**REVISED EXHIBIT D**

**VENDOR RISK ASSESSMENT QUESTIONS**

**BIDDERS MUST SUBMIT THIS REVISED EXHIBIT D AS PART OF THEIR BID. USE THE SPACE BELOW TO PROVIDE A RESPONSE/COMMENTS FOR EACH REQUIREMENT.**

|  |
| --- |
| Security Certifications |
| Shall have a Service Organization Control (SOC) Report |
| Shall have a HIPAA Certification |
| Risk Management |
| Shall have a risk assessment program that has been approved by management, communicated to appropriate constituents and has an owner to maintain and review the program |
| Shall have a risk treatment plan that has been communicated to management |
| Compliance |
| Shall have an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues |
| Shall have audits performed to ensure compliance with any legal, regulatory or industry requirements |
| Shall have procedures to ensure compliance with legislative, regulatory, and contractual requirements on the use of material where intellectual property rights may be applied |
| Shall have an internal compliance and ethics reporting mechanism and training program for constituents to report compliance issues |
| Right to Audit |
| Shall allow Alameda county to audit the service you will provide |
| Security Policy |
| Shall have an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy |
| Shall have employees to annually re-acknowledge compliance with information security policies |
| Shall have a well-planned internal audit plan to measure compliance with Information Security Policies |
| Shall perform periodic reviews to update security policies and guidelines for relevance and emerging topics |
| Shall have controls in place to restrict your ability to transmit customer data to unauthorized personnel outside the company |
| Security Organization |
| Shall have a full time information security officer |
| Shall have roles and responsibilities for protecting assets and implementing security measure explicitly defined and communicated to all department/groups |
| Have a formal risk analysis process to assist management in identifying security threats |
| Awareness & Training |
| Shall have a formal , on-going Security Training program |
| Implemented a process to measure effectiveness of security training |
| The on-going Security Awareness program to include instructing users on how to detect and avoid social engineering attacks |
| Users are being educated on how to report suspected security violations or vulnerabilities |
| The importance of Information Security visible through the organization (e.g. posters, company meetings etc.) |
| Recruitment Process/New Employee Orientation |
| New hire workers subjected to a history and background check |
| Employees receive introductory security awareness training |
| Employee Exit /Transfer |
| Human Resource department provide administrators with a list of: Workers transferring department Workers leaving company |
| There is a process to notify system administrator when workers leave the business |
| Exit interviews conducted to recover the property given to worker\ |
| There is a program for immediate removal of employees system access when departing employee is identified as disgruntled or high risk |
| Access /exit controls employed in your facility |
| Change Management |
| Shall have document change control procedures to manage all modification to development/production environment |
| Change control performed on regular basis |
| Changes are approved in change control document |
| Alameda County to sign off on the changes affecting them |
| There is a documented procedure for performing emergency changes outside the change control process. |
| Router /Firewall |
| Shall always maintain a current network diagram |
| At a minimum , state full firewall been deployed at all external connections |
| firewall configured with policy that all services are denied unless expressly permitted |
| Have a process /criteria to evaluate the risk of protocols/port before implementing it on firewall |
| All services prohibited unless specifically requested |
| Access to all firewalls, routers and proxies restricted to only those individuals who need to manage these devices |
| There a process in place to ensure that all routers /firewalls have the latest software and that they are patched regularly |
| VPN and remote access |
| Shall not allow remote access to computers that do not implement antivirus software |
| Shall have a process in place to cancel VPN access rights as soon as their project is completed or their reason for having VPN access is invalidated |
| Security In Application Development |
| Shall have system development methodology address information security during the discovery and development phase |
| Shall perform a security code review during each phase of development |
| Are there separate environments for each customer for development and testing of systems |
| All software developers working on software given orientation in security requirements of customer before they start to work on project |
| There shall no employees with access to both the non-production and the production environment |
| All developed software tested for viruses and background before they are pushed to production |
| Data Security |
| Backups of business critical data done regularly |
| Sensitive data at rest and in motion are encrypted |
| Have an on-line mechanism to verify that all backups complete successfully |
| Periodically restore information from backup tapes to ensure data integrity |
| Backup tapes kept in an environmentally controlled and secured area |
| There is a regular audit conducted to account for all backup tapes |
| Backup tapes destroyed if yes then what is the procedure used to destroy them |
| Data Classification |
| All critical business data have an owner |
| Critical information classified according to a classification guideline |
| Access to sensitive customer data have to be authorized by the owners of the data |
| Server Vulnerability and Hardening |
| There is a process to proactively obtain latest security patches and updates |
| Shall have a process to identify network, application and OS based systems vulnerabilities |
| Shall use automated tools to assess system vulnerabilities |
| Shall perform regular penetration testing at periodic intervals by an external vendor |
| Have all business critical systems used in customer software development been analyzed for their security risks |
| Users with super user privileged reviewed and revised regularly |
| Have Antivirus software running on all you systems used for Customers |
| Have a procedure to ensure that all servers, User machines and laptops are configured to automatically install virus definition files |
| Account Management |
| All user account deleted on users departure date |
| System to disable user account after a period of inactivity |
| System to lock user accounts after a number of failed login attempts |
| Shall have privilege accounts fully logged and subject to regular review |
| Shall have a policy on privilege accounts |
| Have a completed list of personnel having admin or root privileges |
| Shall disable all the default accounts in all your server applications |
| Password Management and Authentication |
| All users forced to change their passwords at first sign-on |
| Shall have passwords expire periodically |
| All users shall be prohibited from frequently re-using passwords |
| Monitoring and Logging |
| Shall have security auditing enabled on business critical systems |
| Shall have process to review security audit logs in timely, consistent manner and act upon any threats identified on those reviews |
| There is an automated alerting/notification process that is initiated when defined security threshold exceeds |
| Shall use effective IDS, URL filtering and other security monitoring software |
| Incident Response |
| There is a process for user to report when they have identified a potential security incident |
| Shall have a documented security incident response procedure |
| Shall communicate the security Incident Response procedure to all employees |
| Conduct drills to verify the readiness of the company to any security incident |
| Disaster Recovery |
| Shall have formal written Disaster Recovery Plans covering the partial or full loss of servers , critical applications, physical facilities |
| Are there disaster recovery facilities for critical system located in geographically independent area |
| Shall have an owner responsible for devising and maintaining DRPs |
| Laptop Security |
| There is a process to ensure that business and customer critical data is encrypted |
| All employees who travel with laptops provided with the theft prevention devices |
| Physical Security (Server Rooms) |
| Are servers kept in protected areas with restricted access |
| Shall periodically review list of people who have access to server room |
| Asset Inventory |
| Shall have an inventory of authorized assets and are they regularly reviewed |
| There is a process in place to ensure that inventory for all computer equipment is maintained for accuracy |
| Shall have a method of secure disposal on unwanted documents and equipment's |