AEREN IT SOLUTIONS PVT LTD

SECURITY ASSESSMENT SHEET

(A) General Security Governance

Question(s)	**Answer (please be concise)**
1) In your company, is there an established security program? If yes: • Is the security program based on any standard or best practice (please name specific standards/best practices that apply, e.g. ISO 27001/ISO 27002, SAS 70 Type II, systrust, PCI DSS, PA DSS, SOX, etc.)? • Is a member of staff or group formally chartered with responsibility for information security? • Who do they report to (if possible, please provide the appropriate organizational charts)? • Is your security program regularly audited by an independent third party? If yes: ○ How often are these audits performed? ○ Is it possible for Client to obtain a management summary of recent reports?	Yes, ISO 27001 Yes Yes Third party audit is done quarterly. Yes
2) Do you regularly have an independent third party perform penetration tests on all systems relevant to the project you are bidding for (including all systems that are or may be used to access or process data relevant to that project)? If yes: • How often are these penetration tests performed? • Is it possible for Client to obtain management summaries of recent reports as well as management summaries of mitigation plans that counter identified issues? (please note	Yes, Third party penetration is done. Yes, Third party penetration is done quarterly. Yes, We can provide reports of Manage Engine Firewall Analyzer 7 and UTM box Juniper SSG 5.

that all information provided to Client under NDA will be treated as strictly confidential by Client; the review of penetration testing management summaries is an important part of the vendor assessment and failing to provide those can result in a delay of the project as we need to perform a more thorough non-intrusive vendor assessment ourselves)	
3) Do you regularly perform internal audits with a focus on information security? If yes: • Who conducts these audits and how are their results used? • How often are these audits done?	Yes, We have internal auditor. Internal Audits are performed every month.
4) Are security policies in place? If yes: • Please provide a list of topics covered by your security policies. • How often are security policies reviewed, audited and updated? • What is the process for handling policy violations?	Yes, Policy related to security of Physical IT Assets/ Software Assets in the organization, network Security related to Company's password etc. Security Policy's are reviewed quarterly. Violations are recorded and should be resolved in 15 days of period.
5) Do you perform regular risk assessments with regard to information security? If yes: • What methodology do you use? • How often are risk assessments reviewed/updated? • Who defines an acceptable level of residual risk? • What is the process for dealing with risks identified during the risk assessment?	Yes, OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation. Risk assessments are done quarterly basis. Vulnerable risks are recorded and should be mandatory to resolve in 15 days of period.
6) Do you assess the security of your vendors and/or sub-contractors (those relevant to the project you are bidding for)?	Yes
7) Do you have (security) incident response procedures in place?	Yes,

If yes: • Please outline your incident response procedure. • What groups within the company are involved with incident response? • Do you notify customers of impacting security incidents?	 • Incident Iidentification, Cclassification and Eescalation. • IT Team, IT Security Team, Internal audit manager. • Yes
8) Did you have any security incidents in the past 5 years? If yes: • Has end user or sensitive corporate data been compromised (or could that have happened)? • Did any production servers or workstations get compromised (e.g. someone unauthorized was able to read/write files or execute code of their choosing)? • Have there been any application-level security vulnerabilities/compromises (e.g. circumvention of authorization controls; common web attacks, SQL injection, XSS, etc)? • Have you been impacted by malware infections? • Did you notify impacted customers?	NO NO NO NO NO Yes

(B) Personnel Security

Question(s)	**Answer (please be concise)**
1) Is your staff regularly trained on current security and awareness best practices? If yes: • Are there audience specific trainings? If yes, for what groups? • How often are these trainings done? • Do temps/interns/contractors undergo security trainings as well?	Yes, Everyone when join the company is given IT induction training for its equipment usage and security policies. Once a year the policy is reviewed and trainings if required are given to the staff.
2) Do you perform background checks on employees?	Every employee/IT user before joining goes thru a third party background check. We don't repeat background checks for existing staff.
3) Please explain your termination process,	Every employee/contractor has to sign a

both for the case when an employee leaves as well as when an employee is terminated.	legal Service agreement before doing any work and once they leave the company they are legally bonded with the non-data sharing clause for 5 years.

(C) Physical and Environmental

(C.1) Physical Security at Data Center

Question(s)	**Answer (please be concise)**
1) Please describe the basic physical properties of the data center: • What physical security/access control measures have been implemented (e.g. cages, guard, CCTV, type of access control, etc)? • Is the facility used exclusively by you?	CCTV system has been installed Yes, It is CEO only having Access to the CCTV System. No one Network Based Password Protected DVR has been installed and is being monitored in CEO Room.
2) Has a risk analysis with regard to the physical risks been done?	Yes
3) Is physical access monitored? If yes: • How? (e.g. motion detectors, guards, alarms, CCTV, etc.) • Are there physical entry logs? • How long are physical entry logs retained? • How are physical security incidents identified and how are they escalated? • Under what conditions are clients notified of physical security breaches?	Yes CCTV System Installed Time Attendance system installed which records the every IN/OUT Entry Every Person entered is being captured in the DVR Recording System Physical Security not at all breaches
4) Do you have procedures in place regarding granting and removing physical access rights? If yes, please explain your procedures.	Yes, a policy document is in placed Only CEO of the company authorizes the physical access, IT manager grants the physical access and log book is marinated for every change.
5) Do you have measures in place to protect against power outages?	Yes

If yes: • How long can the systems relevant to the project you are bidding for survive on UPS? • Are there backup generators? If yes: ○ How often are they tested? ○ How much backup fuel is available, and how long can power be provided on this supply? ○ Are there priority fuel supply contracts in place?	 UPS for Half an Hour Yes Once in week The whole week Yes
6) Is there monitoring for power supply, HVAC, temperature and other environmental controls in place at your facilities?	Yes
7) Do you protect against environmental threats such as fire, water, cable damage, etc?	Yes

(D) Network

Question(s)	**Answer (please be concise)**
1) Do you have configuration guidelines for network equipment? If yes: • For what equipment do configuration guidelines exist? • Please outline the security requirements in the configuration guidelines.	Yes Internet Broadband, Wi-Fi Access Point, Firewall, Domain Controller Server. Any device configuration change will be done after the approval of Program Manager.
2) Do you use firewalls to filter all inbound and outbound traffic? If yes: • Are all external servers in a DMZ, separate from internal servers and clients? • Do you use firewalls between internal	Yes, We have UTM Box, Juniper SSG 5 Yes.

servers and clients?	Yes.
3) Do you have measures against network level attacks implemented? If yes: • What measures do you have against sniffing? • What measures do you have against ARP spoofing?	Yes Deep Inspection enabled on firewall. Juniper firewall SSG 5 has been configured for ARP spoofing.
4) Network device management: • Is there a separate management network for managing network devices? ○ If yes, who has access to the management network? • Please explain how remote administration access works (e.g. from corporate or NOC to data center). • Please name all protocols used to manage network devices that do not encrypt traffic (e.g. SNMP (v1, v2c, ...), telnet, etc.) • Do you use centralized management software (such as HP OpenView or similar)? If yes, please specify. • How do you authenticate to network devices (passwords, token, keys, etc.)? • Do you use centrally maintained authentication, authorization and accounting services (Radius, TACACS, or Kerberos?)	We are not using Remote management and VPN connectivity. But we have Juniper firewall by using that we can use VPN service if required. NA NA NO NO, We don't use VPN and Remote Access
5) Do you monitor your network? If yes: • What operational monitoring do you have (uptime)? • Do you monitor firewall logs? If yes, what is monitored?	Yes We have Advent Firewall Analyser, Alerts has been configured on the same. Advent Firewall analyzer logs can be maintained more than one year.
7) Administrative access to network devices:	Yes It is under my control is well documented with me.
8) Do you provide remote access for regular	No, We don't use remote access.

employees?	
9) Do you have a change management process for changes to network devices? If yes: • What are the general procedures? • What are the specific procedures for changing security configurations (e.g. changes to firewall rules)?	Yes We have Our Technical expert and every change management is approved by me before implemented. It also documented.
10) Is management of your devices outsourced?	We have our own IT Security and Network expert.

(E) System

(E.1) Servers

Question(s)	**Answer (please be concise)**
1) General software environment: • What operating systems do you use on the servers relevant to the project you are bidding for? • What middleware do you use on the systems relevant to the project you are bidding for? • What other applications do you use on the systems relevant to the project you are bidding for?	Windows 2008 R2 Server and client machines as Window XP with Service pack 3. Microsoft Office
2) Do you have a process for installing updates and security patches for operating systems and applications? If yes: • What is the process for deploying/installing OS patches? • What is the process for identifying and deploying/installing applicable application patches (e.g. for applications that are not covered by WindowsUpdate, or your package manager)? • Do you have vulnerability management procedures?	Yes, WSUS (Windows Software Updates Server) First we apply patch on 1 Machine, if there is no issue on that machine, Update is applied on all machines of our network.

3) Do you scan your hosts for for host level vulnerabilities? If yes: • How often? • What product do you use?	Yes, Once in month GFI Languard
4) Is anti-virus deployed on your servers? If yes: • How often are rules updated? • How is it monitored?	Yes, Daily Updates IT is Centrally monitored from server.
5) Do your systems log to a centralized log infrastructure? If yes: • Are logs monitored? • By whom? • How long are logs retained?	Yes, Yes, Network Admin Quarterly.
6) Administrative access to servers: • What operational groups and how many persons in which group have admin/root/privileged access to servers? • How is administrative access monitored and audited? • Do all administrators have a personalized account? If yes: ○ How are root/administrator passwords retained? ○ Who has access to these passwords?	 Only Single Administrator is allowed to access as admin group member. Internal Auditor checks the server logs and monitor and verify the configuration changes which was done on the server.
7) Do you have change and configuration management procedures for systems and applications? If yes: • Please outline.	We have already explained above
8) Backup: • How often are backups done? • Where are backups stored? Who has access? • How are backups encrypted? • How are end-of-life backup mediums destroyed? • How often do you test your backups?	Yes Daily Specific to machine Backup test is done once in a month.

• How frequently are off-site backups revalidated by doing a test restore?	Same once in a month.
9) Do you provide multiple services from a single physical machine?	Yes.

(E.2) Clients (Workstations/Laptops/...)

Question(s)	**Answer (please be concise)**
1) Do you have operating system hardening or build standards for your clients? If yes: • If you use a specific standard, please specify. • If you have your own hardening and build standards, please outline the security requirements.	AS Above explained
2) Do you have a process for installing updates and security patches for operating systems and applications? If yes: • What is the process for deploying/installing OS patches? • What is the process for identifying and deploying/installing applicable application patches (e.g. for applications that are not covered by WindowsUpdate, or your package manager)? • Do you have vulnerability management procedures?	As above explained
3) Do you scan your clients for for host level vulnerabilities? If yes: • How often? • What product do you use?	Yes, Already explained above
4) Is anti-virus deployed on your clients? If yes: • How often are rules updated? • How is it monitored?	Yes, Already explained above
5) Do your clients log to a centralized log infrastructure?	Yes, Domain server, Network Admin maintained the logs and logs are maintained for a year.

6) Administrative access to clients: • Who has administrative access to clients? • What access level do regular users have on their workstations? • What are the procedures when a user requires non-standard software to be installed?	 Only IT Manager Specific applications Only with approval of IT manger and Network admin, the software can installed

(F) Business Continuity/Disaster Recovery

Question(s)	**Answer (please be concise)**
1) Do you have a plan for dealing with disasters? If yes: • What scenarios are covered? • How are disasters defined/classified? • How often do you test your DRP?	Yes Backup has been taken and kept in my custody Incase hdd crashed of the particular system Once in a month.
2) Do you have backup sites for every critical function? If yes: • What are the maximum outage times if a facility is destroyed? • Do you maintain logically and physically redundant DNS for all domain names referenced by your product, and all DNS dependencies your product may contain?	Yes 1 Day. No.
3) Do you have the ability to mitigate internet sourced denial of service attacks? If yes: • What preventive, detective and corrective controls do you have in place? • Can you provide a usable product during sustained 100% bursts in legitimate utilization or sustained distributed denial of service attacks?	Yes We have deep inspection installed for packet scanning. DOS attacks are managed by Juniper firewall.