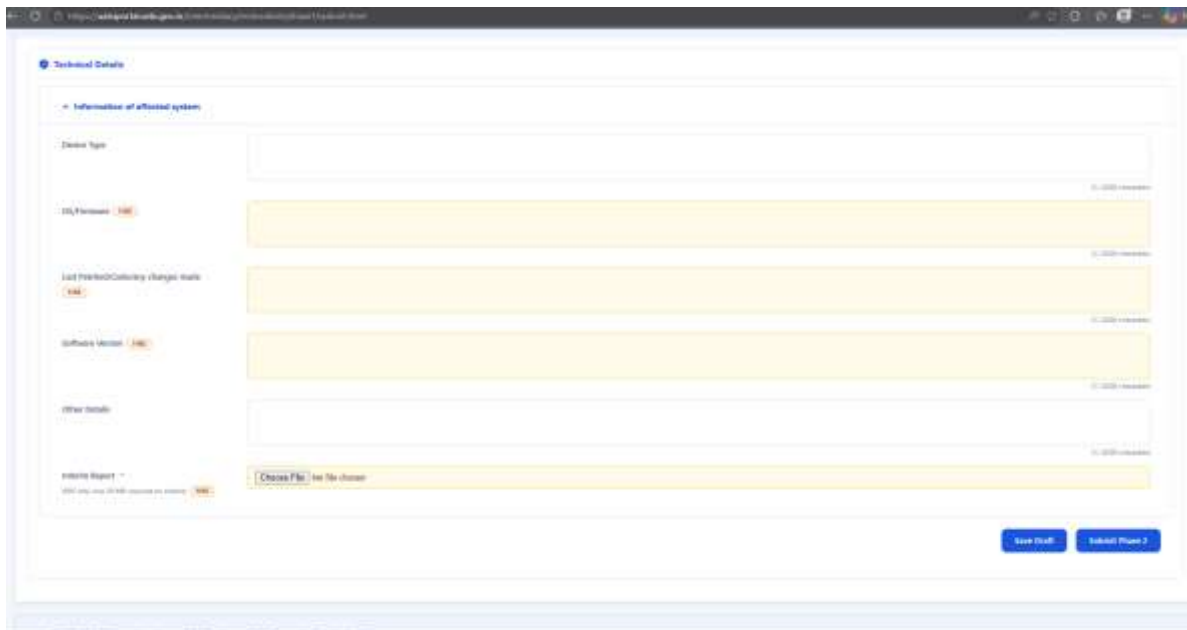
Step 2.1. Go to CISO-> Incident -> Security Incident Form



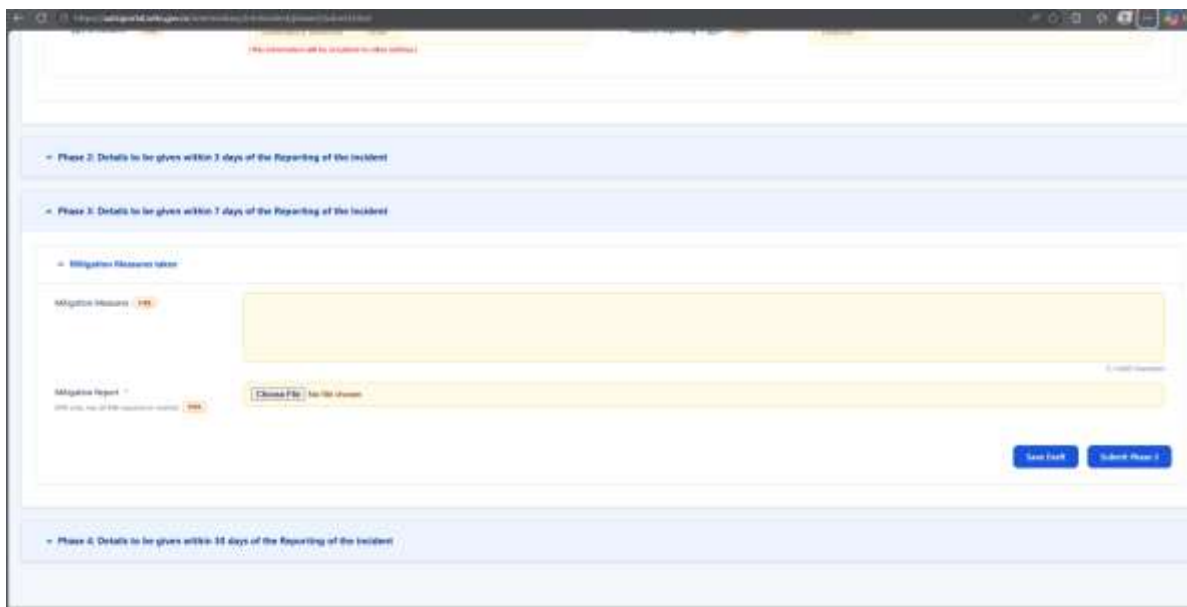
Step 2.2. Fill all the details of Phase 1 (Initial Reporting) and submit:

The screenshot shows the 'Incident Reporting Portal' for Phase 1: Initial Reporting. The form is titled 'Phase 1: Initial Reporting' and includes a progress indicator showing '1' of 4 steps. The form is divided into two main sections: 'Basic Details' and 'Additional capacity / role registered with SEBI'. The 'Basic Details' section includes fields for 'Applicant Name', 'Registered Entity Type', 'CISO First Name', 'CISO Last Name', 'CISO Email', 'CISO Mobile Number', 'CISO Landline', and 'Select Reporting Identifier'. The 'Additional capacity / role registered with SEBI' section includes a dropdown for 'Capacity / role' and a text field for 'SEBI registration no. for that role'. The form is designed with a clean, professional layout using yellow and blue colors.

Step 2.3. Fill all the details of Phase 2 (Within 3 days of the Reporting of incident) and submit:



Step 2.4. Fill all the details of Phase 3 (Within 7 days of the reporting of the incident) and submit:



Step 2.5. Fill all the details of Phase 3 (Within 30 days of the reporting of the incident) and submit:

The screenshot shows the 'Phase 4: Details to be given within 15 days of the Reporting of the Incident' form. The form is titled 'Root Cause Analysis' and contains several input fields and sections:

- Number of systems affected:** A text input field with the value '1'.
- How was the incident detected?:** A text input field.
- Chronology of the event to be:** A text input field.
- Root Cause Analysis:** A large text area for detailed analysis.
- Actions Taken:** A text input field.
- Other Details:** A text input field.
- Actual Date and Time of Resolution:** A text input field.

Each input field has a small '100%' indicator next to it. The form is displayed on a web browser with a Windows taskbar visible at the bottom.

3. Steps to View Incidence Details which you have submitted

Step 3.1. Go to CISO -> Incident -> View Your Submission

The screenshot shows the 'Phase 1: Initial Reporting' form. The form is titled 'Basic Details' and contains several input fields and sections:

- Applicant Name:** A text input field with the value 'INDIAN SECURITIES'.
- Regulated Entity Type:** A dropdown menu with the value 'Qualified SEI'.
- CISO Name:** A text input field with the value 'Rajesh'.
- CISO Email:** A text input field with the value 'rajesh@indiansec.com'.
- CISO Mobile:** A text input field with the value '9999999999'.
- Designated Authority:** A text input field.
- CISO Mobile Number:** A text input field.
- CISO Email:** A text input field.
- CISO Landline:** A text input field.

Each input field has a small '100%' indicator next to it. The form is displayed on a web browser with a Windows taskbar visible at the bottom.

4. Steps to View Incident Details from common pool

Step 4.1. Go to CISO -> Incident -> Securities Market Incident Reports

Securities Market Incident Reports

From DATE: To DATE:

S.No.	Incident Type	Incident Description	Initiators of Complaint (If any)	Affected System Type	Affected System Details	Details of Malicious File/Firm	Any Other Relevant Details	Period from 30 Months	Details of Malicious File/Firm	Reg. FRO/PO Assets	Case
1	System crash/ Unusual usage and system access pattern identified	---	---	Test	CS/Networks/Security test Software version test	---	---	---	---	---	1000 1171
2	Initial engineering changes identified whether correct or not	Test Description	CSF Request available; Malicious File; Application Traffic on the system is blocked.	CSF Request	---	Test Description	---	---	Test Details	---	1000 1171