# CONTROLS AND CYBERSECURITY QUESTIONNAIRE

# General Information

|  |  |
| --- | --- |
| **Contact Information Detailed Information** | |
| Organization Name: |  |
| Head Office Location: |  |
| Overall Account Manager Name: |  |
| Overall Account Manager Phone Number: |  |
| Overall Account Manager Email Address: |  |
| Technical Contact Name: |  |
| Technical Contact Phone Number: |  |
| Technical Contact Email Address: |  |
| **Assessment Owner Information (This section should be completed by CONTRACTING ORGANIZATION)** | |
| Assessment Owner Name: |  |
| Assessment Owner Title: |  |
| Assessment Owner Phone Number: |  |
| Assessment Owner Email Address: |  |
| Date Questionnaire Submitted: |  |

# Security

*Please answer the following items by placing an ‘x’ in the appropriate yes/no column.*

*Please also provide any additional details in the ‘comment’ field to ensure clarity and understanding.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Category** | **Yes** | **No** | **Comment** |
| **Assessment and Authorization** |  |  |  |
| Do you have a governing body to review and approve information system changes; e.g., change control |  |  |  |
| Do you enforce change control for your information systems |  |  |  |
| Do you monitor your information systems to enforce security requirements and compliance with security policies |  |  |  |
|  |  |  |  |
| **Risk Assessment** |  |  |  |
| Do you maintain or adopt a consistent risk assessment approach, methodology or framework, e.g. NIST-800 SP30 |  |  |  |
| Do you have a documented security risk assessment program for your information systems |  |  |  |
| Do you perform regular security assessments of your information systems |  |  |  |
| Do you monitor and scan information systems for unauthorized access and security vulnerabilities |  |  |  |
| Do you scan your information systems for security vulnerabilities at least once a year |  |  |  |
| Do you use 3rd party tools or services to perform your security vulnerability scans |  |  |  |
| Can you provide documentation describing your vulnerability assessment and remediation processes |  |  |  |
| Do you perform security risk assessments on all new information systems before they are implemented |  |  |  |
| Do you perform security risk assessments on all new business processes before they are implemented |  |  |  |
| Do you perform security risk assessments on all new hardware, software, infrastructure and equipment prior to implementation |  |  |  |
| Do you use 3rd party to perform security assessment of your information systems |  |  |  |
| Do you have a structured process to resolve all critical vulnerabilities identified during a penetration test? |  |  |  |
|  |  |  |  |
| **System and Services Acquisition** |  |  |  |
| Do you perform security assessments of your suppliers, contractors and business partners |  |  |  |
| Do you perform security assessments of third party products and services |  |  |  |
| Do you track and maintain software licensing in accordance with licensing, contracts, copyright and exportation laws, e.g. Export Control Classification Number |  |  |  |
| Do you monitor and track the download and installation of software |  |  |  |
| Do you allow unlicensed software on your information systems |  |  |  |
| Do you have policies governing who, where and how software can be installed |  |  |  |
|  |  |  |  |
| **Program Management** |  |  |  |
| Do you have an information security officer |  |  |  |
| Do you have a senior corporate officer responsible for the implementation and enforcement of your security policies |  |  |  |
| Do you have Information Security staff to support Security Awareness, Policy Enforcement, Risk Assessment and Mitigation, and Regulatory Compliance activities |  |  |  |
| Do you outsource any part of your information security program |  |  |  |
| Do you publish and maintain corporate security policies |  |  |  |
| If requested can you supply copies of relevant security policies |  |  |  |
| Are there documented penalties for noncompliance with your security policies |  |  |  |
| Are your security policies evaluated annually |  |  |  |
| Are your security policy updates based on risk assessments |  |  |  |
| If requested can you supply documentation describing the processes you use to ensure you are compliant with relevant laws and regulations governing data or physical security |  |  |  |
| Do you adopt a risk certification and accreditation policy in your security program (e.g. ISO) |  |  |  |
|  |  |  |  |
| **Awareness and Training** |  |  |  |
| Do you maintain a formal security awareness and training program |  |  |  |
| Are all employees and contractors required to participate in security awareness training |  |  |  |
|  |  |  |  |
| **Configuration Management** |  |  |  |
| Do you maintain a Configuration Management program for your information systems |  |  |  |
| Do you evaluate and approve standard system configurations based on security policies |  |  |  |
| Are unnecessary ports, services and functions removed or disabled as part of your standard information systems configurations |  |  |  |
| If required, can you document the enabled ports, services and functions in your standard system configuration |  |  |  |
| Do you have a security configuration baseline enforced by security policies to all the information systems |  |  |  |
|  |  |  |  |
| **Disaster Recovery** |  |  |  |
| Do you maintain a tested and repeatable backup and recovery plan |  |  |  |
| Is a business impact analysis used to identify critical business processes |  |  |  |
| Do you have documented SLAs for recovery of critical business processes |  |  |  |
|  |  |  |  |
| **Incident Response** |  |  |  |
| Do you maintain a security incident response plan |  |  |  |
| If requested, can you supply documentation describing your security incident response plan |  |  |  |
| Do you have a process for notifying customers of potential or confirmed security incidents |  |  |  |
| Are you insured to cover the cost of security breaches and subsequent corrective efforts |  |  |  |
|  |  |  |  |
| **Maintenance** |  |  |  |
| Do you test and apply security patches for your information systems on a regular basis |  |  |  |
| Do you use an automated security patch management solution for your information systems |  |  |  |
| If requested can you supply documentation describing your security patching process |  |  |  |
| Do you use an automated solution to apply manufacturer updates to your information systems |  |  |  |
|  |  |  |  |
| **Media Protection** |  |  |  |
| Do you have security policies governing electronic media |  |  |  |
| Do you have security policies for media sanitization |  |  |  |
| Do you have a documented process to securely remove data from media that is to be reused or discarded |  |  |  |
| Do you shred confidential paper waste |  |  |  |
|  |  |  |  |
| **Physical and Environmental Protection** |  |  |  |
| Do you adhere to formal information security standards or certifications such as NIST, ISO, COBIT, ITIL, PCI DSS |  |  |  |
| Do you adhere to any formal information security regulations such as SOX, HIPAA, FISMA |  |  |  |
| Does your data center meet Tier 3 data center facility standards as specified in the TIA-942 standard published by the Telecommunications Industry Association |  |  |  |
| Can you provide a current SSAE report or other industry recognized audit report |  |  |  |
| Can you provide documentation describing the security controls for your information systems facilities |  |  |  |
| Is your data center staffed 24/7 |  |  |  |
| Does your data center use electronic locks or key pads |  |  |  |
| Does your data center use badges, tokens or access cards |  |  |  |
| Does your data center use biometric readers |  |  |  |
| Does your data center use man traps |  |  |  |
| Does your data center use guards |  |  |  |
| Does your data center use locked cages |  |  |  |
| Does your data center use UPS (Uninterrupted Power Supply) and Generators |  |  |  |
| Does your data center have redundant utility and service connections |  |  |  |
| Does your data center have fire and flood detection and suppression systems |  |  |  |
| Do you have a documented approval and authorization process for granting access to your data center |  |  |  |
| Can you document the personnel with physical access to your data center |  |  |  |
| Can you document the personnel with remote access to your data center |  |  |  |
| Are visitors required to sign in before accessing your facilities |  |  |  |
| Do you maintain visitor logs for your facilities for more than 30 days |  |  |  |
| Do you monitor and escort visitors at all times while in your facilities |  |  |  |
| Are all service providers escorted at all times while accessing your facilities |  |  |  |
| Are all service providers screened before being granted access to your facilities |  |  |  |
|  |  |  |  |
| **Personnel Security** |  |  |  |
| Do you perform background checks on all employees and contractors |  |  |  |
|  |  |  |  |
| **System and Information integrity** |  |  |  |
| Do you use an automated anti-virus and malware detection solution for all of your information systems |  |  |  |
| Do you use a monitoring system to detect unauthorized access and security attacks on your information systems |  |  |  |
| Do you use an intrusion prevention or detection system |  |  |  |
| Are firewalls used to control access to all of your public facing information systems |  |  |  |
| Do you review and log all firewall activities |  |  |  |
| Are default vendor or manufacturer passwords changed for all information system devices and applications |  |  |  |
| Are your information systems maintained at current security patch levels |  |  |  |
| Do you use web application firewalls to protect all your web applications? Just public internet facing? |  |  |  |
|  |  |  |  |
| **Third Party Providers** |  |  |  |
| Do you maintain a program to assess your suppliers’ ability to comply with your security policies and requirements |  |  |  |
| Do you communicate your security policies to your suppliers, business partners and contractors regularly |  |  |  |
| Do you have a program to assess and review security risks presented by your vendors |  |  |  |
| Do you have a program to monitor your suppliers’ performance and service level agreement compliance |  |  |  |
| Do your business partners or contractors have access to your customer’s data or customer’s systems |  |  |  |
|  |  |  |  |
| **Data Protection** |  |  |  |
| Do you have the ability to encrypt confidential data while “at rest” |  |  |  |
| Do you have the ability to encrypt confidential data while “in transit” |  |  |  |
| If requested can you provide documentation that describes the technology and processes you use to secure confidential data |  |  |  |
| Do you separate your corporate data from the data belonging to your customers |  |  |  |
| Can you maintain separation between the data belonging to each of your customers |  |  |  |
| If requested can you provide formal documentation that describes how you maintain separation for your customer’s data |  |  |  |
| Can you maintain physical and/or logical separation between the data belonging to each of your customers |  |  |  |
| If requested, can you provide formal documentation that describes how you maintain separation for each of your customer’s data |  |  |  |
|  |  |  |  |
| **Access Controls** |  |  |  |
| Do you have security policies governing access to your information systems? |  |  |  |
| Do you have a documented process for user account management? |  |  |  |
| Is access to your information systems and data restricted according to the least level of privilege and by job role? |  |  |  |
| Do you have security policies to govern who has remote access to your information system and how? |  |  |  |
| Do you have security policies governing the secure use of mobile devices to access your information systems? |  |  |  |
| Do you enforce strong authentication requirements on internal network systems which may be used to administer, monitor, and or control systems containing customer data? |  |  |  |
|  |  |  |  |
| **Audit and Accountability** |  |  |  |
| Do you have security policies governing audit requirements for your information systems? |  |  |  |
| Do you enforce auditing and logging processes for account management? |  |  |  |
| Do you perform regular physical audits? |  |  |  |
| Do you perform regular audits of your information systems? |  |  |  |
| Do you use group or shared accounts on a regular basis for performing critical functions and/or administrative tasks on the systems housing customer data? |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Identification and Authentication** |  |  |  |
| Do you have security policies requiring all users to be uniquely identified and authenticated? |  |  |  |
| Do you use a centralized identity management system to authenticate personnel, business partners, contractors or customers? |  |  |  |
| Do you have security policies governing password strength, usage and expiration? Password strength includes items such as minimum length, complexity requirements, etc. |  |  |  |
| Do you have security policies requiring user identities to be verified before their passwords are reset or re-issued? |  |  |  |
| Do you have security policies requiring passwords to be encrypted in storage and in transmission? |  |  |  |
| Do you have security policies restricting the number of unsuccessful login attempts to your information systems? |  |  |  |
| Do you have security policies requiring multifactor authentication for remote access? |  |  |  |
|  |  |  |  |
| **System and Communications Protection** |  |  |  |
| Do you have security policies requiring encryption of confidential data during transmission? |  |  |  |
| Do you enforce use of current protocols such as SSLv3 and TLSv1.1? |  |  |  |
| Do you have security policies requiring encryption of confidential data during storage? |  |  |  |
| Do you have security policies governing minimum levels of encryption for data at rest (e.g. AES-256)? |  |  |  |
| If requested can you provide additional documentation describing how you encrypt confidential data in transit and at rest? |  |  |  |
|  |  |  |  |
| **Application Security** |  |  |  |
| Do you periodically test your application for security vulnerabilities? |  |  |  |
| Do you have a documented process for remediation of vulnerabilities detected during security testing? |  |  |  |
| Do you leverage 3rd party enterprise grade tools to perform automated scanning of the application (e.g. HP Web Inspect, IBM App Scan, etc)? |  |  |  |
| Do you leverage open source free tools to perform manual security testing (e.g. OWASP ZAP, Burp Proxy, Nikto, etc)? |  |  |  |
| Do you perform static code analysis to identify potential security vulnerabilities in the application prior to deployment? |  |  |  |
| Does your application have any known security vulnerabilities? |  |  |  |
| Do you have a documented process for supplying security patches and notifying your customers about known security vulnerabilities? |  |  |  |
| Does your application require support or services from 3rd parties? |  |  |  |
| Do you have a dedicated customer support team for your product? |  |  |  |
| Does your application send data over the internet to other 3rd parties? |  |  |  |
| Does your application support secure transmission of data over the internet by using TLS, SSL, SSH or SFTP? |  |  |  |
| Does your application require the use of an internet accessible web interface? |  |  |  |
| Does your application integrate with common operating systems, network infrastructure and database platforms? |  |  |  |
| Do you document the operating systems, infrastructure and databases that are not supported by your application? |  |  |  |
| Will updating the application platform or supporting infrastructure void the application warranty or support agreement? |  |  |  |
| Is the application compatible with commercial antivirus and malware software? |  |  |  |
| Does the application have the ability to archive transactions or snapshots of data between backups? |  |  |  |
| Do you outsource any of the components in your application? |  |  |  |
| Are service accounts required to run the application? |  |  |  |
| Can the application administrator enforce password policies for complexity, strength, age, expiration and reuse? |  |  |  |
| Does the application force users to change their password upon first login into the application? |  |  |  |
| Are application passwords encrypted at all times; in transit and at rest? |  |  |  |
| Does the application ‘salt’ passwords when encrypting/hashing? |  |  |  |
| Are application passwords ever viewable in clear text by users, administrators, support personnel or developers? |  |  |  |
| Can the application be configured to lock user accounts after a predetermined number of consecutive unsuccessful logon attempts? |  |  |  |
| Can the application prevent users from logging into the application more than once at the same time with the same user ID? In other words, are multiple sessions allowed for the same user? |  |  |  |
| Does the application allow for strict, granular control over user access to only allow access to functions required for the user to do their job (role based access in support of least privilege)? |  |  |  |
| Can the application be configured to disconnect user sessions after predefined period of inactivity (e.g. 15 minute session time-out)? |  |  |  |
| Does the application require users to have local administrator permissions for it to function? |  |  |  |
| Do application administrators require local administrator permissions? |  |  |  |
| Is there documentation that describes the application’s security configuration requirements? |  |  |  |
| Is there documentation that explains where and how application IDs and passwords are stored and secured? |  |  |  |
| Have the application’s security controls been tested by an independent 3rd party? |  |  |  |
| Does the application produce audit logs? |  |  |  |
| Can the application audit logs be encrypted? |  |  |  |
| Does the application have the ability to audit user activities based on predefined or customizable business rules? |  |  |  |
| Does the application have the ability to send alerts or emails based on audit logging events? |  |  |  |
| Are there any limitations or restrictions on the application’s ability to perform audit logging? |  |  |  |
| Can the application log user authentication activities such as unsuccessful logons, successful logons and logoffs? |  |  |  |
| Can the application audit logs be exported in a standard format for consumption by log aggregation solutions (e.g. Splunk) for centralized storage and reference purposes? |  |  |  |
| Is there documentation that describes the auditing functionality, features and capabilities? |  |  |  |
| Can the application audit and log user activities such as application screens viewed and application reports printed? |  |  |  |
| Does the application integrate with or support 3rd party audit protocols and tools such as NTP? |  |  |  |
| Does the application have predefined audit log reporting capability? |  |  |  |
| Does the application have customizable audit log reporting capability? |  |  |  |
| Does the application require additional 3rd party software or systems for audit logging or reporting functionality? |  |  |  |
| Are the audit log files protected from unauthorized access? |  |  |  |
| Does the application administrator have the ability to determine which events to audit and log based on policy? |  |  |  |
| Can access to audit logs be restricted by job role? |  |  |  |
| Does your application integrate with enterprise identity management tools for *authentication*? |  |  |  |
| Does your application integrate with enterprise identity management tools for *authorization* to the application resources and operations? |  |  |  |
| Do you have documentation that explains how your application manages security for application *users*? |  |  |  |
| Do you have documentation that explains how your application manages security for application *data*? |  |  |  |
| Do you follow a Secure Development Lifecycle program? |  |  |  |
| Are security principles incorporated into the design and development of your application? |  |  |  |
| Do you use version management during your development process? |  |  |  |
| Can you provide documentation explaining how security is incorporated into each phase of your application development life cycle? |  |  |  |
| Do you follow OWASP guidelines for the development of secure web applications and web services? |  |  |  |
| Does your support staff require remote access to the application? |  |  |  |
| Does your support staff require direct access to the application? |  |  |  |
| Can you provide documentation that describes your support personnel’s requirements for application support activities? |  |  |  |
| Does the application provide remote support access or control capability? |  |  |  |
| Do you have an automated process to ensure software development tools are updated and patched regularly? |  |  |  |
| Do you have a process for development and release of application updates and patches? |  |  |  |
| Do you have a process to identify and release security patches on a regular basis? |  |  |  |
| Was your application code security testing performed by an internal resource? |  |  |  |
| Was your application code review performed by a 3rd party? |  |  |  |
| Do you have a process for regular security testing of your application code? |  |  |  |
| Can you provide documentation that describes your security testing and remediation processes and the security testing tools or services used? |  |  |  |
| Do you conduct security testing separately from functional testing? |  |  |  |
| Do you have a formal security patch update process that corresponds to your application security assessments? |  |  |  |
| Do you have a process to provide customer support for your application’s security vulnerabilities; including exploits and mitigation strategies? |  |  |  |
| Do you have an ongoing secure application development training program for your development and testing personnel? |  |  |  |
| Do your application development and teams receive regular training updates on current secure application development best practices? |  |  |  |
| Do you have a formal process to notify your customers of security issues related to the use of your application? |  |  |  |
| Do you have a formal process for customers to report security problems associated with your application? |  |  |  |
| Can you provide documentation that describes the code base for your application; e.g. Ajax, Java, Javascript, .NET , PHP, Ruby, Python? |  |  |  |
| Can you provide documentation explaining how to securely configure your application? |  |  |  |