CDSL/OPS/DP/POLCY/2025/203 **March 27, 2025**

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 hereby informed that CDSL has developed a facility for online submission for quarterly cyber incident reporting through audit web portal. 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 quarter Jan' 2025 – Mar' 2025 is **15th April, 2025 in audit web portal.**

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

Queries regarding this communiqué may be addressed to CDSL –emails may be sent to: dpinfosec@cdslindia.com and connect through our IVR Number 022-62343333.

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

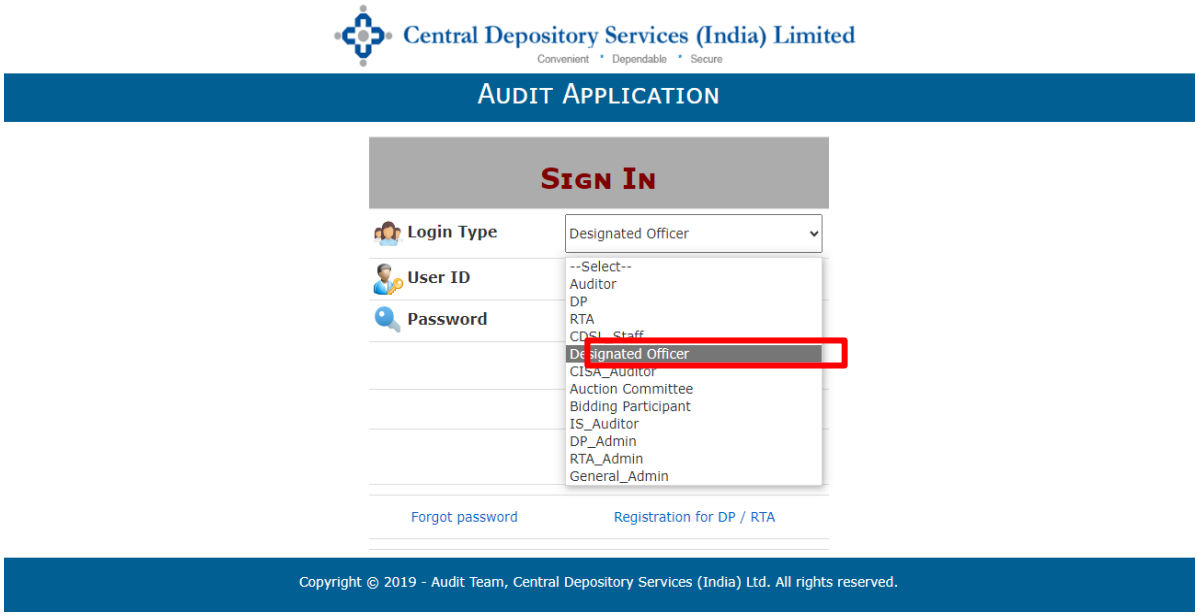
sd/-

Prasad Chawathe
Assistant Vice President – Information Security

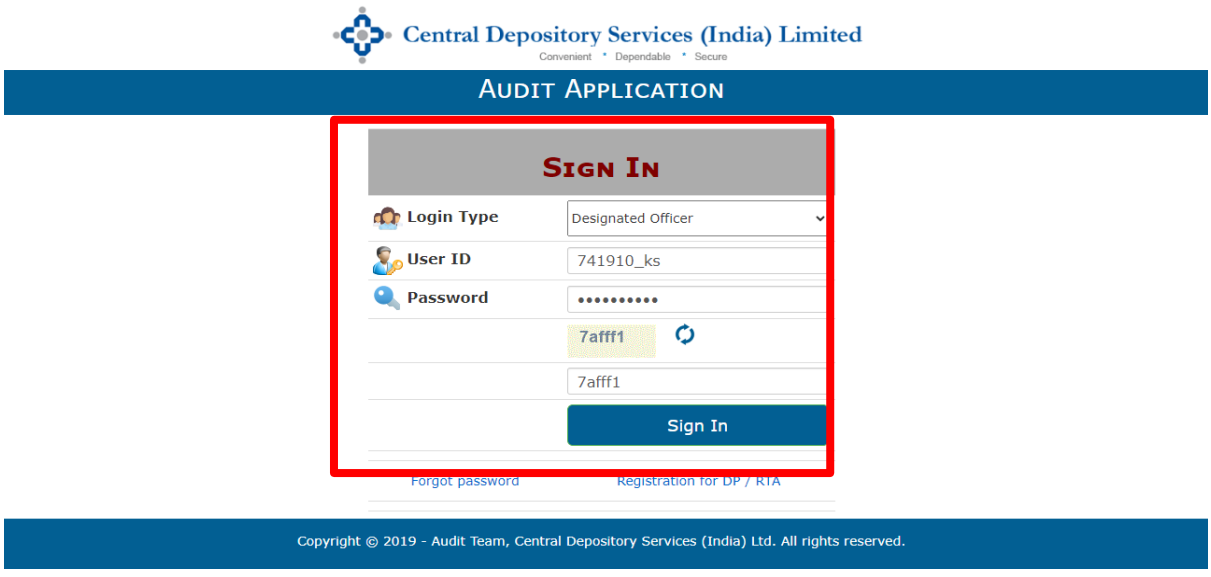
Annexure A

Guidelines to submit Quarterly Cyber Incident Report

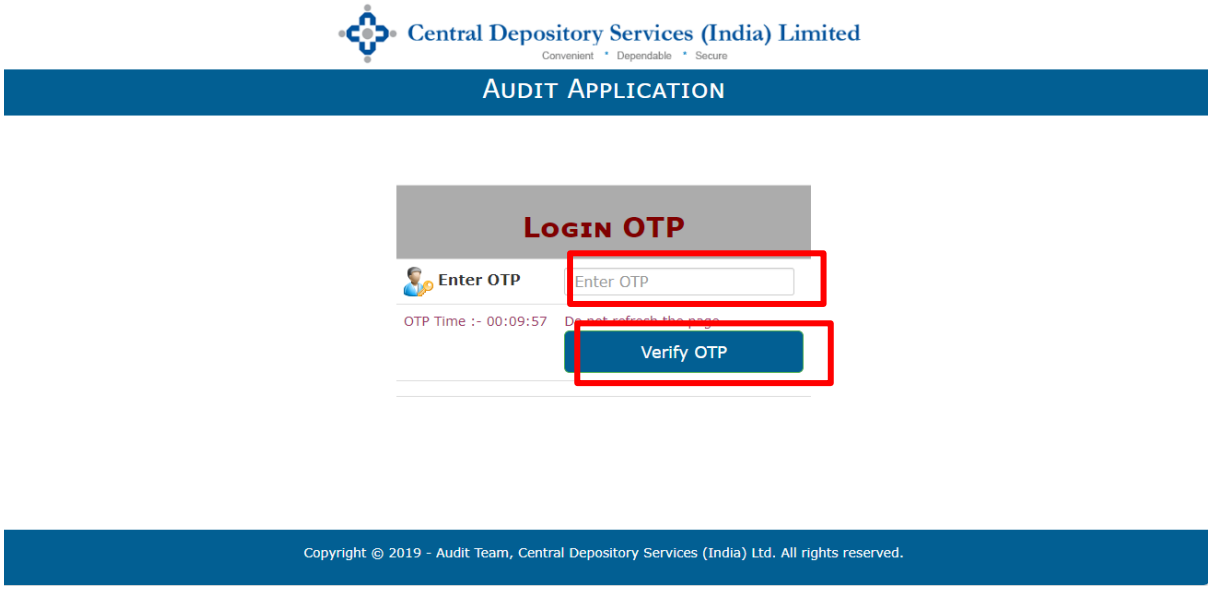
1. Open the Audit Web Portal.
   - Link: https://auditweb.cdslindia.com/Login.aspx
   - Click on Login Type and select "**Designated Officer**" login.



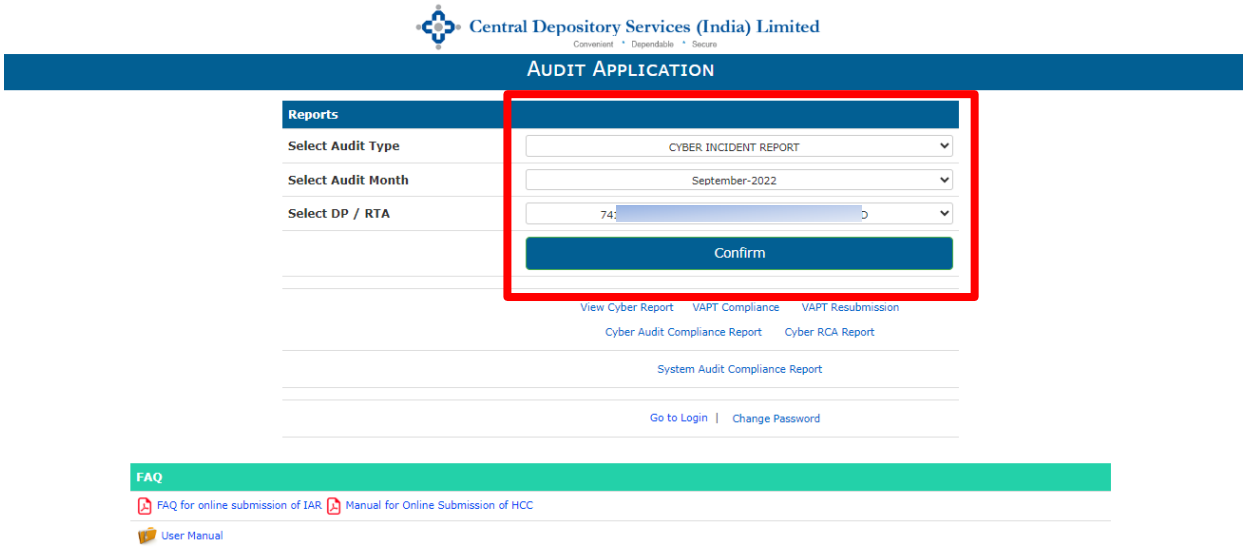
2. Fill the below required information and click on "**Sign In**" Button:
   - User ID, Password & Captcha



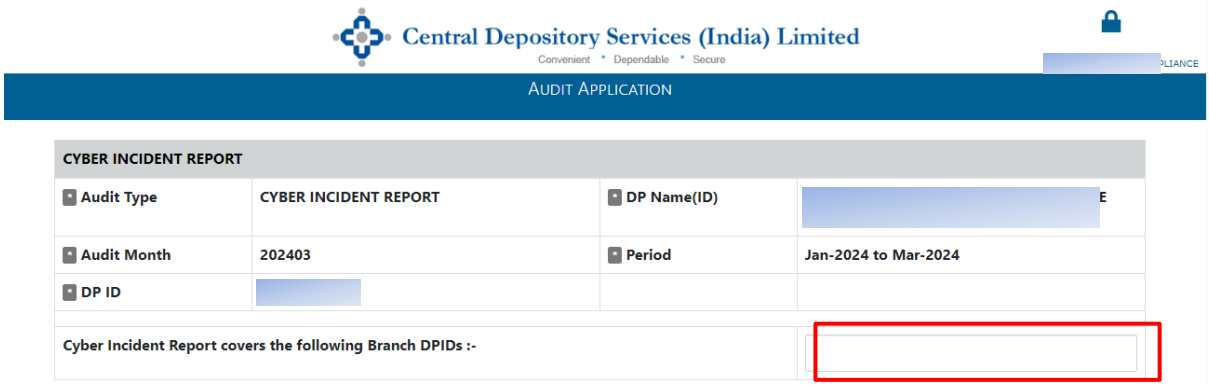
3. Enter the OTP:
    - You will receive the OTP on both your DP's registered mobile number and email Id.



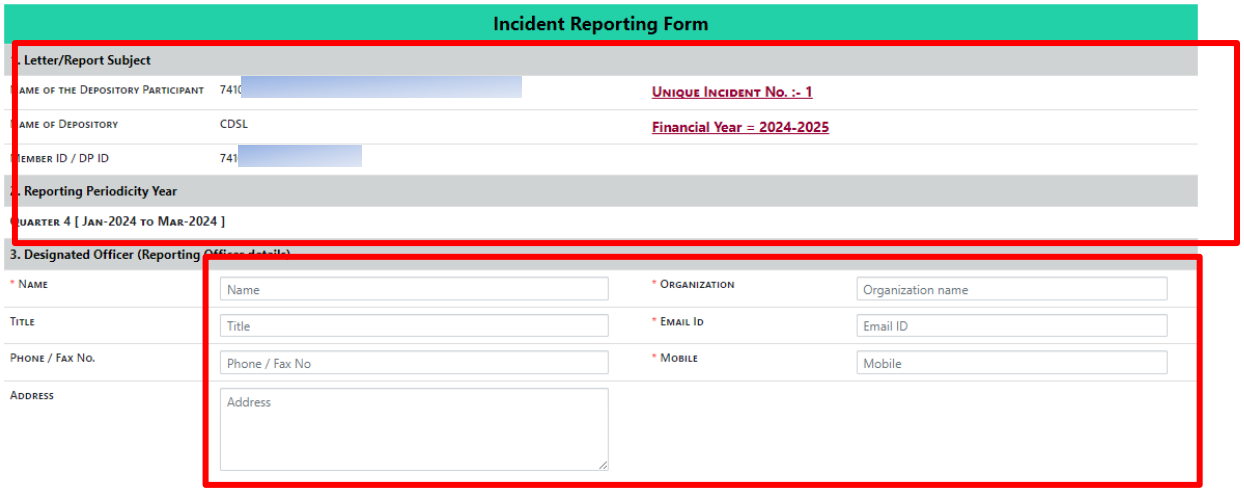
4. Select required information for submitting **quarterly** "**Cyber Incident**" report:
    - Select Audit Type: **CYBER INCIDENT REPORT**
    - Select Audit Month: **Select quarter month**
    - Select DP/RTA: **Select your DP ID**
    - Click on the "**Confirm**" Button



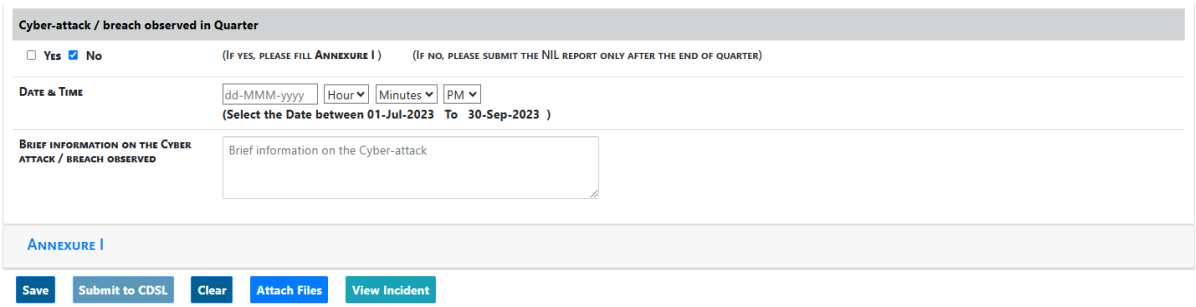
5. The following screen will appear. Main DP can mention the branch DP IDs , if they are submitting consolidated report for branch DP IDs.



6. Fill in the details in the prescribed format in:
   1. **Letter/Report Subject**
   2. **Reporting Periodicity Year**
   3. **Designated Officers details**.

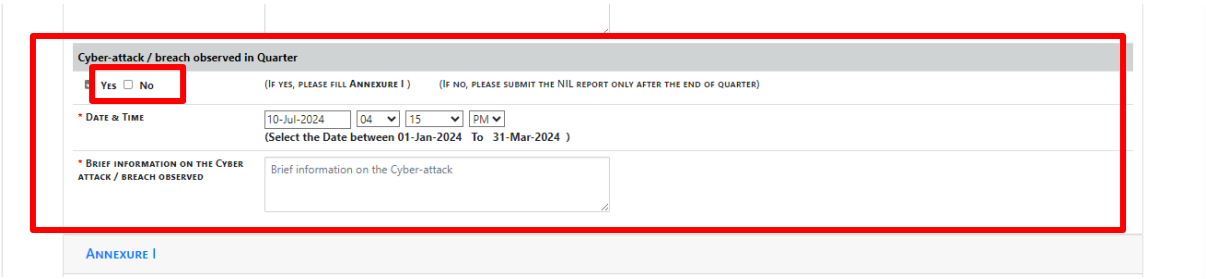


7. Select the option **NO** in Cyber-attack/breach observed in Quarter: **(If no incident has occurred)**

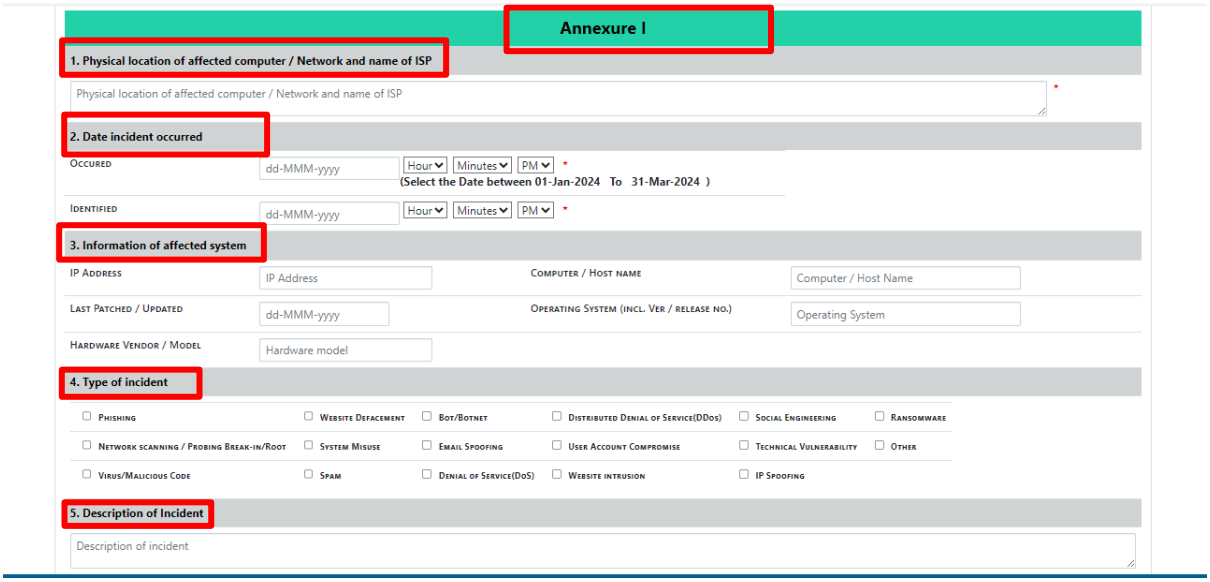


The Report is submitted as NIL report.

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



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



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 dd-MMM-yyyy Hour Minutes PM *
(Select the Date between 01-Jan-2024 To 31-Mar-2024)

IDENTIFIED dd-MMM-yyyy Hour Minutes PM *

3. Information of affected system

IP ADDRESS IP Address | COMPUTER / HOST NAME Computer / Host Name

LAST PATCHED / UPDATED dd-MMM-yyyy | OPERATING SYSTEM (INCL. VER / RELEASE NO.) Operating System

HARDWARE VENDOR / MODEL Hardware model

4. Type of incident

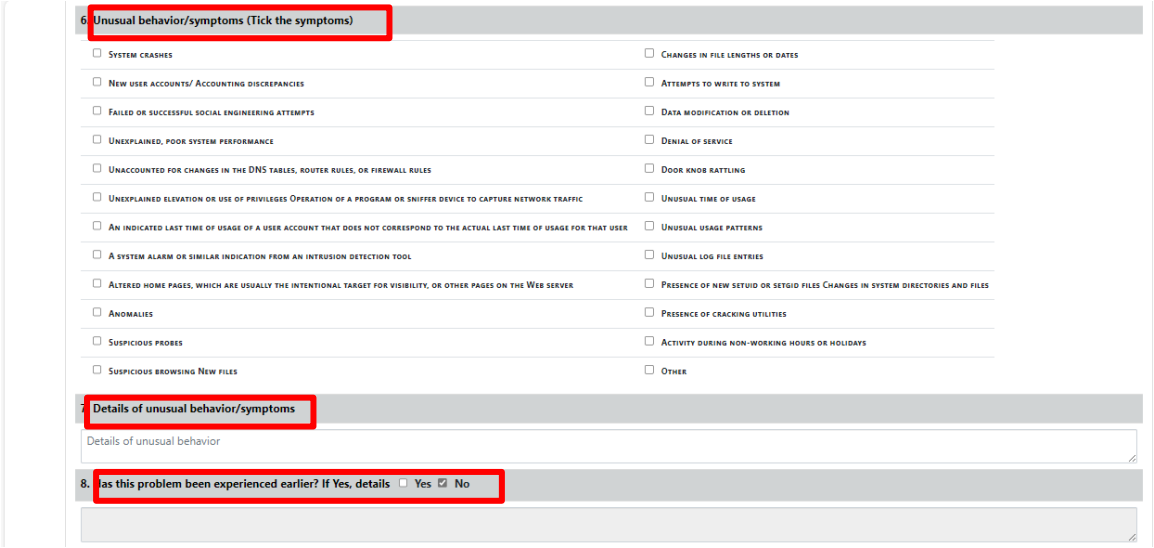
☐ PHISHING ☐ WEBSITE DEFACEMENT ☐ BOT/BOTNET ☐ DISTRIBUTED DENIAL OF SERVICE(DDOS) ☐ SOCIAL ENGINEERING ☐ RANSOMWARE
☐ NETWORK SCANNING / PROBING BREAK-IN/ROOT ☐ SYSTEM MISUSE ☐ EMAIL SPOOFING ☐ USER ACCOUNT COMPROMISE ☐ TECHNICAL VULNERABILITY ☐ OTHER
☐ VIRUS/MALICIOUS CODE ☐ SPAM ☐ DENIAL OF SERVICE(DOS) ☐ 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)

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

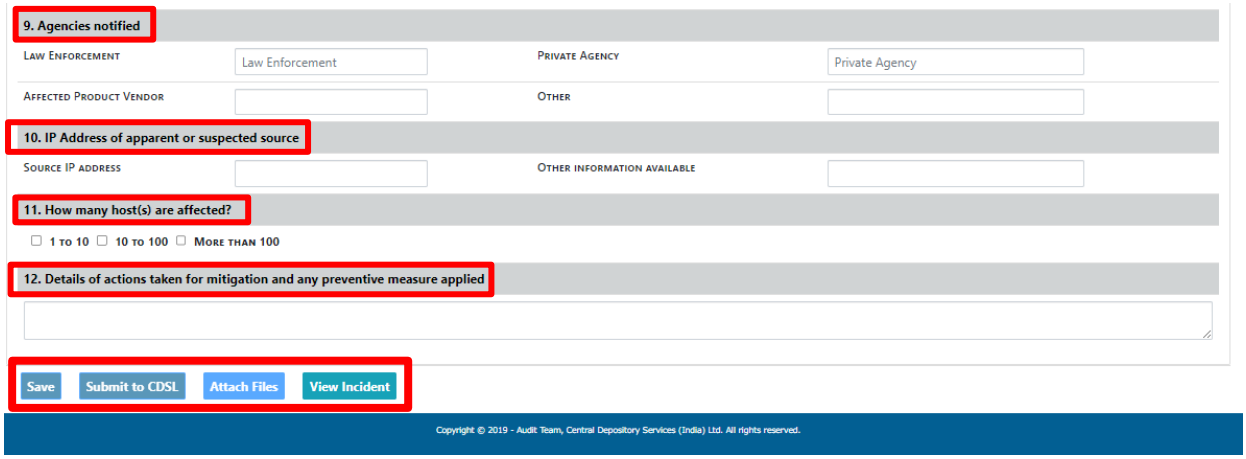
7. Details of unusual behavior/symptoms

Details of unusual behavior

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

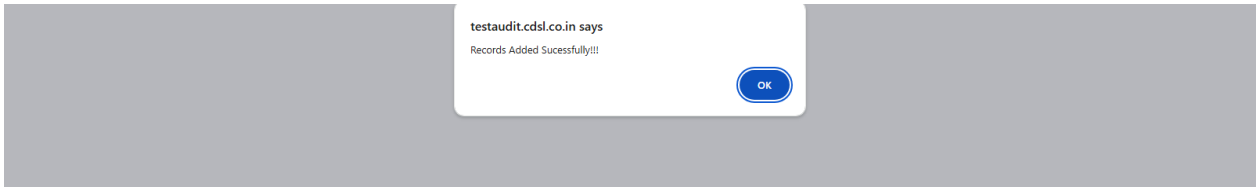
11. Fill the below Information:

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

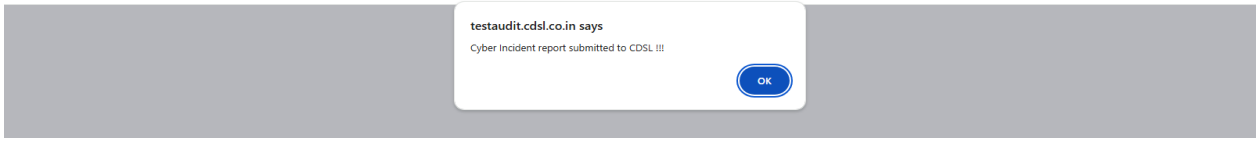


Attach Files: Click "**Attach Files**" to upload relevant documents.

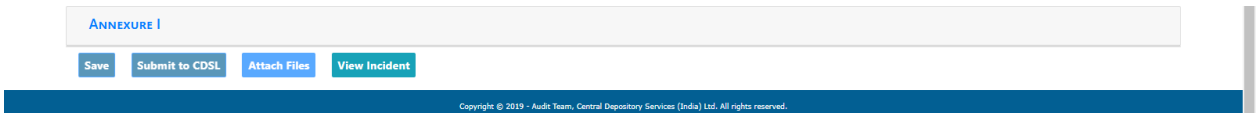
Save: Click "Save" to save your information as a draft.



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.**

***