LAWDESK BUSINESS PARTNER DATA SECURITY REVIEW

BUSINESS NAME: _____ BUSINESS CONTACT: _____
ADDRESS: _____ PHONE NO.: _____
_____ DATE SUBMITTED: _____

Physical & Logical Security (*PLEASE RESPOND TO QUESTIONS IN DETAIL*)

Physical Access

1. Please describe in detail the security measures in place to protect servers, routers, and other network devices. _____
2. Are locks and alarms armed during off-hours? _____
3. Are all unauthorized intrusions or attempted intrusions reported to the Information Security Officer? _____
4. Who within the organization has access to the computer room? _____
5. Are PCs and workstations secured with password-protected screensavers? _____

Logical Access and Controls

1. How are user ID and passwords utilized and monitored? _____
2. Describe in detail, how unauthorized access attempts are reported to management? _____
3. Is an Intrusion Detection System in place? Is it monitored real-time? Describe in detail your monitoring process. _____
4. Is network protected from unauthorized access using firewalls? ☐Yes ☐ No, If Yes, Model _ _ Manufacturer _____
5. Describe your network firewall protection systems. _____ _____
6. If applicable, do you intend to firewall your network from Company's Network? ☐Yes ☐ No
7. If applicable, will you store any Company's sensitive data? ☐Yes ☐ No
    - If yes, for what purpose is it stored. _____
    - How long will it be stored? _____ Is it encrypted while stored? ☐Yes ☐ No
8. Is a wireless network implemented in your facility? ☐Yes ☐ No

9. How is your network monitored for unauthorized access attempts, excessive or unusual network activity? _____

10. Are you using anti-virus software? ☐ Yes ☐ No; If so, Manufacturer _____ Product Name _____ Version _____

11. Provide examples of network activity documentation. _____

12. What was the date of the last network penetration test that was performed at your facility?

_____

13. Describe in detail the controls in place to ensure complete and accurate data transmissions.

_____

14. Do you encrypt sensitive data? Destribe _____

- Do you utilize a secure virtual private network ("VPN") to set up your remote connections? ☐ Yes ☐ No; If so, Manufacturer _____ Product Name _____ Version _____

Fire Suppression

1. Please describe in detail the fire detection and suppression systems in place.

_____

2. Are adequate fire instructions posted? _____

3. Is there a fire alarm device present? _____

4. Are computer operators familiar with emergency power-off procedures? _____

5. Where wet pipe sprinkler systems are in use, are adequate systems in place to protect against water damage? _____

Policies and Procedures

1. Are adequate Policies & Procedures in place and enforced? _____

- Do you have Policies & Procedures for the following:
  - Systems Development & Change Control? ☐ Yes ☐ No
  - Network Security and Access Controls? ☐ Yes ☐ No
  - Computer Operations and Processing Procedures? ☐ Yes ☐ No
  - Telecommunications Operations? ☐ Yes ☐ No
  - Security Incident & Handling Procedures ☐ Yes ☐ No

2. How often are Policies & Procedures reviewed? _____

Tape Back-up and Data Storage Security

1. Describe in detail the critical file backup process and frequency. _____
2. Are backup tapes stored at an off-site secure location? _
3. Is data encrypted before being transported off-site? _____
4. Are periodic inventories of archival tapes and disks taken? _____
5. Is access to stored backups limited to authorized personnel? _____ Are logs kept? _

Disposal of Confidential Information

1. In detail, describe the process for the disposal of confidential information including paper documents, CDs, floppy disks, etc. _____
2. Describe the procedures in place for the disposal of hardware and data removal from disk.

   _____

Contingency Planning

1. Do you have a Disaster Recovery Plan? _____
   - Please provide a high-level summary of the plan.
2. Is adequacy and effectiveness of the IT disaster recovery/contingency plan reviewed, tested, and maintained on a regular basis? _____
3. Is a copy of the IT contingency plan stored off-site? _____
4. Are all-critical resources covered by the plan, including all data and telecom components?

   _____
5. Has the plan been approved by Senior Management? _____
6. Do you have adequate backup power in the event of an outage? _____
   - Are UPS units in place on critical hardware? How much time do the batteries provide? _____
   - Do you utilize a backup generator? How long before the generators are at full capacity? _____

Audits/Examinations

1. Please provide a summary of the IT audits performed during the last 2 years.

   _____

2. Has management taken appropriate and timely action to address the deficiencies noted in the audit report? _____

3. Do you have a formal vendor management process in place for your mission critical vendors?
   ☐ Yes ☐ No

4. Are you Payment Card Industry Security Standards (PCI) compliant? ☐ Yes ☐ No
   If yes,☐ Self-Certified ☐ Auditor Certified
   If no, do you have plans to become PCI compliant? ☐ Yes ☐ No
   Expected Date to be completed:_____

Personnel

1. Please describe procedures for potential new employees.

   - Background checks _____
   - Fingerprints _____

2. Please provide a copy of the Confidentiality or non-disclosure agreement employees' sign as part of their initial terms and conditions of employment. _____

3. Is there a continuing security education program for IT staff? _____

4. Please describe in detail Incident Management procedures to handle security incidents.

   _____

GENERAL

Insurance

1. Please provide a corporate insurance coverage certificate.

Foreign Based

1. Do you have a foreign-based facility that is providing service to Company? _____ If so, what is the location? _____

ADDITIONAL COMMENTS