Central Depository Services (India) Limited

Convenient ⌖ Dependable ⌖ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/IS/DP/POLCY/2026/221 **March 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 hereby informed that CDSL has a facility for online submission for quarterly cyber incident reporting through an 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 **Q4 (January– March 2026)** is **15th April 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 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

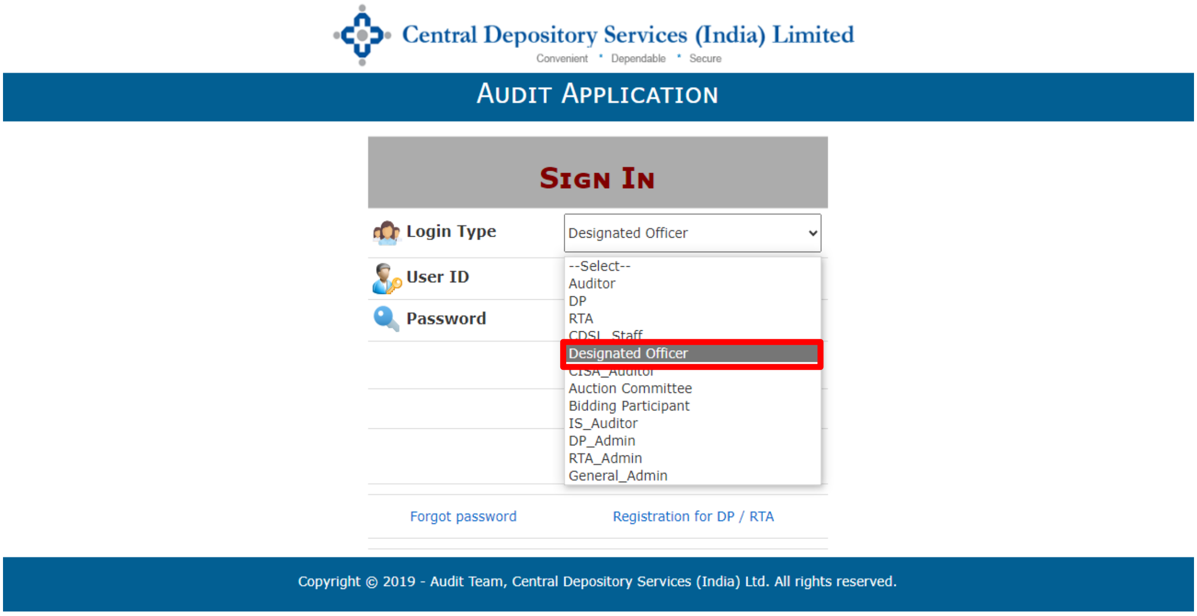
sd/-

Mrugen Vijay Munjpara
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.



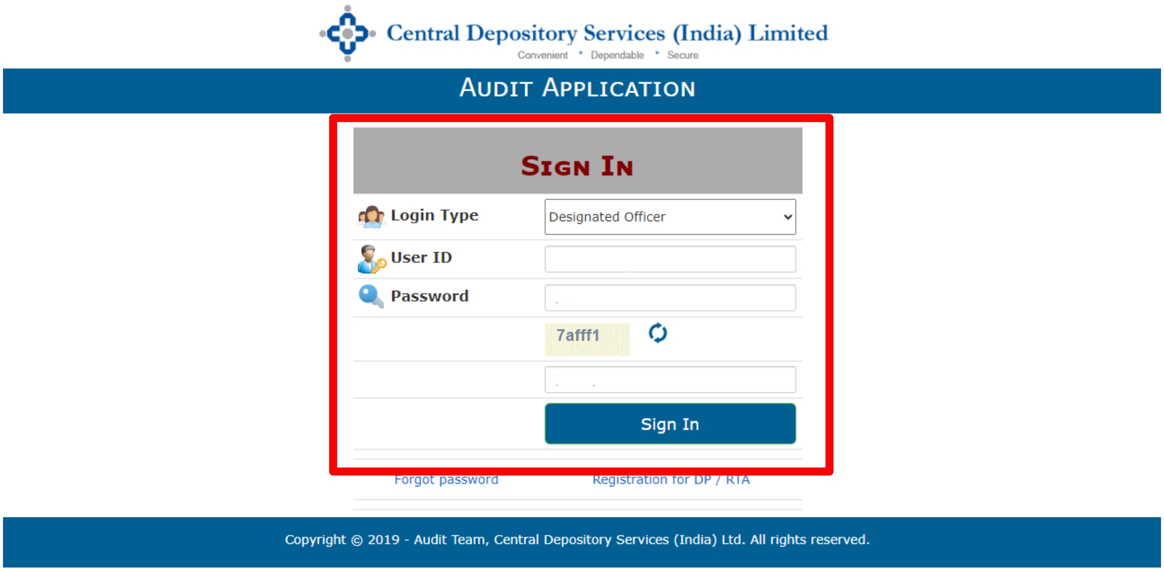
Central Depository Services (India) Limited
Convenient • Dependable • Secure
AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

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



Central Depository Services (India) Limited
Convenient • Dependable • Secure
AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

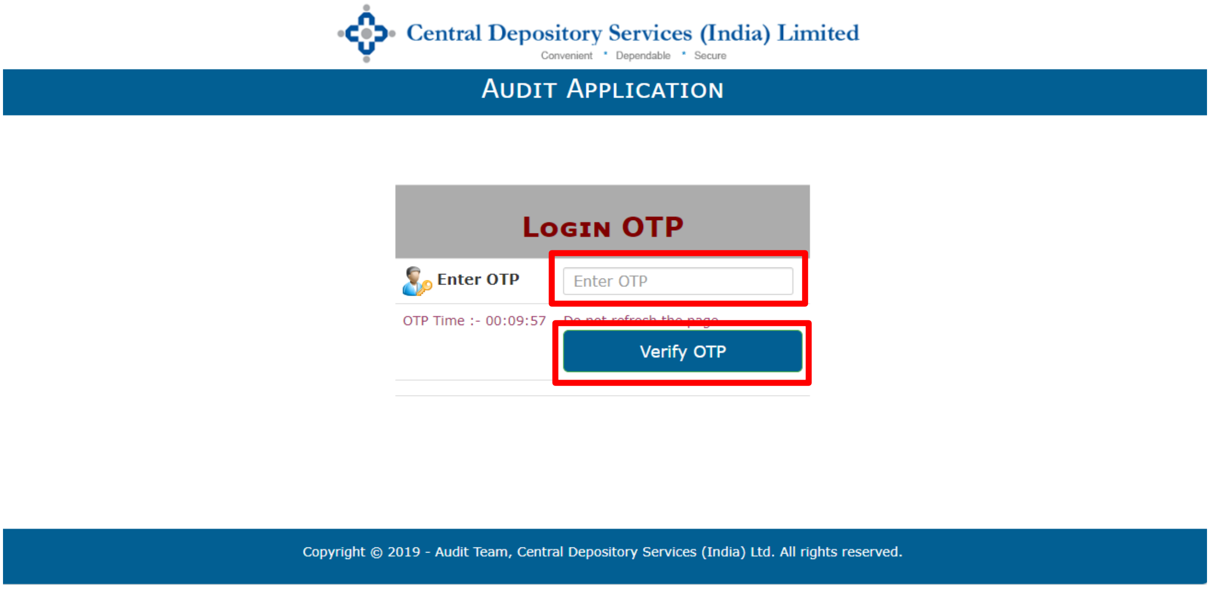
User ID:

Password:

7afff1

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

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



Central Depository Services (India) Limited
Convenient • Dependable • Secure

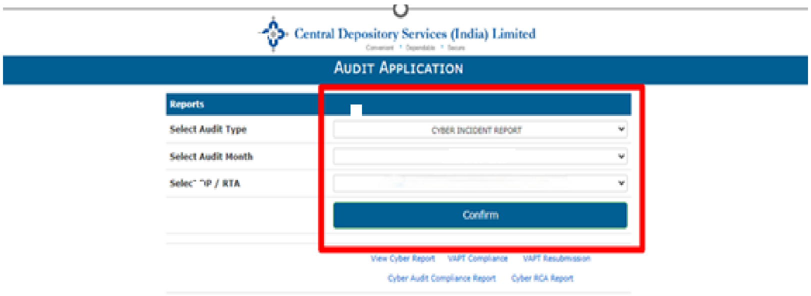
AUDIT APPLICATION

LOGIN OTP

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

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

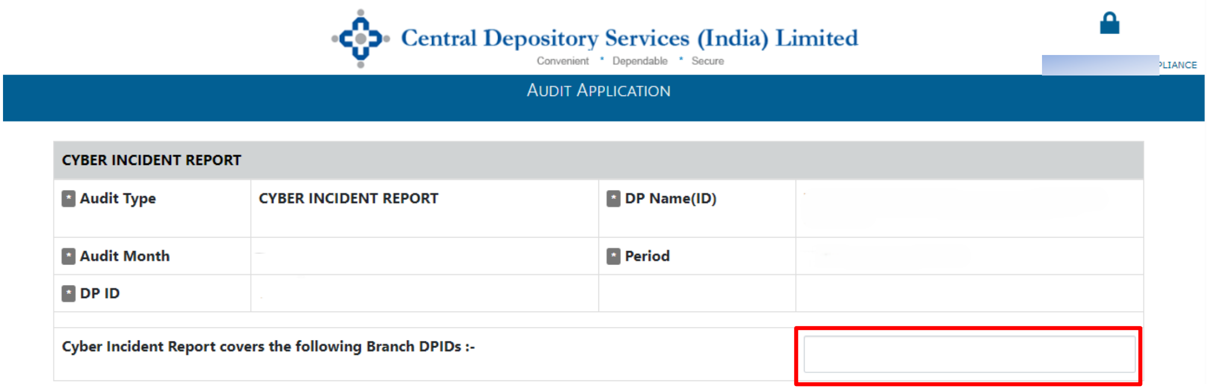


Central Depository Services (India) Limited
Convenient • Dependable • Secure

AUDIT APPLICATION

Reports	
Select Audit Type	CYBER INCIDENT REPORT
Select Audit Month	
Selec" "P / RTA	

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



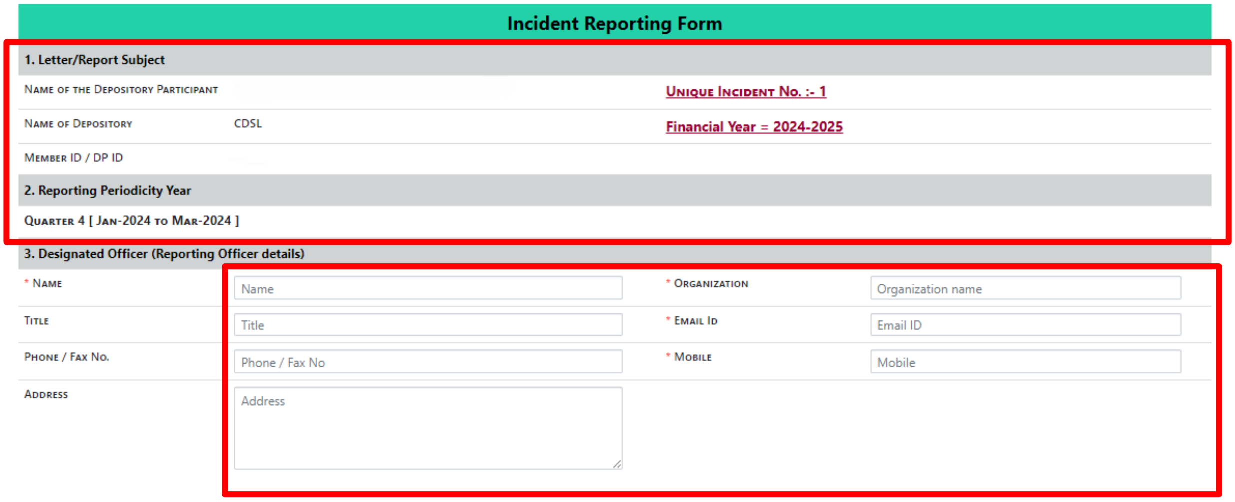
Central Depository Services (India) Limited
Convenient • Dependable • Secure

AUDIT APPLICATION

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

Cyber Incident Report covers the following Branch DPIDs :-

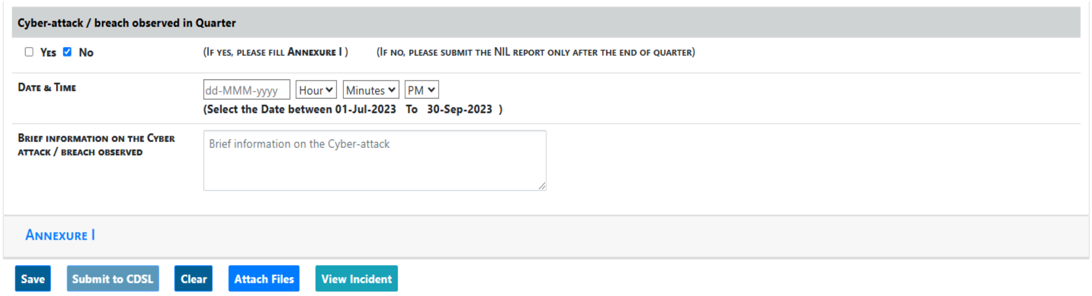
6. Fill in the details in the prescribed format in:
   1. **Letter/Report Subject**
   2. **Reporting Periodicity Year**
   3. **Designated Officers details**.



Incident Reporting Form

1. Letter/Report Subject			
NAME OF THE DEPOSITORY PARTICIPANT		**UNIQUE INCIDENT NO. :- 1**	
NAME OF DEPOSITORY	CDSL	**Financial Year = 2024-2025**	
MEMBER ID / DP ID			
2. Reporting Periodicity Year			
QUARTER 4 [JAN-2024 TO MAR-2024]			
3. Designated Officer (Reporting Officer details)			
* NAME	Name	* ORGANIZATION	Organization name
TITLE	Title	* EMAIL ID	Email ID
PHONE / FAX NO.	Phone / Fax No	* MOBILE	Mobile
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

□ YES ☑ 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 ▾ (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

The Report is submitted as NIL report.

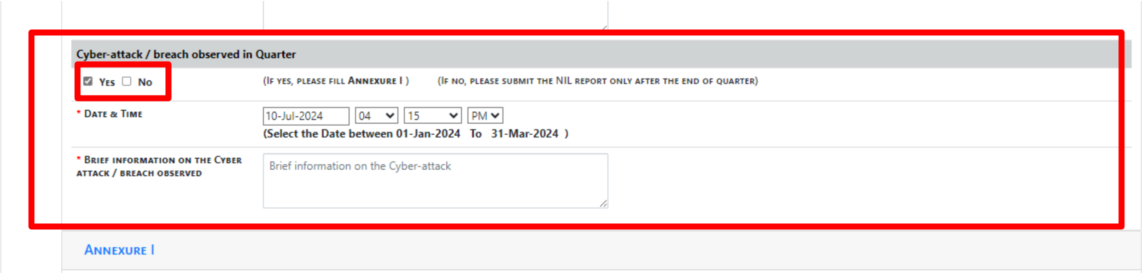
Please note that if you save the report as **NIL** without submitting it to CDSL, then upon re-login, when you attempt to submit the report, you will receive the following message.

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



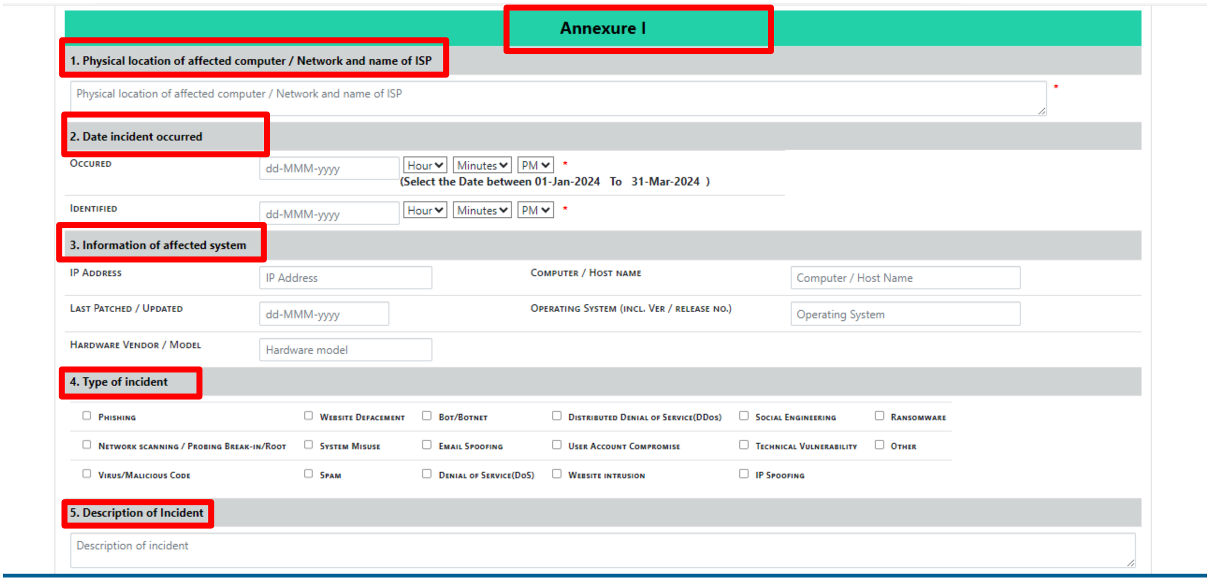
Cyber-attack / breach observed in Quarter

☑ 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

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

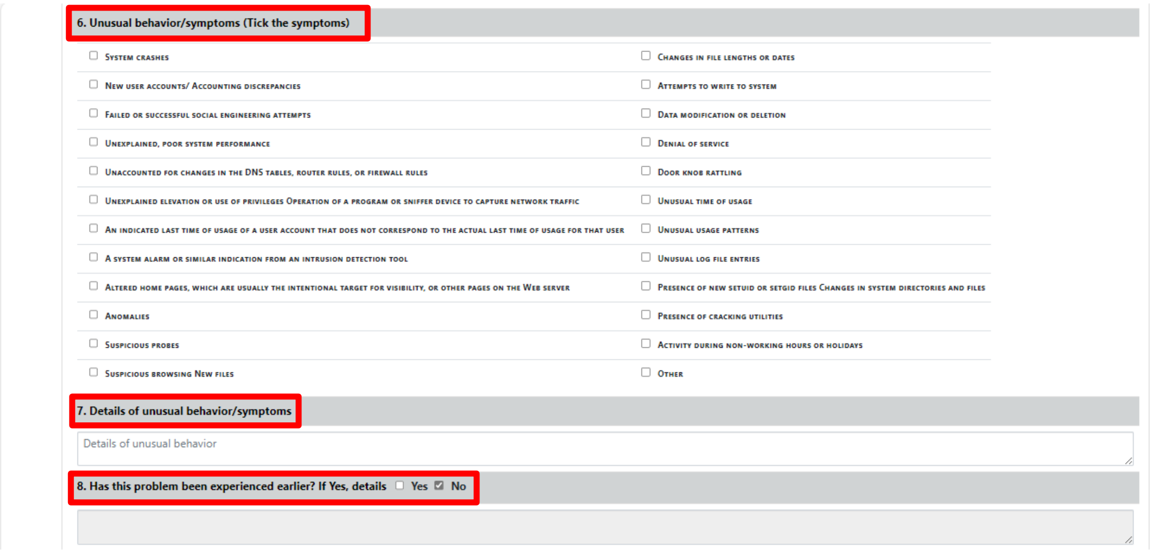
□ Phishing	□ Website Defacement	□ Bot/Botnet	□ Distributed Denial of Service(DDos)	□ Social Engineering	□ Ransomware
□ Network scanning / Probing Break-in/Root	□ System Misuse	□ Email Spoofing	□ User Account Compromise	□ Technical Vulnerability	□ Other
□ Virus/Malicious Code	□ Spam	□ Denial of Service(DoS)	□ 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

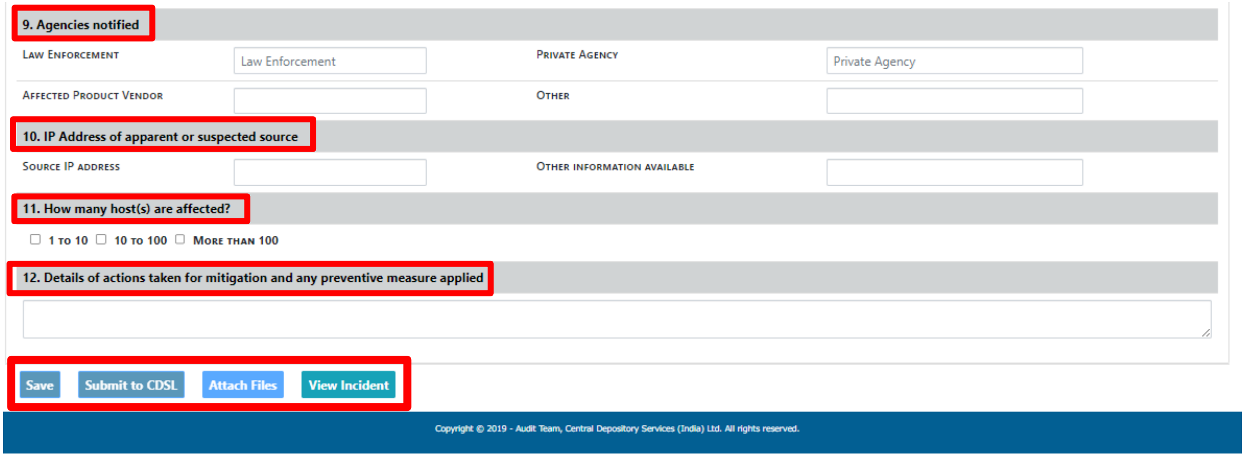
7. Details of unusual behavior/symptoms

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?



9. Agencies notified

Law Enforcement: Law Enforcement
Private Agency: Private Agency
Affected Product Vendor:
Other:

10. IP Address of apparent or suspected source

Source IP address:
Other information available:

11. How many host(s) are affected?

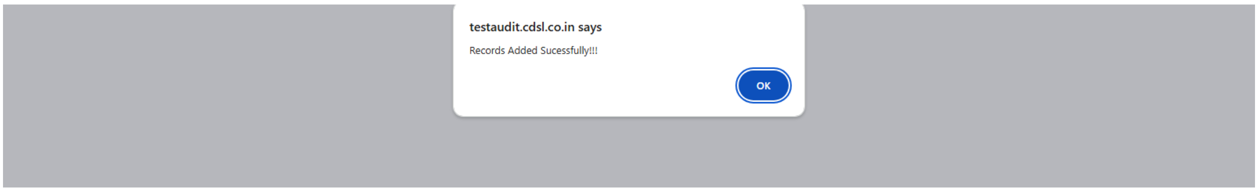
☐ 1 to 10 ☐ 10 to 100 ☐ More than 100

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

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

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

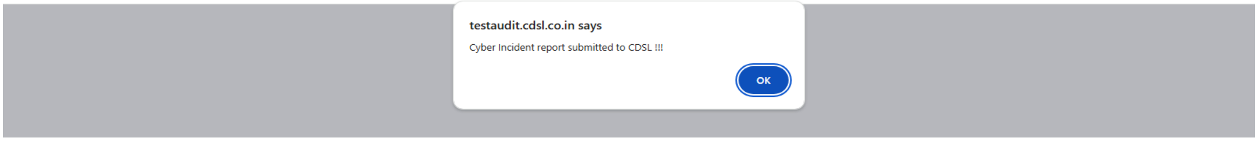
Save: Click "Save" to save your information as a draft.



testaudit.cdsl.co.in says

Records Added Sucessfully!!!

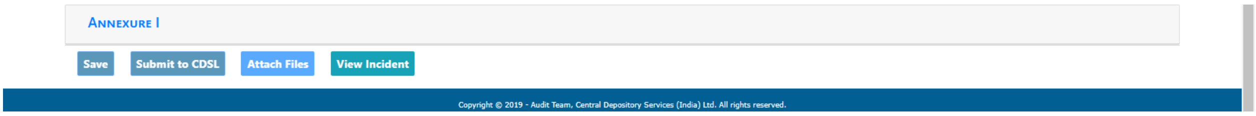
Records are added successfully



testaudit.cdsl.co.in says

Cyber Incident report submitted to CDSL !!!

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



Annexure I

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

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.**

***