REC POWER DISTRIBUTION
ISO 9001:2015, ISO 14001 : 2015 & OHSAS 18001 : 2007 Certified Company

आरईसी पावर डिस्ट्रीब्यूशन कम्पनी लिमिटेड
REC POWER DISTRIBUTION COMPANY LIMITED
(A wholly owned subsidiary of REC Limited, a 'Navratna CPSE' under Ministry of Power. Govt. of India)
CIN No. RECPDCL-U40101DL2007GOI165779
Corporate Office: D Block, REC World Headquarter, Plot No.I-4, Sector 29, Gurugram, Haryana - 122001.
Website: www.recpdcl.in, E-mail: co@recpdcl.in
Regd. Office: Core-4, SCOPE Complex, 7 Lodhi Road, New Delhi-110003, Phone 011-43091500 Fax: 011-24360644

स्वच्छ भारत
एक कदम स्वच्छता की ओर

RECPDCL/IT/2021/3207 Date: - 08.02.2021

To,
As per list attached (**Annexure- III**)

Sub: - **Inviting quotation to engage CERT-IN empanelled security auditing agency to conduct security audit of RECPDCL website (www.recpdcl.in).**

Dear Sir,

REC Power Distribution Company Limited (REC PDCL) an ISO 9001:2015, ISO 14001:2015 & OHSAS 18001:2007 Certified Company, a wholly owned subsidiary of REC Ltd., a 'Navratna' CPSE under Ministry of Power, intends to conduct a security audit of its website i.e. www.recpdcl.in through a CERT-IN empanelled security auditing agency of DeitY, Ministry of Communication & IT, Govt. of India. The objective of this audit is to assess security vulnerabilities as per the latest standards and reduce the risk.

The detailed objective &deliverables of the Security audit is enclosed as Annexure – I and the scope of work enclosed as Annexure - II. As your company is CERT-In emplaned agency as per the information available in CERT-In website (https://www.cert-in.org.in/PDF/Empanel_org_2020.pdf) you are requested to send your quotation as per the following format.

S. No.	Description	Amount (in Rs.)	Taxes (if any)	Total Price (in Rs.) (inclusive of taxes)
1	Lump sum amount to Complete all levels of Security Audit of RECPDCL website with Report Generation, recommendations and issue a Security Clearance Certificate. (As per scope of work & deliverables at Annexure I & II)			
GRAND TOTAL				

Terms & Conditions:

1. The price bids of those firms will be opened who fulfils the terms and conditions.
2. Only those Organizations/firms registered with the CERT-in-empanelled for information security audit are eligible for submitting the quotation.
3. Incomplete or conditional quotation will not be entertained.
4. No quotation will be accepted after closing date and time.
5. The agency will be removed from empanelment if due to any reason CERT-In has removed or not extended the empanelment of the agency.
6. The selected agency will not outsource any activity to other agency.
7. The selected agency will maintain confidentiality of the findings of security audit and ensure that the findings and corrective actions are shared with concerned stake holders of the project
8. **Schedule**: The first round of website audit report should be submitted to RECPDCL within 10 days after the work order issued by RECPDCL and consecutive round report if any, should be submitted within 5 days.

9. The bidder may remain present himself /herself or his/her authorized representative at the time of opening the quotation.
10. Any firm/organization blacklisted by a Govt./Semi Govt. Deptt. shall not be considered for this bid and bid will be rejected straightway.
11. A copy of terms & conditions attached as and Scope of work attached as duly signed by the tenderer, as a token of acceptance of the same should be attached along-with the tender.
12. The Tender Committee reserves the right to relax any terms and condition in the Govt. interest, with the approval of competent authority.
13. All disputes are subject to the jurisdiction of the Courts in the N.C.T. of Delhi.
14. Prices should be indicated in Indian Rupees only and in the respective units indicated at each row.
15. Calculations against each row as specified in the price schedule should be carried out carefully both for the total of each row and the Grand Total. Furnishing of any miscalculation etc. shall be at the bidder's risk and cost and the bid may be liable for summary rejection.
16. **Payment Terms:** 100% payment will be made only after submitting the final security audit certificate on completion of Audit of RECPDCL website.
17. Under no circumstances any extra/ additional taxes, duties, levies etc. shall be payable to the bidder by RECPDCL unless such a tax, duty or levy has been newly introduced and notified by the Government of India.
18. The bidder shall be the single point of contact for RECPDCL till the completion of audit process.
19. **Penalty Clause:**
    a. Failure to complete the audit along with deliverables on or before the stipulated date will entail a penalty equal to 1% of the value of the contract price per week / part their of subject to maximum of 10 % of total contract value.
    b. In case of delay in compliance with the order beyond 15 days of the stipulated time period, RECPDCL have right to cancel the order.

NOTE: DOCUMENTS REQUIRED TO BE ATTACHED WITH BID

1. Copy of GSTIN Registration and PAN.
2. Copy of authorization with CERT-in empanelment.
3. Copy of terms and conditions duly signed with seal of the firm/organization, in token of acceptance of terms and conditions.
4. Bidder should submit undertaking letter to this effect for single point of contact.

You are requested to quote your best rates as offered to the Government organisations in a sealed cover indicating "COMMERCIAL BID FOR CONDUCTING THE SECUIRTY AUDIT OF RECPDCL WEBSITE" addressed to the undersigned to reach on or before 15.02.2021, 11:00 AM(Address: D- Block, REC World Headquarter, Plot No. I-4, Sector-29, Gurugram (Haryana)-122001) and submitted sealed quotation will be opened on 15.02.2021 at 12:00 PM (on same day).

Yours Faithfully,

(Alok Singh)
General Manager (Tech.)

Objectives:

1. To conduct security audit to assess vulnerabilities to the RECPDCL Website i.e. www.recpdcl.in as per the ISO standards and OWASP top 10 vulnerabilities (Web & Mobile). The audit shall be conducted to review the intent and vulnerabilities to the organisations website.
2. Security Audit is intended to give developers and security teams the resources they need to build and maintain secure website. Through the project, our goal is to classify security risks and provide developmental controls to reduce their impact or likelihood of exploitation.
3. To identify the vulnerabilities present in the RECPDCL website.
4. To identify the corrective measures and rectification of the vulnerabilities in RECPDCL website.

Deliverables:

- The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.
- The agency should provide support to the development team for changes in coding to remove the vulnerabilities.
- Vulnerability Assessment Report, Penetration Test Report.
- Compliance review should be done after ensuring that changes to remove the vulnerabilities are completed by the development team.
- Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application or website has no vulnerabilities as a result of changes done in the code
- 1 day training session on the security for – No. of participants to also cover facilitation for closure of audit findings.

The proposed scope of work

A. Audit of the RECPDCL website:

1. The audit has to be done on the following parameters -
   - To Assess Flaws in the Design of the website.
   - Attempting to guess passwords using password-cracking tools.
   - Validations of various data inputs.
   - Exception handling and logging.
   - Logical access control and authorization.
   - Evaluate the environment under which the website /application runs.
   - An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.
   - Malicious modification of data.
   - Website/ Application Security Audit
   - Penetration Testing
   - Vulnerability Testing
   - Compliance Review
2. Checking if commonly known holes in the website exist.
3 RECPDCL website should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) (refer table 6.1).
4 The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website "Certified for Security".
5 Auditor must test website for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/application.
   - ✓ Vulnerabilities to SQL Injections
   - ✓ CRLF injections
   - ✓ Directory Traversal
   - ✓ Authentication hacking/attacks
   - ✓ Password strength on authentication pages
   - ✓ Scan Java Script for security vulnerabilities
   - ✓ File inclusion attacks
   - ✓ Exploitable hacking vulnerable
   - ✓ Web server information security
   - ✓ Cross site scripting
   - ✓ PHP remote scripts vulnerability
   - ✓ HTTP Injection
   - ✓ Phishing a website
   - ✓ Buffer Overflows, Invalid inputs, insecure storage etc.
   - ✓ Any other attack that can be a vulnerability to the website or web applications.

6 *The Top 10 Web application security vulnerabilities, which are given below, should also be checked, but not restricted to the following. The best practices in the industry must be followed.*

6.1- Top Ten Most Critical Web Application Security Vulnerabilities		
A1	**Injection**	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	**Broken Authentication**	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3	**Sensitive Data Exposure**	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4	**XML External Entities (XXE)**	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6	**Security Misconfiguration**	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7	**Cross-Site Scripting (XSS)**	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8	**Insecure Deserialization**	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9	**Using Components with Known Vulnerabilities**	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10	**Insufficient Logging & Monitoring**	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

7 *Auditor to test vulnerabilities in Website as per Industry practices/OWASP.*

B. <u>Audit Report</u>

The website security audit report is a key audit output and must contain the following:

1. Identification of Auditee (Address & contact information)
2. Dates and Location(s) of audit
3. Terms of reference (as agreed between the Auditee and Auditor), including the standard for Audit, if any.
4. Audit plan.
5. Additional mandatory or voluntary standards or regulations applicable to the Auditee.
6. Audit Standards should be followed.
7. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
   i) Tools used
   ii) List of vulnerabilities identified
   iii) Description of vulnerability
   iv) Risk rating or severity of vulnerability
   v) Test cases used for assessing the vulnerabilities
   vi) Illustration if the test cases to provide the vulnerability
   vii) Applicable screen dumps
8. Analysis of vulnerabilities and issues of concern.
9. Recommendations for action.
10. Personnel involved in the audit.

The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

EMPANELLED INFORMATION SECURITY AUDITING ORGANISATIONS by CERT-In

The List of IT Security Auditing Orgnisations, as given below, is up-to-date valid list of CERT-In Empanelled Information Security Auditing Orgnisations. This list is updated by us as soon as there is any change in it.

1. M/s AAA Technologies Pvt Ltd

278-280, F-Wing, Solaris-1,
Saki Vihar Road, Opp. L&T Gate No. 6,
Powai, Andheri (East),
Mumbai – 400072.
Website URL : http://www.aaatechnologies.co.in
Ph : 022-28573815 / 16
Fax: 022-40152501
Contact Person : Mr. Anjay Agarwal, Chairman & Managing Director
Mobile : +91 09322265876, 9821087283
E-mail : anjay[at]aaatechnologies.co.in

2. M/s AKS Information Technology Services Pvt Ltd

B-21, Sector-59, Noida - 201309 (Uttar Pradesh)
Website URL: https://www.aksitservices.co.in/
Ph: 0120-4545911
TeleFax : 0120-4243669
Contact Person : Mr. Ashish Kumar Saxena, Managing Director
Mobile : +91-7290058951
E-mail : info.cert[at]aksitservices.co.in

3. M/s AQM Technologies Pvt Ltd.

A 401, Raheja Plaza, LBS Road, Nityanand Nagar, Ghatkopar West,
Mumbai, Maharashtra 400086.
INDIA
Phone number :022 4050 8200
Fax: -
Contact Person: Mr. Sanjay PARIKH
E-mail:sanjay.parikh[at]aqmtechnologies.com
Contact No : +91-8291858027 / 022-40508262

4. M/s Allied Boston Consultants India Pvt. Ltd.

2205, Express Trade Towers-2, B-36, Sector 132,
Noida Expressway, Noida 201301 (U.P.)
Ph : 9891555625, 0120-4113529
Fax: 0120-4113528
Contact Person : Mr. T. Ganguly
E-mail : itsec[at]alliedboston.com

5. M/s A3S Tech & Company

A/95, Kamla Nagar, Delhi-110007
Ph : 9810899624
Fax: 23933429
Contact Person : Sagar Gupta
E-mail :sagar[at]a3stech.co.in

6. M/s Andhra Pradesh Technology Services Ltd

(Govt. of AP Undertaking)

3rd Floor, R&B Building, MG Road, Labbipet,
Vijayawada, Andhra Pradesh 520010
URL: https://www.apts.gov.in/
Land line Phone: 08662468105;
Mobile phone : 9440469194
Fax : N/A
Contact Person : Dr. G Jacob Victor, Executive Director
E-mail : mgr-apcsp-apts[at]ap[dot]gov[dot]in
Alternate Email ID : VictorJacob[dot]G[at]gov[dot]in

7. M/s BHARAT ELECTRONICS LIMITED

Office of the GM/Software,
BEL Software SBU
Bharat Electronics Limited
Jalahalli, Bengaluru - 560013
Karnataka
Ph :080-22197197, or 080-28383120
Fax:080-28380100
Contact Person : Mrs. Anna Peter, Sr.DGM (Software), BEL/SW
E-mail : ITSecurityAuditTeam[at]bel.co.in
Mobile : +91 9844296344
Ph :080-22195563

8. M/s Bharti Airtel Service Limited

Plot# 16, Udyog Vihar-Phase-IV
Sector 18, Gurgaon-122016
Ph : +91-9987891999
Fax:
Contact Person : Amit Chaudhary
E-mail : amit.chaudhary[at]airtel[dot]com

9. M/s Centre for Development of Advanced Computing (C - DAC)

Plot No. 6 & 7, Hardware Park,
Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510
Ph : +919441233972, +917382303598
Fax: NA
Contact Person : Ch A S Murty
E-mail : cswan[at]cdac.in, chasmurty[at]cdac.in

10. M/s Crossbow Labs LLP

Unit 406, Brigade IRV Center, Nallurhalli,
Whitefield, Bangalore
Karnataka 560066,
India
Ph : +91 80 470 91427
Fax:No Fax
Contact Person : Mr. Rosan Thomas
E-mail :cert[at]crossbowlabs.com

11. M/s CyberQ Consulting Pvt Ltd.

J-1917, Chittaranjan Park, New Delhi - 110019
Ph :9899139870/7042081393
Fax:NA
Contact Person : Mr. Debopriyo Kar
E-mail :debopriyo.kar[at]cyberqindia.com

12. M/s CyRAAC Services Private Limited

2nd Floor, Napa Prime, 7/24, 11th Main Road,
4th Block East, Jayanagar,
Bengaluru - 560011
Ph : +919886210050
Fax:
Contact Person : Mr. Murari Shanker
E-mail : ms[at]cyraacs.com

13. M/s Codec Networks Pvt Ltd

B-136, Surajmal Vihar, Delhi 110092
Ph : +91 9971676124, +91 9911738718
Fax: N.A
Contact Person : Mr. Piyush Mittal
E-mail : amittal[at]codecnetworks[dot]com; piyush[at]codecnetworks[dot]com

14. M/s Deloitte Touche Tohmatsu India LLP

7th Floor, Building 10, Tower B, DLF Cyber City Complex,
DLF City Phase II, Gurgaon, Haryana, India
Ph : +91 9811663776
Fax: 0124-6792012
Contact Person : Mr. Gautam Kapoor
E-mail : gkapoor[at]deloitte.com

15. M/s eSec Forte Technologies Pvt. Ltd.

Postal address:311, Jwala Mill Road, Udyog Vihar - Phase 4,
Gurugram, Haryana, 122015, India
Ph : +91 9871699555
Fax: +91 0124 4264666
Contact Person : Kunal Bajaj
E-mail : kunal[at]esecforte.com

16. M/s ITORIZIN TECHNOLOGY SOLUTIONS PVT LTD

8/14, SHAHID NAGAR, GROUND FLOOR. WING “A”.
KOLKATA – 700078. West Bengal, India
Ph : 9883019472
Fax: NIL
Contact Person : Sangeeta Ganguly
E-mail : g.sangeeta[at]itorizin[dot]in / connect[at]itorizin[dot]in

17. M/s Grant Thornton India LLP

L 41, Connaught Circus, Outer Circle,
New Delhi. PIN - 110 001
Ph : 0124-4628000 (Ext. 277)
Fax: +91 124 462 8001
Contact Person : Mr. Akshay Garkel, Partner Cyber
Mobile: +91 9820208515
E-mail : Akshay.Garkel[at]IN.GT.COM and cyber[at]IN.GT.COM

18. M/s KPMG Assurance and Consulting Services LLP

DLF Building No. 10, 8th Floor, Tower C,
DLF Cyber City, Phase 2,
Gurgaon, Haryana-122002
Ph : +91 9810081050
Fax: +91 124 254 9101
Contact Person : Mr. Atul Gupta (Partner, Cyber Security)
E-mail : atulgupta[at]kpmg.com

19. M/s Mahindra Special Services Group

(Division of Mahindra Defence Systems Limited)

Mahindra Towers, P.K Kurne Chowk,
Dr. G.M Bhosale Marg, Worli,
Mumbai - 400018, India
Ph: 9769015546
Fax: NA
Contact Person: Mr. Rajesh Huddar
E-mail :rajesh.huddar[at]mahindrassg.com

20. M/s Maverick Quality Advisory Services Private Limited

123 RADHEY SHYAM PARK P.O SAHIBABAD
Ghaziabad, U.P, INDIA – 201005
Ph :9871991928
Contact Person : Mr. Ashok Vardhan,Director
E-mail :ashok[at]mqasglobal.com

21. Madhya Pradesh Agency for Promotion of Information Technology (MAP_IT)

(A Regt. Society of Department of Science & Technology, Government of Madhya Pradesh)

47-A , State IT Center, Arera Hills,
Bhopal, Madhya Pradesh- 462011
Ph: 0755-2518713, 0755-2518702
Fax: 0755-2579824
Contact person : Mr. Vinay Pandey
Mobile:+91-0755-2518710
Email: vinay[dot]pandey[at]mapit [dot] gov [dot] in

22. M/s Mirox Cyber Security & Technology Pvt Ltd

4th Floor Nila Technopark Kariyavttom PO 695581
Trivandrum, Kerala
Phone +91 471 4016888 / +91 471 4000545
Mobile 9995199499, 9995799499
Contact Person : Mr. Rajesh Babu
Mobile: 9995799499
Email- rb[at]miroxindia.com/rbmirox2000[at]gmail.com

23. M/s Net Square Solutions Private Limited

1, SanjivBaug baug, Near Parimal Crossing, Paldi,
Ahmedabad - 380007, Gujarat
Fax : +91 7926651051
Contact Person : Ms. Jinal Harsora
Email: jinal[at]net-square.com
Mobile: +91 75063 76777

24. M/s Network Intelligence India Pvt. Ltd.

2nd Floor, 204, Ecospace IT Park,
Off Old Nagardas Road, Andheri-E, Mumbai-400069.
Ph :+919820049549
Fax: NA
Contact Person : Mr. Kanwal Kumar Mookhey
E-mail :kkmookhey[at]niiconsulting.com

25. M/s Paladion Networks Pvt. Ltd.

Shilpa Vidya, 49 1st Main, 3rd Phase
JP Nagar, Bangalore - 560078
Ph : +91-80-42543444
Fax: +91-80-41208929
Contact Person : Mr. Balaji Venkatasubramanian
E-mail : balaji.v[at]paladion.net

26. M/s Payatu Technologies Pvt Ltd

502,5th Floor, Tej House,
5 MG Road, Camp, Pune-411001
Ph : +91-20-41207726
Fax: NA
Contact Person : Mr. Pranshu Jaiswal
E-mail : cert[at]payatu.com

27. M/s Price water house Coopers Pvt. Ltd.

7th & 8th Floor, Tower B, Building 8,
DLF Cyber City, Gurgaon, Haryana -122002
Ph : [91] 9811299662
Fax: [91] (124) 462 0620
Contact Person : Mr.Rahul Aggarwal
E-mail : rahul2.aggarwal[at]pwc.com

28. M/s Protiviti India Member Private Limited

GTB Nagar, Lalbaug, Everard Nagar,
Sion, Mumbai, Maharashtra 400022
Ph :022 6626 3333
Contact Person : Mr. Sandeep Gupta (Managing Director)
E-mail :Sandeep.Gupta[at]protivitiglobal.in
Phone: +91-9702730000

29. M/s PRIME INFOSERV LLP

60, SIBACHAL ROAD, BIRATI, KOLKATA 700051
Ph : 033- 40085677, Mobile no.- +91 9830017040
Fax:
Contact Person : Sushobhan Mukherjee
E-mail : smukherjee[at]primeinfoserv[dot]com, info[at]primeinfoerv[dot]com

30. M/s Qseap Infotech Pvt. Ltd.

Unit No.105, Building No.03, Sector No.03,
Millennium Business Park, Mahape(MIDC),
Maharashtra- 400710, India
Ph :9987655544
Fax:NA
Contact Person : Mr. Abhijit Doke
E-mail :abhijitd[at]qseap.com

31. M/s QRC Assurance and Solutions Private Limited

Office No 508, Plot No 8, Ellora Fiesta, Sector -11,
Sanpada, Navi Mumbai, Maharashtra, India, 400705
Ph : +91-9920256566
Fax: NA
Contact Person : Kalpesh Vyas
E-mail : kalpesh.vyas[at]qrcsolutionz[dot]com

32. M/s RSM Astute Consulting Pvt. Ltd.

301-307, A Wing, Technopolis Knowledge Park,
Mahakali Caves Road, Andheri (East),
Mumbai – 400093
Tel: 91-22- 6108 5555
Contact Person :Mr. Anup Nair
E-mail : anup.nair[at]rsmindia.in
Mobile No. +91 8828428080
Website : www.rsmindia.in

33. M/s RNR Consulting Private Limited

E-16/169, Sector-8, Rohini, Delhi 110085
Ph : +91 9999132873 , +91 9971214199
Fax: N/A
Contact Person : Nitish Goyal , Practice Head – Information and Cyber Security
E-mail : nitish[at]consultrnr[dot]com

34. M/s SecureLayer7 Technologies Private Limited

Plot No. 28, Vyankatesh Nagar, Beside Totala Hospital,
Jalna Road, Aurangabad, MH 431001
Ph : +91-844-844-0533
Fax: NA
Contact Person : Mr. Sandeep Kamble
E-mail : cert[at]securelayer7.net

35. M/s SecurEyes Techno Services Pvt. Ltd.

4th Floor, Delta Block, Sigma Soft Tech Park,
Whitefield Main Road, Varathur, Bangalore - 560066
Phone Number: +91 9449035102/ 080-41264078
Fax:NA
Contact Person : Ms. Uma Pendyala
E-mail :umap[at]secureyes.net

36. M/s Security Brigade InfoSec Pvt. Ltd.

3rd Floor, Kohinoor Estate, Lower Parel,
Mumbai - 400013
Ph : +919004041456
Fax: -
Contact Person : Mr. Jamila Pittalwala
E-mail : certin[at]securitybrigade.com

37. M/s Sysman Computers

312, Sundram, Rani Laxmi Chowk,
Sion Circle, Mumbai 400022
Ph : 99672-48000 / 99672-47000 / 022-2407-3814
website : www.sysman.in
Contact Person : Dr. Rakesh M Goyal, Director
E-mail : rakesh[at]sysman.in, सिसमैन@सिसमैन.भारत

38. STQC Directorate, Ministry of Electronics and IT, Govt. of India

Electronics Niketan, 6 C G O Complex, Lodhi Road, New Delhi-110003
Ph :011 24301816, 24301382
Fax:011 24363083
Contact Person : Mr. Gautam Prasad
E-mail : gprasad[at]stqc.gov.in; headits[at]stqc.gov.in

39. M/s Sattrix Information Security Pvt. Ltd.

28, Damubhai Colony, Nr. Anjali Cross Road, Bhatta,
Paldi, Ahmedabad-380007.
Ph : +91 9825077151
Fax:
Contact Person : Bhavik Patel
E-mail : bhavik.patel[at]sattrix[dot]com

40. M/s TAC InfoSec Private Limited

C203, 4th Floor, World Tech Tower
Phase-8B, Mohali-160055
Ph : 9876200821, 9988850821
Contact Person : Mr. Trishneet Arora, Founder and CEO
E-mail :ceo[at]tacsecurity.co.in

41. M/s Tata Communications Ltd

Tower 4, 4th to 8th Floor, Equinox Business Park,
LBS Marg, Kurla (W), Mumbai 400070
Ph : +91 22 66592000
Contact Person : Mr.Ratnajit Bhattacharjee - DGM-GRC Product/Services
Mr.Mohit Shukla - DGM Cyber Security Products
E-mail : Ratnajit.Bhattacharjee[at]tatacommunications.com,
mohit.shukla@tatacommunications.com
Mobile : 9810093811, 9873334607

42. M/s Talakunchi Networks Pvt Ltd

Postal address: 505, Topiwala Centre,
Off S.V. Road, Goregaon West, Mumbai 400104
Phone: +91-9920099782
Contact Person : Vishal Shah
E-mail: certin[at]talakunchi.com

43. M/s Tata Advanced Systems Ltd.

Cyber & Physical Security Division
Postal address: Office No. 15, 6th floor, Tower 1,
Stellar IT Park, C-25, Sector-62 Noida, Uttar Pradesh, India. PIN - 201307
Fax: 0120 4847459
Contact Person : Argha Bose - (Head , Cyber Security Practice)
Email: argha.bose[at]tataadvancedsystems[dot]com
Mobile no.: 7028007432

44. M/s Xiarch Solutions Private Limited

352, 2nd Floor, Tarun Enclave,
Pitampura, New Delhi-110034, India
Ph :011-45510033
Fax:011-66173033
Contact Person : Mr. Utsav Mittal, Principal Consultant
E-mail : utsav[at]xiarch.com, cert[at]xiarch.com

45. M/s Yoganandh & Ram LLP

G-1, Shree Vishnu Apartments, 12, Twelfth Cross Street,
Dhandeeswaram Nagar, Velachery, Chennai - 600042
Ph : 044-22432030
Fax: Nil
Contact Person : Mr. Manoj Kumar Jain
E-mail : manoj[at]yandr.in / isaudit[at]yandr.in
Mobile : 9940156515 / 98415 82933