1. **General Information**

|  |
| --- |
| **Service/Software/System Description** |
| **Response Date** |  |
| **Vendor/Company Name** |  |
| **Name of Product/Service** |  |
| **Short Description of Product/Service** |  |
| **Vendor Contact** |  |
| **Information Processed or Stored**(General description of information including sensitive data elements) |  |

**B. Security Practices**

| **Question** | **Y/N/NA** | **Comments** | **Document/URL** |
| --- | --- | --- | --- |
| **1.0 SECURITY CERTIFICATION** |
| **1.1** | Can the vendor provide a formal security certification, such as an EDUCASE HECVAT or SOC 2 Type II report (and for all sub-service providers)? (If so, please provide all documentation.) |  |  |  |
| **1.2** | Can the vendor provide a copy of information security policies and procedures?(If so, please provide all documentation.) |  |  |  |
| **If the answer to 1.1 is YES, complete ONLY sections 2.0, 3.0, 4.0 and 5.0 below.****If the answer to 1.1 is NO, complete ALL remaining sections.** |
| **2.0 DATA LOCATION AND OWNERSHIP** |
| **2.1** | Does the service provider outsource hosting of their application and data storage servers to a third-party? (If so please provide name of the provider) |  |  |  |
| **2.2** | Will any data be physically stored outside of USA? |  |  |  |
| **2.3** | Does the university have exclusive ownership of their data? The service provider should have a limited, revocable, non-transferable, non-sublicensable, license to use university’s data solely for the limited purpose of providing services. |  |  |  |
| **3.0 TERMINATION OF SERVICES** |
| **3.1** | Are there written provisions for the timely transfer and format of data from the service provider to the university upon any termination of the service agreement? |  |  |  |
| **3.2** | Are there written provisions for the timely transfer and format of data from the service provider in the eventuality that the service provider is unable to continue providing the contracted service? |  |  |  |
| **4.0 USER AUTHENTICATION** |  |  |  |
| **4.1** | Can users of the hosted service be authenticated by university systems? |  |  |  |
| **4.2** | If users are authenticated by the hosting service provider: |  |  |  |
|  | **4.2.1** | Will user IDs assigned by the service provider match university user ids? |  |  |  |
| **4.2.2** | Will each user have a unique user id? |  |  |  |
| **4.2.3** | Can the service provider's system be configured to require strong passwords?  |  |  |  |
| **4.2.4** | Can university dictate password criteria as needed to ensure compliance with university security standards? |  |  |  |
| **4.2.5** | Does the service provider provide a function to enable users to change their own password securely? |  |  |  |
| **4.2.6** | Can the service provider's system be configured to support multifactor authentication?  |  |  |  |
| **4.2.7** | Can accounts be locked after a university defined number of unsuccessful login attempts? |  |  |  |
| **4.2.8** | Can the service provider's system terminate a user’s session after a defined period of inactivity (requiring user to re-authenticate)? |  |  |  |
| **4.2.9** | Does the hosted service provide a logout on-demand option? |  |  |  |
| **4.2.10** | Are passwords encrypted during network transit? |  |  |  |
| **4.2.11** | Are passwords encrypted in storage? |  |  |  |
| **4.2.12** | Are all attempted and successful logins logged, including date/time, user id, source network address, and are logs maintained for at least one year? |  |  |  |
|  |  | **a.** | Are authentication logs available to the university either raw or by on-demand/user-scheduled reports?  |  |  |  |
|  |  | **b.** | Are logs of authentication changes maintained and made available to the university? |  |  |  |
| **5.0 USER AUTHORIZATION** |
| **5.1** | Will users be authorized by a university based system (LDAP, NDS, AD, PeopleSoft roles)? |  |  |  |
| **5.2** | If user authorization is provided by the service provider's system: |  |  |  |
|  | **5.2.1** | Will user access be managed by the university? |  |  |  |
| **5.2.2** | Does the service provider’s system offer the ability to restrict access within the application based on roles assigned to authorized users? |  |  |  |
| **5.2.3** | Will the service provider's system provide easy to read security reports that identify users and their access levels for periodic review? |  |  |  |
| **5.2.4** | Can the authorization process be configured to automatically disable user accounts or access privileges after a defined period of non-use since the last valid login? |  |  |  |
| **5.2.5** | Are changes to user authorizations logged and made available to the university? |  |  |  |
| **5.3** | Can the service provider’s security controls detect and report unauthorized access attempts? |  |  |  |
| **Complete sections 6-10 only if the answer to 1.1 is ‘NO’** |
| **6.0 DATA SECURITY** |
| **6.1** | Can university data residing on service provider’s systems be encrypted? |  |  |  |
| **6.2** | Is all network transfer of university data encrypted when in transit using TLS 1.2 or higher? |  |  |  |
| **6.3** | Is all physical transfer of university data encrypted (e.g. backups to tape, disk, DVD)? |  |  |  |
| **6.4** | Will any university data be stored, temporarily or otherwise, on end-user workstations, portable devices, or removable media by the service provider?  |  |  |  |
|  | **6.4.1** | If so, will the stored data be encrypted using a strong encryption methodology? |  |  |  |
| **6.5** | If encryption is used, are there procedures for key management (generation, distribution, storage, use, destruction, and archiving)? |  |  |  |
| **6.6** | Will the service provider's developers and systems administration staff who have access to university data, have unique account IDs assigned to them?  |  |  |  |
| **6.7** | Are the duties of the service provider’s technical staff separated to ensure least privilege and individual accountability? |  |  |  |
| **6.8**  | Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? |  |  |  |
| **6.9** | Is the activity of the service provider's technical staff logged when performing system maintenance? |  |  |  |
|  | **6.9.1** | If so, are activity logs maintained for at least one year? |  |  |  |
| **6.10** | Is user-level access to university data logged, monitored, and possible security violations investigated? |  |  |  |
|  | **6.10.1** | Can this log data be made available to university? |  |  |  |
| **6.10.2** | Does this log data specify the data element or data record accessed and the action taken upon the data (e.g. View, Modify, Delete)? |  |  |  |
| **6.10.3** | Can the log data support after-the-fact investigations detailing who, when, and how data or systems were accessed? |  |  |  |
| **6.10.4** | Will the service provider's system provide easy to read access audit reports for periodic review? |  |  |  |
| **6.10.5** | Will access to the audit reports be logged and strictly controlled? |  |  |  |
| **7.0 OPERATIONAL CONTROLS** |
| **7.1** | Has the service provider taken measures to ensure the physical security of the data center(s) in which the application and data storage servers are housed, specifically addressing access controlled and audited entry ways, temperature monitoring and control, fire prevention and suppression, and use of a backup power source? |  |  |  |
| **7.2** | If the service provider is currently providing hosting services for other clients, is multi-client access effectively controlled to ensure users are restricted to only the data they are authorized to access? |  |  |  |
| **7.3** | Does the service provider maintain and apply host security configuration standards on their servers and verify them whenever changes are made? |  |  |  |
| **7.4** | Does the service provider have and exercise a process to maintain current patch levels of software running on their systems?  |  |  |  |
| **7.5** | Does the service provider implement anti-malware controls on servers? |  |  |  |
| **7.6** | Are network vulnerability scans routinely performed with critical and high security vulnerabilities resolved within 14 days? |  |  |  |
| **7.7** | Is an intrusion detections system in place to monitor the network of suspicious activity? |  |  |  |
| **7.8** | Are system logs being forwarded to a remote log server and monitored for security events? |  |  |  |
| **7.9** | Does the service provider practice effective electronic data destruction procedures when hardware is recycled for repair or removed for disposal? |  |  |  |
| **7.9.1** | If the service provider outsources information destruction services, is the outsourced destruction service a National Association of Information Destruction (NAID) Certified Operation? |  |  |  |
| **7.10** | Is a process in place to purge old records from service provider systems? |  |  |  |
| **7.11** | Does the service provider have a full time security function with specific responsibility to monitor and protect the systems on which the university data resides? |  |  |  |
| **7.12** | Does the service provider have an information security audit or evaluation program for their operation? |  |  |  |
| **7.13** | Are employment background checks done for service provider employees, who have access to university data?  |  |  |  |
| **7.14** | Does the service provider have an effective procedure for timely termination of access of their staff and university users (upon notification) who no longer need access to the service provider’s system? |  |  |  |
| **7.15** | Does the service provider employ change control procedures for all software, network devices, and servers to ensure they are properly approved and tested before being released into production? |  |  |  |
| **7.16** | Can service provider staff remotely access systems that store university data? If so, what methods are used? |  |  |  |
| **7.17** | What administrative access will university IT workers have to hosted service on vendor systems? |  |  |  |
| **8.0 SECURITY INCIDENT RESPONSE** |
| **8.1** | Can the service provider comment on or have a documented process for reporting security incidents involving systems used to store/access/modify hosted university data to the university Unit contact or, if appropriate, law enforcement? |  |  |  |
|  | **8.1.1** | Will the vendor participate in the university security incident response process? |  |  |  |
|  | **8.1.2** | Will the vendor share the cost of security incident response? |  |  |  |
| **8.2** | Are security incidents monitored and tracked until resolved? |  |  |  |
| **8.3** | Is incident information and common vulnerabilities or threats shared with owners of interconnected systems or data hosting customers? |  |  |  |
| **8.4** | Will a third party ever have access to the service provider's hardware or systems that store university data? |  |  |  |
| **8.5** | Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise? |  |  |  |
| **8.6** | Does the service provider employ file integrity monitoring (such as Tripwire) or other controls to detect system compromises? |  |  |  |
| **8.7** | In the case of a security breach or unexpected exposure of university data, what are the hosting service provider’s incident response procedures? |  |  |  |
| **8.8** | What is the service provider's process for disclosing to the university any data requests, such as subpoenas or warrants, from a third party? |  |  |  |
| **9.0 RECOVERABILITY** |
| **9.1** | Is the service provider fully aware of the university’s availability and recoverability objectives? |  |  |  |
| **9.2** | Does the service provider have and follow a data and system backup plan commensurate with the university’s recoverability objective? |  |  |  |
| **9.3** | Does the service provider have the capability to recover from a security incident, complete system failure or destruction within the time-frame of the university’s recoverability objective? |  |  |  |
| **10.0 APPLICATION SECURITY** (Complete this section only if the service provided is Software as a Service) |
| **10.1** | Does the software development life-cycle model used by the hosting service provider in the development of their software, incorporate features from any standards based framework models such as OWASP, SANS, or NIST SP800-64? If so, please provide procedure document. |  |  |  |
| **10.2** | Is non-sensitive test data used for development? |  |  |  |
| **10.3** | Do databases containing university data reside on separate dedicated servers (separate from application or web servers)?  |  |  |  |
| **10.4** | Does the service provider have change management policies in place? |  |  |  |
| **10.5** | Are application security scans or source code security reviews performed regularly?  |  |  |  |
| **10.6** | Does the service provider use any application intrusion prevention controls such as a web application firewall?  |  |  |  |
| **11.0 TESTING AND VALIDATION** |
| **11.1** | Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? |  |  |  |
| **11.2** | Does the service provider use a separate test environment to test applications prior to being placed into production?  |  |  |  |
| **11.3** | Does the service provider use live university data for testing? |  |  |  |
| **11.4** | Does the service provider tests its network for security vulnerabilities, including conducting system/network penetration tests? |  |  |  |