NetDiligence®

Vendor Security Due Diligence Checklist

INTRODUCTION:

The following template outlines a BASIC, ENTRY-LEVEL vendor security checklist that can be modified and used by eRisk Hub clients as ONE element of an effective vendor security management program. The purpose of this checklist is to permit the client to obtain from a current/prospective vendor a solid understanding of the nature and strength of the vendor's security/privacy practices.

We encourage eRisk Hub clients who do not presently utilize such a checklist to add/modify its contents for their own unique settings – and then begin to require completion (by vendor representatives) as part of the initial vetting (and/or contract renewal) process that the client undertakes when entertaining the use of vendor-provided IT and related services.

VENDOR CONTACT 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 Business Contact Name: _____

Title: _____

Telephone: _____

Email: _____

Primary Security Contact Name: _____

Title: _____

Telephone: _____

Email: _____

TYPES OF SERVICES TO BE PROVIDED TO CLIENT

Identify which services are being offered/provided to the client by vendor (check all that apply):

- ☐ Internet Service Provider (ISP) or Other Data Network Services.
- ☐ Commercial Co-location/Cloud Hosting (Physical, Network, and/or System-Level Only).
- ☐ Commercial Co-location/Cloud Hosting (P, N, and S – plus Application/ASP-Level).
- ☐ Original Application Development.
- ☐ Payment Processing Services.
- ☐ Outsourced Retail Sales/Fulfillment/Service.
- ☐ Outsourced Commercial Business Operations Processing.
- ☐ Outsourced Healthcare-Related Provider, Back-Office, or Insurance Services.
- ☐ Managed Security Services Provider.
- ☐ Business/Marketing Consultancy Services.
- ☐ IT/Technical Consultancy Services.
- ☐ Independent Audit/Compliance Services.
- ☐ Other (include description):

_____

_____

_____

_____

From what locations are the services being provided on the client's behalf (check all that apply):

- ☐ At the client's on-site premises only?
- ☐ At the vendor's on-site premises only?
- ☐ At a third-party location not owned/operated by either the client/vendor?
- ☐ Does the vendor anticipate sub-contracting out some/all of the provided services?

  If so, identify (by company name and location) all sub-contracted vendors who will participate in any aspect of the provided services?

  _____

  _____

  _____

  _____

NATURE OF THE MISSION-CRITICALITY OF THE SERVICES BEING PROVIDED

Identify the underlying business criticality assumption(s) associated with the services being provided on the client's behalf (check all that apply):

- ☐ The service represents or supports a real-time, *human health or safety activity* that requires 24x7x365 availability on the client's behalf (and is covered under a formal SLA contract).
- ☐ The service represents or supports a real-time, *revenue generating activity* that requires 24x7x365 availability on the client's behalf (and is covered under a formal SLA contract).
- ☐ The service represents or supports a batch/periodic, *revenue generating activity* that requires general availability on the client's behalf, but which may include agreed-upon provisions for less than 99% availability due to scheduled or unscheduled outages.
- ☐ The service represents or supports an *important business-related back-office support function* that requires general availability to the client's employees or customers, but which may include agreed-upon provisions for less than 99% availability due to scheduled or unscheduled outages.
- ☐ The service represents supports a non-essential, ancillary, and/or value-added function that is not generally subject to high-availability requirements by the client.

NATURE OF THE SENSITIVITY OF THE INFORMATION BEING HANDLED OR PROCESSED

Identify the sensitivity of the information being entrusted into the vendor's care as a required element of the services being offered to the client:

- ☐ The vendor will receive, handle, process, store, and/or transmit *Personally Identifiable Information (PII)* associated with the client's customers, employees, or other involved parties. *(PII includes, but is not limited to, names, addresses, SSNs, DLs, purchase histories, etc.)*
- ☐ The vendor will receive, handle, process, store, and/or transmit *Payment Cardholder Information (PCI)* associated with the client's customers. *(PCI includes debit/credit card numbers, expiration dates, track 1/2 data, etc.)*
- ☐ The vendor will receive, handle, process, store, and/or transmit *Other Types Of Financial Account/Payment Information* associated with the client's customers, employees, or other involved parties. *(This can include bank/brokerage account numbers, ACH codes, balances, debts, etc.)*
- ☐ The vendor will receive, handle, process, store, and/or transmit *Private Health Information (PHI)* associated with the client's customers, employees, or other involved parties. *(PHI can include paper/electronic health records, treatment data, etc.)*
- ☐ The vendor will receive, handle, process, store, and/or transmit *Competitive Business Information* associated with the client's profit-seeking activities, intellectual property, legal/compliance, or other types of data elements subject to client-assigned confidentiality requirements.
- ☐ The vendor will receive, handle, process, store, and/or transmit *Publicly Available Information* associated with the client's overall activities.

OPEN-ENDED QUESTIONS RELATING TO VENDOR'S SECURITY/PRIVACY

For the remainder of this form, supply the best possible written responses to the questions posed within each of the following topic areas. Responses will be compared with the client's own practices in order to determine whether the vendor's practices meet or exceed the maturity levels contemplated by the client as part of the proposed services relationship.

INFORMATION SECURITY MANAGEMENT CAPABILITIES

1. Identify by name/role the vendor senior manager responsible for developing, implementing, and enforcing information security requirements:

2. Identify the size (in FTEs) and skills composition 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:

3. Identify what types of current security-centric certifications are held by members of the security team (e.g., CISSP, CISA/CISM):

4. 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:

REGULATORY/COMPLIANCE ACTIVITIES AND CERTIFICATIONS

1. Identify each of the relevant certifications (and latest compliance dates) maintained by the vendor that speak to independent audit confirmation of the vendor's security practices (examples include PCI DSS/ASV, Sarbanes-Oxley, SAS 70/SSAE 16, HIPAA/HITECH, GLBA, etc.):

2. To the extent that the most recent audit reports identified in question (1) identified any unaddressed security gaps or issues, briefly summarize the steps that have been taken – or are still pending – to fully resolve them:

3. Beyond the scope of the formal audits identified in question (1), please summarize any ongoing security-related audit activities that are regularly performed by the vendor's in-house security team or other third party security firms – including the use of vulnerability scanning and/or penetration testing:

4. In the specific case where healthcare-related data is being managed by the vendor through the additional support of sub-contractors, identify the extent to which the vendor has obtained legally sufficient Business Associate agreements for each of the sub-contractors who will have potential access to the client's PHI data:

PROTECTION/SEGREGATION OF CLIENT-SUPPLIED DATA STRATEGY

1. When sensitive client data of any of the types mentioned earlier (PII, PCI, PHI, Competitive 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.):

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):

3. Identify how access control rights are governed with respect to employee access to client data, including management-driven account provisioning/termination and role-based assignments:

4. Identify how individual servers under vendor's control are pre-hardened in order to minimize the presence of non-essential commands, data, and TCP/IP ports/services prior to their deployment and vendor hosting of sensitive client data:

5. Identify branded solutions currently in use by the vendor that provide for effective anti-virus and malware prevention within the environment(s) that transmit/house sensitive client data:

6. Identify branded solutions currently in use by the vendor that provide for effective intrusion detection/prevention system (IDS/IPS) capabilities within the environment(s) that transmit/house sensitive client data:

7. Identify any branded solutions in use by the vendor that provide for effective data loss prevention (DLP), security information event management (SIEM), distributed denial-of-service (DDoS) or any other types of advanced protection capabilities within the environment(s) that transmit/house sensitive client data:

8. Identify branded solutions currently in use by the vendor that provide for effective change management control and/or automated system patching capabilities within the environment(s) that transmit/house sensitive client data:

APPLICATION DEVELOPMENT SECURITY PRACTICES

1. To the extent that the vendor employs in-house original code developers in the creation/maintenance of applications that transmit/house/process mission-critical and/or sensitive client data, identify who is responsible for security architect functions involving the requirements, design, coding, and testing of new/updated code:

2. Identify the extent to which all original code developers within the vendor's employ have received either formal or informal instruction regarding secure coding practices, such as those promulgated by OWASP or other standards-based entities:

3. Identify the extent to which all new/updated original code that will be utilized to transmit/house/process mission-critical and/or sensitive client data is subjected to pre-production application-level vulnerability scanning (utilizing a commercial solution such as IBM's AppScan, HP's WebInspect, etc.) and/or active penetration testing – preferably by third party security vendors – prior to final deployment decisions:

4. To the extent that the vendor relies upon third party code development vendors within this context, confirm that the vendor has undertaken review of questions (1-3) above with each of the outsourced vendors and has obtained satisfactory responses in all cases.

SERVICE AVAILABILITY AND DISASTER RECOVERY CAPABILITIES

1. Identify the architectural and branded solution-based capabilities by which the vendor has incorporated high-availability (e.g., HOT-HOT, HOT-WARM) technology solutions designed to ensure compliance with client/vendor SLA terms that require real-time availability of services associated with the transmission/hosting/processing of mission-critical client data:

2. Identify the extent to which – if at all – vendor's system availability architecture is based upon geographically diverse placement of nodes/domains constituting the mission-critical services involving client data:

3. Identify the extent to which the vendor performs regular disaster recovery plan testing involving the network/system assets that incorporate the transmission/hosting/processing of mission-critical client data:

4. Identify the extent to which sufficient UPS and longer-term backup generator capacity exist at all vendor locations that incorporate the hosting/processing of mission-critical client data:

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 associated with resolving suspected/confirmed information security incidents:

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

3. Identify the extent to which the vendor employs an assigned Privacy Officer and/or a dedicated privacy management team/function:

4. Within the context of the vendor's privacy program, please identify the capabilities associated with identifying and dealing with a potential data privacy breach that could involve unauthorized exposure of client's sensitive data while in the custody of vendor's environment(s):

5. Identify the extent to which vendor has ready access to skilled data forensics capabilities on either an in-house or external standby basis should the need ever arise:

6. 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:

---

7. 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:

Use Disclaimer

It should be noted that NetDiligence® makes no warranties regarding the use of this template by eRisk Hub clients, and all such use must be considered AS IS without further commitment or obligation by NetDiligence.

Contact Mark Greisiger (email: mark.greisiger@netdiligence.com or phone: 610.525.6383) for questions or comments about this form.