Vendor Assessment Questionnaire

INSTRUCTIONS:

The following questionnaire is a standard part of our Vendor Assessment Process. To be considered for services, please fill this out to the best of your ability. If you have a website or knowledgebase that contains this information, you may provide those links or documents.

VENDOR GENERAL INFORMATION

Vendor Company Name: ______________________________

Primary Business Address: ______________________________

____

City: ______________________________ State: _______ Zip: ___________

Years In Business: ________

Primary Industry Classification: ______________________________

(e.g., ISP/Network, ASP/Hosting, Application Development, Managed Security, Consultancy)

Primary Services Provided: ______________________________

Primary Business Contact Name: ______________________________

Title: ______________________________

Phone/Email: ______________________________

Primary Security Contact Name: ______________________________

Title: ______________________________

Phone/Email: ______________________________

Regulatory Compliance Activities and/or Certifications ______________________________

____

GENERAL QUESTIONS

Identify which are employed by your company (check all that apply):

□ FIPS Validated Cryptography in use. If yes, in what capacity: ________________________

□ FIPS Compliant Cryptography in use. If yes, in what capacity: ________________________

□ Written screening process for new team members to include background checks

□ US Citizens Only. If not, please note:

□ 3rd Party Audit Process of Security

□ Internal Audit Process for Security

□ Penetration testing. For product? ___________ For company? _____________

□ Change Management Processes

□ IPS/IDS/EDR/MDR/SIEM/SOAR deployed. Please detail: ___________________________________

□ Hosting Platform and Location of Data: ____

INFORMATION SECURITY MANAGEMENT CAPABILITIES

1. Identify the size (in FTEs) and skills composition, current security-centric certifications , etc. of the vendor's dedicated information security team – and indicate to what extent (if any) that employees will be assigned specifically to the security oversight of client's data/activities entrusted with vendor:

____

____

2. If vendor in turn relies upon downstream vendors to provided security-centric support (e.g., MSSP) services, please identify these vendors and the functions they will be providing as part of the service agreement with the client:

____

____

PROTECTION/SEGREGATION OF CLIENT-SUPPLIED DATA STRATEGY

1. When sensitive client data of any of the types (PII, PCI, PHI, Competitive Data, Client Data) are entrusted into vendor's care, identify the means by which such data is segregated from that of other clients while in system storage (e.g., physical segregation, logical segregation via VLANs/firewalls, separate DB instances, etc.). Include how access control rights are governed with respect to employee access to client data, including management-driven account provisioning/termination and role-based assignments:

____

____

2. Identify each of the means that exist within vendor's environment by which client-supplied data is encrypted while in-transit and/or at-rest (including, where possible, the names of the branded solutions being used and the size/strength of the encryption keys):

____

____

INCIDENT RESPONSE AND PRIVACY CAPABILITIES

1. Identify the nature and extent of the vendor's overall incident response plan, including the employee teams who are involved in the incident reporting, escalation, and remediation tasks, as well as ready access to skilled data forensics capabilities, associated with resolving suspected/confirmed information security incidents. Please include the frequency of tabletop exercises and indicate if the CSuite is involved:

____

____

2. Within the context of the vendor's overall incident response plan, specifically describe the timing and manner in which COMPANY will be apprised of reported incidents and subsequent resolution tasks:

____

____

3. Identify the extent to which vendor has developed/implemented breach notification procedures and/or templates that are approved and ready for use in the event that client's sensitive data is subjected to an unauthorized data breach event:

4. Within the context of the past two years, identify any significant information security or privacy breach incidents that negatively impacted any of vendor's clients – and briefly describe the efforts undertaken by vendor to address/resolve them and provide for meaningful changes to the vendor's information security /privacy practices designed to prevent recurrence.

VENDOR-MAINTAINED CYBER INSURANCE POLICY PROTECTIONS

1. Briefly summarize the extent to which vendor maintains current cyber liability insurance policy coverage to protect the vendor (and clients via indemnification) against substantial monetary losses arising from either first-party or third-party liability risks, and the amount of coverage:

REFERENCES

1. Please provide 2 current customer references: