AUDIT WEST

IT Risk & Compliance Advisory Services

# Vendor Risk Assessment Questionnaire

**VENDOR INFORMATION:**

| | |
|---|---|
| Vendor Name: | |
| Vendor Address: | |
| Vendor Contact Name: | |
| Vendor Contact Phone No: | |
| Vendor Contact Email: | |

**DATA SENSITIVITY**

What is the nature of data that vendor will have access to? (Mark all that apply)

☐No Risk: No data exchanged, no security impact

☐Low Risk: Only demographic information and projected financial information

☐Medium Risk: Only names, addresses and phone numbers

☐High Risk: Non-public private information (NPI), for example SSN, medical, financial, proprietary, and private information about real individuals

**Questionnaire Instructions:**

Please complete the following questionnaire. Where details or descriptions are requested, please describe in Comments (or "Additional Information and Comments" section at end of questionnaire), or attach documentation with the requested details. Use N/A for Not Applicable where needed (enter under Comments).

| Risk Assessment Categories | Yes | No | Comments |
|---|---|---|---|
| ***Policies and Procedures*** | | | |
| Has a security policy document(s) been published and enforced in your organization? | ☐ | ☐ | |
| Do you have policies and procedures covering the following: | | | |
| • HR practices? | ☐ | ☐ | |
| • Authorized/acceptable use of networked services? | ☐ | ☐ | |
| • Use of corporate email, intranet, and Internet | ☐ | ☐ | |
| • Password management? | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| • Software/hardware acquisition | ☐ | ☐ | |
| • Change Management? | ☐ | ☐ | |
| • Encryption policy and standards? | ☐ | ☐ | |
| • Security related incident response/handling? | ☐ | ☐ | |
| • Data handling policy (to include data use, storage and destruction of sensitive data)? | ☐ | ☐ | |
| • Third party access and remote access? | ☐ | ☐ | |
| Do you outsource any security management functionality? | ☐ | ☐ | |
| Are policies and procedures updated frequently? | ☐ | ☐ | |
| Is a senior corporate official directly responsible for the implementation of your organizational security policy? | ☐ | ☐ | |
| Are procedures employed to ensure compliance with privacy laws/regulation requirements related to maintaining security, confidentiality, and protection of customer data? | ☐ | ☐ | |
| Do you have information security staff dedicated to the following? | | | |
| • Security awareness? | ☐ | ☐ | |
| • Policy enforcement? | ☐ | ☐ | |
| • Risk evaluation? | ☐ | ☐ | |
| • Risk mitigation? | ☐ | ☐ | |
| • Regulatory compliance? | ☐ | ☐ | |
| Are the consequences of non-compliance to the policies clearly documented? | ☐ | ☐ | |
| ***Patch Management*** | **Yes** | **No** | **Comments** |
| Do you apply security patches on a regular basis? | ☐ | ☐ | |
| Do you have an automated patch management solution deployed? | ☐ | ☐ | |
| Do you have vendor agreements in place for timely availability and application of software updates? | ☐ | ☐ | |
| ***Physical Security*** | **Yes** | **No** | **Comments** |
| What kind of perimeter control(s) are applied to data center location(s)? | | | |
| • Access tokens/cards? | ☐ | ☐ | |
| • Key pad controls? | ☐ | ☐ | |
| • Man trap? | ☐ | ☐ | |
| • Biometric controls? | ☐ | ☐ | |
| • Guards? | ☐ | ☐ | |
| Do you monitor/log all access to data center(s)? | ☐ | ☐ | |
| Do you have redundant public utility connections? | ☐ | ☐ | |
| Do you employ UPS (Uninterrupted Power Supply), battery banks, generators, etc.? | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| Do you employ fire/flood detection and suppression systems? | ☐ | ☐ | |
| Do you monitor and escort visitors through critical parts of your company? | ☐ | ☐ | |
| Do you maintain visitor logs for more than 30 days? | ☐ | ☐ | |
| ***Information Security Administration*** | **Yes** | **No** | **Comments** |
| Can you provide a recent SAS70/SSAE-16 report or other industry recognized audit report? | ☐ | ☐ | |
| Do you limit administrator level access on network and systems infrastructure? | ☐ | ☐ | |
| Is your information security staff professionally certified (i.e ISC2, SANS)? | ☐ | ☐ | |
| What is the average tenure of your information security staff? | ☐ 1-3 years | | |
| | ☐ 3-5 years | | |
| | ☐ 5+ years | | |
| Is access to security logs strictly controlled (firewall logs, IDS logs, etc.) | ☐ | ☐ | |
| Do you employ version management, build & deploy processes? | ☐ | ☐ | |
| ***Network Infrastructure*** | **Yes** | **No** | **Comments** |
| Do you maintain up-to-date network infrastructure and administration procedures? | ☐ | ☐ | |
| Do you have perimeter scanning/monitoring agreements with managed network services providers? | ☐ | ☐ | |
| Are all your routers configured with access control lists to allow only specific traffic to pass through? | ☐ | ☐ | |
| Do you allow access to your routers via console port only? | ☐ | ☐ | |
| Are all networking devices at the latest patch level? | ☐ | ☐ | |
| Do you have a procedure to keep track of announcement of vulnerability patches for your networking devices? | ☐ | ☐ | |
| Do you ensure default passwords are changed on networking devices? | ☐ | ☐ | |
| Do you control the change frequency and distribution of administrative access to network infrastructure? | ☐ | ☐ | |
| Do you use 802.1x or similar security controls for your wireless network? | ☐ | ☐ | |
| Do you employ the following intrusion detection/protection system(s): | | | |
| • HIDS? | ☐ | ☐ | |
| • NIDS? | ☐ | ☐ | |
| • Honey Pots? | ☐ | ☐ | |
| • Rogue device and services detection? | ☐ | ☐ | |

AUDIT WEST

IT Risk & Compliance Advisory Services

| ***Remote Access and VPN*** | **Yes** | **No** | **Comments** |
|---|---|---|---|
| Are there any remote access/remote control methods available to access your network, as follows: | | | |
| • Call backs? | ☐ | ☐ | |
| • PKI? | ☐ | ☐ | |
| • RADIUS/TACACS? | ☐ | ☐ | |
| • User ID/Password? | ☐ | ☐ | |
| • Token based access control? | ☐ | ☐ | |
| • Other? – If yes, please describe. | ☐ | ☐ | |
| Do you allow supervisory/administrative functions to be performed over unencrypted external links? | ☐ | ☐ | |
| Do you collect/review audit log data on remote access? | ☐ | ☐ | |
| ***Firewall and Intrusion Detection/Prevention*** | **Yes** | **No** | **Comments** |
| Do you have a security team that keeps track of all known vulnerabilities? | ☐ | ☐ | |
| Do you have an Intrusion Detection System (IDS) implemented? | ☐ | ☐ | |
| Do you have an incident response team? | ☐ | ☐ | |
| Do you employ firewalls to protect your network? | ☐ | ☐ | |
| Are your firewall operating systems/software at the latest patch level? | ☐ | ☐ | |
| Have you scanned and verified all allowable services provided by your firewall? | ☐ | ☐ | |
| Do you use firewall reporting tools to analyze your firewall log(s)? | ☐ | ☐ | |
| Do you have your security policy on your firewall documented and verified? | ☐ | ☐ | |
| Do you protect your internal IP address range(s) (e.g., use NAT/RFC1918)? | ☐ | ☐ | |
| Do you restrict both inbound and outbound traffic to only that which is necessary? | ☐ | ☐ | |
| ***Malware Controls*** | **Yes** | **No** | **Comments** |
| Do you scan all emails for viruses? | ☐ | ☐ | |
| Is there an explicit policy requiring anti-virus software on networked computers? | ☐ | ☐ | |
| Do you have centralized administration of virus controls, such as distribution of signature updates, reporting, and policy enforcement? | ☐ | ☐ | |
| Are rules established for scanning outside software and media? | ☐ | ☐ | |
| Does your anti-virus software run in the background with established frequency of scanning? | ☐ | ☐ | |
| Are end users prevented from disabling anti-virus software on personal computers? | ☐ | ☐ | |

| | | | |
|---|---|---|---|
| Do you allow installation of personal and non-corporate approved software on network computers? | ☐ | ☐ | |
| ***Disaster Recovery and Business Continuity*** | **Yes** | **No** | **Comments** |
| Are backup/recovery procedures regularly tested? | ☐ | ☐ | |
| Are backup/restore procedures documented? | ☐ | ☐ | |
| Can you meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services contracted for? | ☐ | ☐ | |
| Is there a business continuity plan (BCP)? | ☐ | ☐ | |
| ***Monitoring*** | **Yes** | **No** | **Comments** |
| Do you monitor the security/policy violations and application/networked services availability? | ☐ | ☐ | |
| Do you log successes and failures to access? | ☐ | ☐ | |
| ***Account Management and Access Control*** | **Yes** | **No** | **Comments** |
| How will our data be secured at your site? | | | |
| Will our data be accessible from the Internet? | ☐ | ☐ | |
| Who will have access to our data? | | | |
| How do you prevent other clients from accessing our data? | | | |
| How and where are user IDs and Passwords stored? How are they secured? | | | |
| Will access credentials be encrypted when passing through public networks? | ☐ | ☐ | |
| Do you employ any mechanisms that facilitate secure data exchange? | ☐ | ☐ | |
| ***E-Commerce (applicable if vendor conducts business online)*** | **Yes** | **No** | **Comments** |
| Are the following maintained in e-commerce systems: | | | |
| • Confidentiality? | ☐ | ☐ | |
| • Authorization? | ☐ | ☐ | |
| • Non-Repudiation? | ☐ | ☐ | |
| • Transaction Integrity? | ☐ | ☐ | |
| • Access code encryption in storage and transmission? | ☐ | ☐ | |

**ADDITIONAL INFORMATION AND COMMENTS:**