



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2026/432

June 30, 2026

QUARTERLY CYBER INCIDENT REPORTING BY DPs

DPs are advised to refer to SEBI circular No: SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022, and CDSL/OPS/DP/POLCY/2025/27 January 10, 2025, wherein all Cyber-attacks, threats, cyber-incidents and breaches experienced by Depositories Participants shall be reported to CDSL.

In view of the above, Depository Participants are required to submit the **Quarterly Cyber Incident Report** through the audit web portal. In case no cyber incident has occurred during the quarter, Depository Participants may select the option “**No**” under Cyber- attack/Breach observed in the Quarter.

Depository Participants must submit a mandatory quarterly report to CDSL on all the cyber-attacks, threats, incidents, breaches, **within 15 days after the end of each quarter**.

The deadline for quarterly cyber incident reporting for the **Q1 (April– June 2026)** is **15th July 2026** in audit web portal, failing which will be treated as non-compliance and penalty will be levied as per communique no: **CDSL/AUDIT/DP/POLCY/2025/105 February 12, 2025**.

For submitting the **quarterly cyber incident report** to CDSL, please refer **Annexure A**.

Queries regarding this communiqué may be sent to dpinfosec@cdslindia.com, or you may contact us on our landline numbers: 022-62343576 / 022-62343461.

For and on behalf of
Central Depository Services (India) Limited

sd/-

Mrugen Vijay Munjpara
Assistant Vice President – Information Security



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Annexure A

Guidelines to submit Quarterly Cyber Incident Report

1. Open the Audit Web Portal.

- Link: <https://auditweb.cdslindia.com/Login.aspx>
- Click on Login Type and select “Designated Officer” login.



AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

User ID: --Select--

Password: [Redacted]

Forgot password Registration for DP / RTA

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

2. Fill the below required information and click on “Sign In” Button:

- User ID, Password & Captcha



AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

User ID: [Empty]

Password: [Empty]

Captcha: 7afff1

Sign In

Forgot password Registration for DP / RTA

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

3. Enter the OTP:

- You will receive the OTP on both your DP's registered mobile number and email Id.



AUDIT APPLICATION

LOGIN OTP

Enter OTP

Enter OTP

OTP Time :- 00:09:57 Do not refresh the page

Verify OTP

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

4. Select required information for submitting quarterly “Cyber Incident” report:

- Select Audit Type: **CYBER INCIDENT REPORT**
- Select Audit Month: **Select quarter month**
- Select DP/RTA: **Select your DP ID**
- Click on the “**Confirm**” Button

AUDIT APPLICATION

Reports

Select Audit Type: CYBER INCIDENT REPORT

Select Audit Month

Select DP / RTA

Confirm

View Cyber Report View Compliance View Resubmission
Cyber Audit Compliance Report Cyber RCA Report



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

- The following screen will appear. Main DP can mention the branch DP IDs , if they are submitting consolidated report for branch DP IDs.

The screenshot shows the 'AUDIT APPLICATION' form. At the top, there is the CDSL logo and the text 'Central Depository Services (India) Limited' with the tagline 'Convenient + Dependable + Secure'. A blue header bar contains the text 'AUDIT APPLICATION'. Below this is a section titled 'CYBER INCIDENT REPORT' with a table containing the following fields:

Audit Type	CYBER INCIDENT REPORT	DP Name(ID)	
Audit Month		Period	
DP ID			

Below the table, there is a text field labeled 'Cyber Incident Report covers the following Branch DPIDs :-' followed by a red-bordered input box.

- Fill in the details in the prescribed format in:

- Letter/Report Subject
- Reporting Periodicity Year
- Designated Officers details. **Change the screenshot**

The screenshot shows the 'Incident Reporting Form' with a green header. The form is divided into three main sections:

- 1. Letter/Report Subject**: Includes fields for 'NAME OF THE DEPOSITORY PARTICIPANT' (CDSL), 'NAME OF DEPOSITORY' (CDSL), and 'MEMBER ID / DP ID'. It also has 'UNIQUE INCIDENT No. :- 1' and 'Financial Year = 2024-2025'.
- 2. Reporting Periodicity Year**: Includes a dropdown menu set to 'QUARTER 4 [JAN-2024 TO MAR-2024]'.
- 3. Designated Officer (Reporting Officer details)**: Includes fields for Name, Title, Phone / Fax No., Address, Organization name, Email ID, and Mobile.

The first two sections are highlighted with a red border in the original image.

- Select the option **NO** in Cyber-attack/breach observed in Quarter: **(If no incident has occurred)**

The screenshot shows the 'Cyber-attack / breach observed in Quarter' form. It has a header with the text 'Cyber-attack / breach observed in Quarter'. Below this is a radio button group with 'Yes' and 'No' options. The 'No' option is selected. There are instructions: '(IF YES, PLEASE FILL ANNEXURE I)' and '(IF NO, PLEASE SUBMIT THE NIL REPORT ONLY AFTER THE END OF QUARTER)'. Below this is a 'DATE & TIME' section with a date picker set to 'dd-MMM-yyyy' and a time picker set to 'Hour', 'Minutes', and 'PM'. Below this is a 'BRIEF INFORMATION ON THE CYBER ATTACK / BREACH OBSERVED' section with a text area. At the bottom, there is a link for 'ANNEXURE I' and a row of buttons: 'Save', 'Submit to CDSL', 'Clear', 'Attach Files', and 'View Incident'.

The Report is submitted as NIL report.



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Please note that if you save the report as **NIL** without submitting it to CDSL, then upon re-login, when you attempt to submit the report, you will receive the following message.

Popup Message --> You are not allowed to submit the Incident, as it is already added/Submit as a NIL Report for this quarter.

If you receive the above popup message, please click on the Submit to CDSL button.

To avoid such popup messages, kindly ensure that the report is first saved and then submitted to CDSL.

8. Select the option **Yes** in Cyber-attack/breach observed in Quarter and fill the below required information: **(if the incident occurred)**

- Date & Time
- Brief information on the Cyber attack
- Then Click on Annexure I

Cyber-attack / breach observed in Quarter

Yes No (If YES, PLEASE FILL ANNEXURE I) (If NO, PLEASE SUBMIT THE NIL REPORT ONLY AFTER THE END OF QUARTER)

* DATE & TIME: 10-Jul-2024 04:15 PM (Select the Date between 01-Jan-2024 To 31-Mar-2024)

* BRIEF INFORMATION ON THE CYBER ATTACK / BREACH OBSERVED: Brief information on the Cyber-attack

[ANNEXURE I](#)

9. Fill the **Annexure I**:

1. Physical location of affected computer/ Network and name of ISP
2. Date incident occurred
3. Information of affected system
4. Select the type/types of incident
5. Description of incident



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Annexure I

1. Physical location of affected computer / Network and name of ISP

Physical location of affected computer / Network and name of ISP

2. Date incident occurred

OccURED *
(Select the Date between 01-Jan-2024 To 31-Mar-2024)

IDENTIFIED *

3. Information of affected system

IP ADDRESS COMPUTER / HOST NAME

LAST PATCHED / UPDATED OPERATING SYSTEM (INCL. VER / RELEASE NO.)

HARDWARE VENDOR / MODEL

4. Type of incident

PHISHING WEBSITE DEFAECMENT BOT/BOTNET DISTRIBUTED DENIAL OF SERVICE(DDoS) SOCIAL ENGINEERING RANSOMWARE

NETWORK SCANNING / PROBING BREAK-IN/ROOT SYSTEM MISUSE EMAIL SPOOFING USER ACCOUNT COMPROMISE TECHNICAL VULNERABILITY OTHER

VIRUS/MALICIOUS CODE SPAM DENIAL OF SERVICE(DoS) WEBSITE INTRUSION IP SPOOFING

5. Description of Incident

Description of incident

10. Fill the below Information:

- Select Unusual behaviour/symptoms (Tick the symptoms)
- Fill the Details of unusual behaviour/symptoms
- Has this problem been experienced earlier? If Yes, Give the description

6. Unusual behavior/symptoms (Tick the symptoms)

<input type="checkbox"/> SYSTEM CRASHES	<input type="checkbox"/> CHANGES IN FILE LENGTHS OR DATES
<input type="checkbox"/> NEW USER ACCOUNTS/ ACCOUNTING DISCREPANCIES	<input type="checkbox"/> ATTEMPTS TO WRITE TO SYSTEM
<input type="checkbox"/> FAILED OR SUCCESSFUL SOCIAL ENGINEERING ATTEMPTS	<input type="checkbox"/> DATA MODIFICATION OR DELETION
<input type="checkbox"/> UNEXPLAINED, POOR SYSTEM PERFORMANCE	<input type="checkbox"/> DENIAL OF SERVICE
<input type="checkbox"/> UNACCOUNTED FOR CHANGES IN THE DNS TABLES, ROUTER RULES, OR FIREWALL RULES	<input type="checkbox"/> DOOR KNOB RATTLING
<input type="checkbox"/> UNEXPLAINED ELEVATION OR USE OF PRIVILEGES OPERATION OF A PROGRAM OR SNIFFER DEVICE TO CAPTURE NETWORK TRAFFIC	<input type="checkbox"/> UNUSUAL TIME OF USAGE
<input type="checkbox"/> AN INDICATED LAST TIME OF USAGE OF A USER ACCOUNT THAT DOES NOT CORRESPOND TO THE ACTUAL LAST TIME OF USAGE FOR THAT USER	<input type="checkbox"/> UNUSUAL USAGE PATTERNS
<input type="checkbox"/> A SYSTEM ALARM OR SIMILAR INDICATION FROM AN INTRUSION DETECTION TOOL	<input type="checkbox"/> UNUSUAL LOG FILE ENTRIES
<input type="checkbox"/> ALTERED HOME PAGES, WHICH ARE USUALLY THE INTENTIONAL TARGET FOR VISIBILITY, OR OTHER PAGES ON THE WEB SERVER	<input type="checkbox"/> PRESENCE OF NEW SETUID OR SETGID FILES CHANGES IN SYSTEM DIRECTORIES AND FILES
<input type="checkbox"/> ANOMALIES	<input type="checkbox"/> PRESENCE OF CRACKING UTILITIES
<input type="checkbox"/> SUSPICIOUS PROBES	<input type="checkbox"/> ACTIVITY DURING NON-WORKING HOURS OR HOLIDAYS
<input type="checkbox"/> SUSPICIOUS BROWSING NEW FILES	<input type="checkbox"/> OTHER

7. Details of unusual behavior/symptoms

Details of unusual behavior

8. Has this problem been experienced earlier? If Yes, details Yes No



Central Depository Services (India) Limited

Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

11. Fill the below Information:

- Agencies notified
- IP Address of apparent or suspected source
- How many host(s) are affected?

9. Agencies notified

LAW ENFORCEMENT	<input type="text" value="Law Enforcement"/>	PRIVATE AGENCY	<input type="text" value="Private Agency"/>
AFFECTED PRODUCT VENDOR	<input type="text"/>	OTHER	<input type="text"/>

10. IP Address of apparent or suspected source

SOURCE IP ADDRESS	<input type="text"/>	OTHER INFORMATION AVAILABLE	<input type="text"/>
-------------------	----------------------	-----------------------------	----------------------

11. How many host(s) are affected?

1 to 10 10 to 100 MORE THAN 100

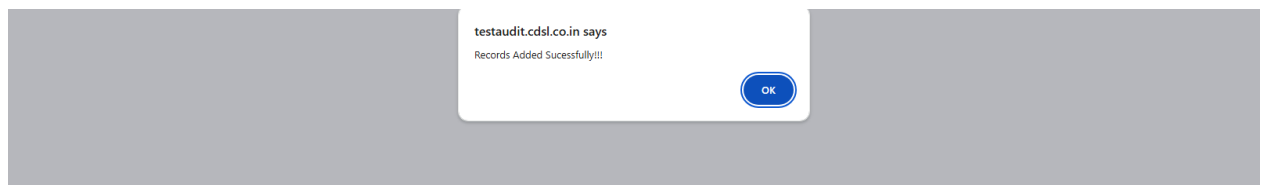
12. Details of actions taken for mitigation and any preventive measure applied

[Save](#) [Submit to CDSL](#) [Attach Files](#) [View Incident](#)

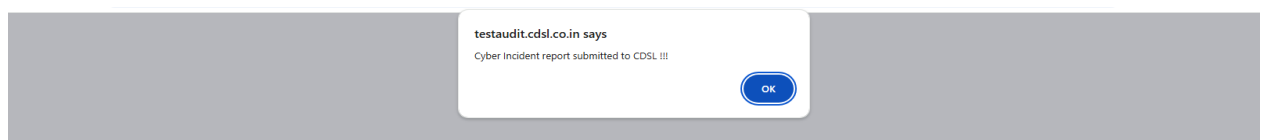
Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

Attach Files: Click "**Attach Files**" to upload relevant documents.

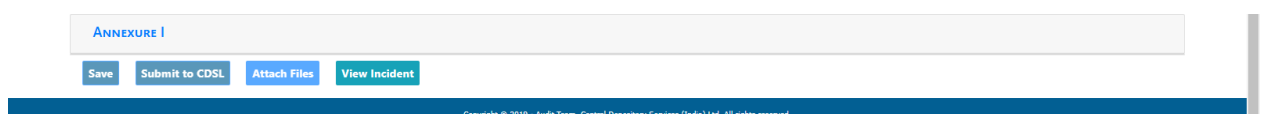
Save: Click "Save" to save your information as a draft.



Records are added successfully



Submit to CDSL: Click "**Submit to CDSL**" to officially submit your report.



View Incident: Click "**View Incident**" to see your submitted reports history.



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Note:

- All incidents report activities must be completed in one continuous action, from saving to submitting the incident report.
- Once you submit the incident report, it cannot be submitted again.
- When you re-login, the scheduled month/DP ID will not appear, that means you have already submitted the incident report.
