|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| S:\InformationTechnology\IT Security\General Documents\Images and Branding\ITSecurity_Logo.png | THIRD-PARTY ASSESSMENT FORM | | | | | | |
| Note: Prior to finalizing business agreements involving confidential data, this completed form should be sent to the TRS Information Security Office ([InfoSec@trs.texas.gov](mailto:InfoSec@trs.texas.gov)) for review concerning the security of information with respect to legal or regulatory compliance and industry standard best practices | | | | | | | |
| Third-Party Provider Name: | | | | |  | Date: |  |
| Address: | | | | |  | Website: |  |
| Support Contact: | | Email: | |  | | Phone: |  |
| Information Security Contact: | | Email: | |  | | Phone: |  |
| **Name of the Service/Product:** | | | | | | | |
| **Technical Description of Communications**:(Client/Agent, Web/TLS, File Transmission, hosted website/WebApp, ASP, etc., SAAS/PAAS/IAAS): | | |  | | | | |
|  | | | | |
| **Describe Pertinent Outsourced/Contracted Service Arrangements:** (such as onsite support, remote support, temporary access, database management, etc.): | | |  | | | | |
|  | | | | |
| **Providing an attestation report from within the last year can be sent to supplement this form.**  **If applicable, please select which form will be sent:**  SOC 2 Type 2 Report  FedRAMP Certification  HITRUST Report  CAIQ  ISO 27001  ISO 27017  SIG | | | | | | | |
| **Is the product/service, either wholly or partially, built in an environment hosted by the following Cloud Service Providers: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle, or IBM?**  AWS  Azure  GCP  Oracle  IBM | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Preliminary Questions  *Teacher Retirement System conducts Assessments on all third parties. Not all assessment questions are relevant to each party.* | Answers | | Category |  |
| What services will TRS receive and what will be included in the service level agreement? |  | | **Overview** |  |
| Has your company obtained a TX-Ramp certification or in the process of doing so?  The Department of Information Resources now mandates that all state agencies contract with computing services that comply with TX-RAMP requirements. |  | | **Overview** |  |
| Will your service/product process or store any confidential information such as Personally Identifiable Information (PII) or Material Non-Public Information (MNPI)? |  | | **Overview** |  |
| Will your product process any protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)? |  | | **Overview** |  |
| Does your company have an established Business Continuity and Disaster Recovery Plan (BCP/DRP)? |  | | **Overview** |  |
| Do you comply with any specific industry standard security framework? (e.g., NIST Special Publication 800-53, ISO 27002, etc.) |  | | **Overview** |  |
| How long has your company conducted business in this industry? |  | | **Overview** |  |
| Describe the structure and size of your Information Security staff. (e.g. Admin, Engineering, QA/Compliance, etc.) |  | | **Overview** |  |
| Describe the structure and size of your Software and System Development teams. (e.g. TRS Support, Implementation, Product Management, etc.) |  | | **Overview** |  |
| Use this area to share information about your environment that will assist those who are evaluating you company data security safeguards. |  | | **Overview** |  |
| Questions | | **Answers** | **Category** |  |
| Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act? | |  | **HIPAA** |  |
| Do you monitor or receive information regarding changes in HIPAA regulations? | |  | **HIPAA** |  |
| Has your organization designated HIPAA Privacy and Security officers as required by the HIPAA Security Rules? | |  | **HIPAA** |  |
| Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)? | |  | **HIPAA** |  |
| Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents? | |  | **HIPAA** |  |
| Do you have a plan to comply with the Breach Notification requirements if there is a breach of data? | |  | **HIPAA** |  |
| Have you conducted a risk analysis as required under the HIPAA Security Rule? | |  | **HIPAA** |  |
| Are you willing to enter into a Business Associate Agreement (BAA)? | |  | **HIPAA** |  |
| Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI) | |  | **HIPAA** |  |
| Can you provide a HIPAA compliance attestation document? | |  | **HIPAA** |  |
|  | |  |  |  |
| Assessment: | | **Answers** | **Category** | **Sub-Category** |
| Has the relevant application been tested for vulnerabilities by a third party? | |  | Application | Quality Assurance |
| State the date of the last test conducted. | |  | Application | Quality Assurance |
| How often does your organization perform vulnerability assessments of the specific product(s) that TRS is interested in utilizing? | |  | Application | Quality Assurance |
| Does your organization have an application security team, focused on secure coding of the relevant applications? | |  | Application | Quality Assurance |
| Do you have alternate data centers in case of disasters? | |  | Business Continuity | Precautions |
| Does your solution support redundancy and load balancing? | |  | Business Continuity | Precautions |
| Are any of your data center located in areas that have a high risk/probability of occurrence for high impact disasters (floods, tornadoes, earthquakes, etc)? | |  | Business Continuity | Precautions |
| Has your organization designated and documented points of contact in case of a disaster? | |  | Business Continuity | Disaster |
| Is there insurance in place for disaster recovery scenarios? If so, please describe. | |  | Business Continuity | Disaster |
| Do you share your business continuity and redundancy plans with your tenants? | |  | Business Continuity | Disaster |
| Describe policies and procedures established for management authorization systems for development or acquisition of new applications, systems, databases, infrastructure, services, and operations? | |  | Change Management |  |
| Does your organization follow a documented Request For Change (RFC) process before implementing any changes? If so, please describe the process. If not, how are requests for change handled? | |  | Change Management |  |
| Does your organization create implementation and back-out plans before action on any proposed changes? If so, please describe the process of creating and auditing these plans. | |  | Change Management |  |
| Is documentation available that describes the installation, configuration and use of products/ services/ features? | |  | Change Management |  |
| Does your company have a quality manual that describes an overview of your key standards for coding, testing, integration, large data volumes, and other areas that affect services? | |  | Change Management |  |
| Do you have controls in place to ensure that all organizationally set standards of quality are being met on all software development? Please describe the controls. | |  | Change Management |  |
| Describe or provide a reference to your solution support strategy in relation to maintaining software currency (i.e. how many concurrent versions are you willing to run and support?). | |  | Change Management |  |
| Is there a documented process for keeping all network equipment up to date with the most current level of patches and updates? | |  | Change Management |  |
| Describe the highest level of data classification that will be managed within your system(s) and/or application(s) (e.g.: Public/ Private/ Internal/ Secret/ Restricted). | |  | Data | TRS Data |
| What TRS data will be stored or transmitted? Include security considerations of sensitive data. | |  | Data | TRS Data |
| How and when is TRS data deleted? | |  | Data | TRS Data |
| Will you be able to provide Certificate of Data Destruction or Erasure after the data has been deleted? | |  | Data | TRS Data |
| How long will the institution's data be available within the system at the completion of this contract? | |  | Data | TRS Data |
| What procedures are in place for handling client confidential information? | |  | Data | TRS Data |
| Is TRS data isolated in a multi-tenant environment? | |  | Data | TRS Data |
| If TRS data is stored in a shared environment, what protections are in place to maintain isolation and privacy of TRS data? | |  | Data | TRS Data |
| Is personal information about TRS transmitted to or received from countries outside of the U.S.? If so, please list the countries. | |  | Data | TRS Data |
| Do you use encryption for data leakage protection? | |  | Data | Encryption |
| How do you encrypt data during transmission and at rest? | |  | Data | Encryption |
| Does your product use HTTPS/TLS for all sensitive communications over the network? | |  | Data | Encryption |
| Is your TLS certificate management a manual or automated process? | |  | Data | Encryption |
| Is a formal risk assessment performed annually? | |  | Governance | Risk Management |
| Does your organization have a governance committee that reports to the board? If so, what are the governance committee's responsibilities? | |  | Governance | Risk Management |
| Are employees subject to background checks? Please describe the type and level of background check. | |  | Human Resources | Policies |
| Are contractors and temporary workers subject to background checks? | |  | Human Resources | Policies |
| Are employees required to sign NDA or confidentiality agreements? | |  | Human Resources | Policies |
| Describe password rules that are enforced for employees for critical systems (e.g. intranet, email). | |  | Human Resources | Policies |
| Describe all documented procedures in place to govern change in employment or termination. | |  | Human Resources | Policies |
| Describe any employee access to client data. | |  | Human Resources | Employee Access |
| How are workplace devices encrypted? | |  | Human Resources | Employee Access |
| If applicable, how are employees able to access our data remotely? | |  | Human Resources | Employee Access |
| Is access to data restricted across your employees on a need to know basis? | |  | Human Resources | Employee Access |
| Do you use antivirus software on all work devices? | |  | Human Resources | Employee Access |
| Describe the organizational structure of your security team. Provide details including roles, responsibilities, and number of team members. | |  | Human Resources | Security Team |
| Are employees required to complete any security awareness training? If so, please describe, including content and frequency. | |  | Human Resources | Training |
| Does your company have a dedicated Security Officer? If so, please describe their official training and certifications. | |  | Human Resources | Security Team |
| Does your organization monitor security threats and attack trends, and how those trends may affect your Platform? | |  | Incident Management | Research |
| Do you have a Bring Your Own Device (BYOD) policy that defines the device(s) and eligibility requirements for BYOD usage? Include any personal electronic devices that are used for work purposes. | |  | Mobile Security | Device Management |
| Do you have password policies for enterprise issued mobile devices or BYOD mobile devices? | |  | Mobile Security | Device Management |
| Do you have a documented and approved list of application stores and applications? | |  | Mobile Security | Device Management |
| Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data? | |  | Mobile Security | Device Management |
| Please describe security systems in place for visitors, including badges, supervision, and sign-in systems. | |  | Physical Security | Access |
| Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process? | |  | Physical Security | Access |
| Are closed-circuit cameras utilized at all entrances and exits in your offices? | |  | Physical Security | Monitoring |
| Does your organization utilize security guards and other physical protections within your office(s)? | |  | Physical Security | Monitoring |
| Describe the access authorization to areas housing sensitive information and equipment. | |  | Physical Security | Access |
| Where are your data centers located? Provide locations for any backup and redundant data centers. | |  | Physical Security | Data Centers |
| Describe physical access controls to your data centers. | |  | Physical Security | Data Centers |
| Do you self-host or use third party for servers? What type of security do the third parties use, if applicable? | |  | Physical Security | Data Centers |
| Does your product have configurable user roles and permissions, including Admin and General User roles? Describe how access can be restricted with these permissions. | |  | Platform | User Access |
| Does your platform provide a mechanisms for TRSs to manage encryption keys? If so, please explain the process and limitations. | |  | Platform | Authentication |
| Does your Platform support single sign-on Federation and 2-Factor Authentication? If so, what protocols do you support? | |  | Platform | Authentication |
| Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)? | |  | Platform | Authentication |
| Does the Platform store user login credentials? If yes, what hashing algorithm is used? | |  | Platform | Authentication |
| Do you provide regular usage, performance, or other reports? | |  | Platform | Reporting |
| Do you provide full audit logs of user behavior? | |  | Platform | Reporting |
| Describe how TRS data is imported and exported from the Platform. | |  | Platform | Data |
| Does your platform provide a mechanism to extract all of our data and will it be in an open/standard output for use elsewhere? | |  | Platform | Data |
| Are all files uploaded by TRSs to the Platform scanned for viruses and malware? | |  | Platform | Data |
| How frequently do you perform platform upgrades? Will these upgrades impact use of the applications relevant to TRS? | |  | Platform | Technology |
| How much notice do you provide for any scheduled downtime? | |  | Platform | Technology |
| How is TRS able to get in contact during unscheduled or extended downtime? | |  | Platform | Technology |
| What is your up time to date? | |  | Platform | Technology |
| Are automated penetration tests performed? If so, how often? | |  | Platform | Technology |
| Do you use automated tools for security testing or code review? | |  | Platform | Technology |
| Do you offer API access? If so, what form do the APIs take? | |  | Platform | Technology |
| Is there an information security policy in place that has been approved by management and communicated to all employees? | |  | Policies | Information Security |
| Is there a security incident management process in place? Please describe. | |  | Policies | Information Security |
| How frequently are your information security policies reviewed? | |  | Policies | Information Security |
| Is there a formal process for reporting and responding to privacy complaints or privacy incidents? Please describe. | |  | Policies | Privacy |
| Is there any disciplinary action protocol for non-compliance with security policies? Please describe in detail. | |  | Policies | Training |
| What training does your development and testing teams receive specific to application security? | |  | Policies | Training |
| What third-party audits are regularly performed? | |  | Security Infrastructure | Audits |
| Does your organization run intrusion detection or intrusion protection on the network? | |  | Security Infrastructure | Network Security |
| Does your company use firewalls to restrict traffic into and out of your network at strategic points? | |  | Security Infrastructure | Network Security |
| How often does your organization update firewall rules/policies? | |  | Security Infrastructure | Network Security |
| What cyber forensic capabilities exist? | |  | Security Infrastructure | Network Security |
| How are your SSL/TLS private keys protected on your web servers? | |  | Security Infrastructure | Network Security |
| Does your organization outsource any operations to third parties? If yes, please describe the operations being outsourced. | |  | Security Infrastructure | Third Parties |
| What access to our organizational data will third parties have? | |  | Security Infrastructure | Third Parties |
| Does your business operate a VPN that allows remote access? | |  | Security Infrastructure | Identity & Access Management |
| Do you provide to tenants user access to data, applications, infrastructure systems and network components upon request? | |  | Security Infrastructure | Identity & Access Management |
| Do you restrict, log, and monitor all access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? | |  | Security Infrastructure | Identity & Access Management |
| Are controls in place to ensure that access to application, programs or object source code is restricted to authorized personnel only? | |  | Security Infrastructure | Identity & Access Management |
| Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? | |  | Security Infrastructure | Identity & Access Management |
| Does your product allow TRS to define the password complexity and lockout threshold? | |  | Security Infrastructure | Identity & Access Management |
| What level of technical support is included in your license agreements? What team members will be available to assist our company with technical support? | |  | Support | Technical Support |
| Is there a 24x7x365 line available for clients to report security incidents? | |  | Support | Technical Support |
| What methods do you use to inform TRS of vulnerabilities? | |  | Vulnerabilities | Communication |
| Are applications scanned for vulnerabilities prior to release? | |  | Vulnerabilities | Scanning |
| Describe or provide reference to how you monitor for and protect against common web application security vulnerabilities(e.g., Injection flaws, XSS, Broken authentication, etc) | |  | Vulnerability | Scanning |
| Do you have an easily discoverable way for external parties to report security vulnerabilities? | |  | Vulnerabilities | Communication |
| Additional comments: |  | | | |

**For TRS Internal Use Only**

**Information Security**

Approved:  Rejected

Comments:

|  |
| --- |
|  |

|  |
| --- |
|  |

Reviewed by:

\*If rejected, executive level approval is required.

**For the Executive Director/Chief Operations and Administration Officer Only**

Approved:  Rejected

Business Justification (If rejected by Information Security Department):

|  |
| --- |
|  |

|  |
| --- |
|  |

Sign:

(Executive approval only)