



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2026/685

October 01, 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 Communiqué No. **CDSL/OPS/DP/POLCY/2025/27** dated January 10, 2025, wherein all cyber-attacks, threats, cyber incidents, and breaches experienced by Depository Participants (DPs) are required to be reported to CDSL.

In view of the above, all DPs are required to submit the **Quarterly Cyber Incident Report** through the **Audit Web Portal within 15 days from the end of each quarter**. This reporting requirement is mandatory for all DPs, irrespective of whether any cyber-attacks, threats, incidents, or breaches were observed during the quarter.

In cases where no such event has occurred during the quarter, the DP shall submit a **Nil Report** by selecting "**No**" under the field "**Cyber-attack/Breach observed in the Quarter.**" Failure to submit a Nil Report shall be treated as non-submission of the Quarterly Cyber Incident Report.

The deadline for submission of the **Quarterly Cyber Incident Report for Q2 (July–September 2026)** through the Audit Web Portal is **October 15, 2026**. Failure to submit the report within the prescribed timeline shall be treated as non-compliance, and the applicable penalty shall be levied in accordance with **CDSL Communiqué No. CDSL/AUDIT/DP/POLCY/2025/105** dated **February 12, 2025**.

For instructions on submitting the Quarterly Cyber Incident Report to CDSL, please refer to **Annexure A**.

Queries regarding this communiqué may be sent to [dpinfosec@cdslindia.com](mailto: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/-

Urmila Chougule  
Senior Manager - Audit, Inspection & Compliance





# Central Depository Services (India) Limited

Convenient \* Dependable \* Secure

## COMMUNIQUE 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: **QUARTERLY CYBER INCIDENT REPORT**
- Select Audit Month: **Select quarter month**
- Select DP/RTA: **Select your DP ID**
- Click on the "Confirm" Button

### AUDIT APPLICATION

|                    |                                 |   |
|--------------------|---------------------------------|---|
| Select Audit Type  | QUARTERLY CYBER INCIDENT REPORT | ▼ |
| Select Audit Month |                                 | ▼ |
| Select DP / RTA    |                                 | ▼ |

Confirm

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



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

| AUDIT APPLICATION                                                                                                                                                                           |                     |                        |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|------------------------|---|
| <b>QUARTERLY INCIDENT REPORTING FORM</b>                                                                                                                                                    |                     |                        |   |
| Date                                                                                                                                                                                        | 29-09-2026 17:52:19 | DP Name(ID)            |   |
| DP ID                                                                                                                                                                                       |                     | UNIQUE INCIDENT No. :- | 1 |
| FINANCIAL YEAR                                                                                                                                                                              | 2026-2027           | Quarter                |   |
| <small>Last date of Submission 15-Jan-2026 . If the report is submitted after this date, then it will be treated as Late Submission. Fields marked with Asterisk (*) are mandatory.</small> |                     |                        |   |
| Quarterly Incident Report covers the following Branch DPIDs :-                                                                                                                              |                     |                        |   |

6. Fill in the details in the prescribed format in:

1. DP Name
2. DP ID
3. Quarter
4. Designated Officers details.

| QUARTERLY INCIDENT REPORTING FORM                                                                                                                                                           |                      |                         |                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------------------|------------------------|
| Date                                                                                                                                                                                        | 29-09-2026 17:52:19  | DP Name(ID)             |                        |
| DP ID                                                                                                                                                                                       |                      | UNIQUE INCIDENT No. :-  | 2                      |
| FINANCIAL YEAR                                                                                                                                                                              | 2026-2027            | Quarter                 |                        |
| <small>Last date of Submission 15-Jan-2026 . If the report is submitted after this date, then it will be treated as Late Submission. Fields marked with Asterisk (*) are mandatory.</small> |                      |                         |                        |
| Quarterly Incident Report covers the following Branch DPIDs :-                                                                                                                              |                      |                         |                        |
| <b>1. Designated Officer (Reporting Officer details)</b>                                                                                                                                    |                      |                         |                        |
| * NAME                                                                                                                                                                                      | Name                 | * DESIGNATION           | Designation name       |
| * MOBILE                                                                                                                                                                                    | Mobile               | * EMAIL ID              | Email ID               |
| ALTERNATE MOBILE NO.                                                                                                                                                                        | Alternate Mobile no. | ALTERNATE OFFICER NAME. | Alternate Officer Name |
| ADDRESS                                                                                                                                                                                     | Address              |                         |                        |

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

| Cyber-attack / breach observed in Quarter                                                                                                                                |                                                                                      |       |                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------|----------------------------|
| <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No (If YES, PLEASE FILL ANNEXURE I) (If NO, PLEASE SUBMIT THE NIL REPORT ONLY AFTER THE END OF QUARTER) |                                                                                      |       |                            |
| DATE & TIME                                                                                                                                                              | dd-MMM-yyyy Hour Minutes PM<br>(Select the Date between 01-Jul-2023 To 30-Sep-2023 ) |       |                            |
| BRIEF INFORMATION ON THE CYBER ATTACK / BREACH OBSERVED                                                                                                                  | Brief information on the Cyber-attack                                                |       |                            |
| ANNEXURE I                                                                                                                                                               |                                                                                      |       |                            |
| Save                                                                                                                                                                     | Submit to CDSL                                                                       | Clear | Attach Files View Incident |

The Report is submitted as NIL report.

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.



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

**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. Details Cyber-attack / breach observed
2. Type of incident
3. Physical location of affected computer / Network and name of ISP
4. Information of affected system
5. IP Address of apparent or suspected source
6. How many host(s) are affected?
7. Unusual behavior/symptoms (Tick the symptoms)



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

### 1. Details Cyber-attack / breach observed

\* INCIDENT DATE & TIME

\* INCIDENT NOTICED/DETECTED DATE & TIME

\* BRIEF INFORMATION ON THE CYBER ATTACK / BREACH OBSERVED

### 2. Type of Incident \*

- |                                                                   |                                         |                                                              |                                                  |                                                                      |                                                             |
|-------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------|
| <input type="checkbox"/> PHISHING                                 | <input type="checkbox"/> SYSTEM MISUSE  | <input type="checkbox"/> DENIAL OF SERVICE(DoS)              | <input type="checkbox"/> SOCIAL ENGINEERING      | <input type="checkbox"/> DATA BREACH                                 | <input type="checkbox"/> IMPERSONATING                      |
| <input type="checkbox"/> NETWORK SCANNING / PROBING BREAK-IN/ROOT | <input type="checkbox"/> SPAM           | <input type="checkbox"/> DISTRIBUTED DENIAL OF SERVICE(DDoS) | <input type="checkbox"/> TECHNICAL VULNERABILITY | <input type="checkbox"/> DATA LEAKED AFFECTING SYSTEM/SERVER/NETWORK | <input type="checkbox"/> UNAUTHORIZED ACCESS IT/SYSTEM DATA |
| <input type="checkbox"/> VIRUS/MALICIOUS CODE                     | <input type="checkbox"/> BOT/BOTNET     | <input type="checkbox"/> USER ACCOUNT COMPROMISE             | <input type="checkbox"/> IP SPOOFING             | <input type="checkbox"/> ATTACK ON INTERNET OF THINGS (IOT) DEVICE   | <input type="checkbox"/> OTHER                              |
| <input type="checkbox"/> WEBSITE DEFACEMENT                       | <input type="checkbox"/> EMAIL SPOOFING | <input type="checkbox"/> WEBSITE INTRUSION                   | <input type="checkbox"/> RANSOMWARE              | <input type="checkbox"/> IDENTITY THEFT AND PHISHING ATTACK          |                                                             |

Others Please Specify (If the Type Of Incident Selected As OTHERS then it is compulsory to specify the Description of Incident )

Description of incident

### 3. Physical location of affected computer / Network and name of ISP

Physical location of affected computer / Network and name of ISP

### 4. Information of affected system

|                                                                     |                                                                                          |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| IP Address <input type="text"/>                                     | COMPUTER / HOST NAME <input type="text"/>                                                |
| LAST PATCHED / UPDATED <input type="text" value="dd-MMM-yyyy"/>     | OPERATING SYSTEM (INCL. VER / RELEASE NO.) <input type="text" value="Operating System"/> |
| HARDWARE VENDOR / MODEL <input type="text" value="Hardware model"/> |                                                                                          |

### 5. IP Address of apparent or suspected source

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

### 6. How many host(s) are affected?

☐ 1 to 10 ☐ 10 to 100 ☐ MORE THAN 100

### 7. 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                                                                          |



# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

Others Please Specify (If the unusual behavior/symptoms Selected As OTHERS then it is compulsory to specify the Details of unusual behavior/symptoms )

Details of unusual behavior

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

9. Agencies notified

|                         |                          |        |             |
|-------------------------|--------------------------|--------|-------------|
| * CERT-IN               | <input type="checkbox"/> | * DATE | dd-MMM-yyyy |
| * SEBI                  | <input type="checkbox"/> | * DATE | dd-MMM-yyyy |
| * NCIIPC                | <input type="checkbox"/> | * DATE | dd-MMM-yyyy |
| LAW ENFORCEMENT         | Law Enforcement          | DATE   | dd-MMM-yyyy |
| PRIVATE AGENCY          | Private Agency           | DATE   | dd-MMM-yyyy |
| AFFECTED PRODUCT VENDOR | Affected Product Vendor  | DATE   | dd-MMM-yyyy |
| OTHERS, PLEASE SPECIFY  | Others, please Specify   | DATE   | dd-MMM-yyyy |

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

11. Declaration

☐ I hereby declare that the details and information above are complete and true to the best of my knowledge.

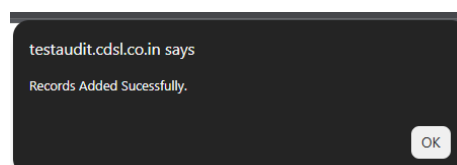
10. Fill the above Information:

- Others Please Specify (If the unusual behavior/symptoms Selected as OTHERS then it is compulsory to specify the Details of unusual behavior/symptoms)
8. Has this problem been experienced earlier? If yes, details
9. Agencies notified
10. Details of actions taken for mitigation and any preventive measure applied
11. Declaration

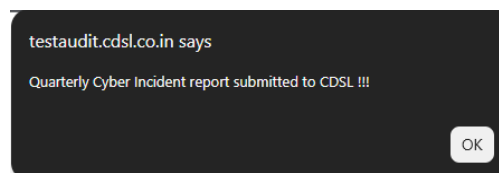
**Attach Files:** Click "**Attach Files**" to upload relevant documents.

**Attach Files**  No file chosen

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



Records are added successfully





# Central Depository Services (India) Limited

Convenient + Dependable + Secure

## COMMUNIQUE TO DEPOSITORY PARTICIPANTS

---

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

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

**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.

\*\*\*