**UF Office of Security and Compliance  
SaaS Security Assessment Questionnaire  
for Hosting Service Provider**

|  |  |
| --- | --- |
| **Service/Software/System Description** | |
| **Name of Service** |  |
| **Short Description of Service** |  |

|  |  |  |
| --- | --- | --- |
| **Sponsoring UF Unit** | **Name** | |
| **Unit/Department/Center Name** |  | |
| **Lead Project Administrator** |  | |
| **Lead Technical Contact** |  | |
| **Unit Information Security Administrator (ISA)** |  | |
| **Unit Information Security Manager (ISM)** |  | |
| **Additional UF Contacts**  ***list any additional administrative contacts***  ***or those providing technical support from***  ***other units*** | **Name** | **Unit** |
|  |  |
|  |  |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Hosting Service Provider** | | | |
| **Company Name** |  | | |
| **Contacts** | **Name** | **Phone** | **Email Address** |
| **Administrative Representative** |  |  |  |
| **Technical Contact** |  |  |  |
| **Reference URL** |  | | |
| **Additional Information Needed** |  | | |

**Data Classification Definitions**

UF Restricted Data: Data, which the University of Florida is obligated by policy, law, or legal contract to protect against unauthorized disclosure.

**Security Controls**

|  |  |
| --- | --- |
| **1.0 HIGH LEVEL DESCRIPTION** | |
| **1.1** | Please provide a brief description of the purpose of the system, including how the information will be used. If possible, include a simple diagram of the dataflow and where Restricted Data will be stored. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2.0 AUTHENTICATION** | | | | **YES** | **NO** |
| **2.1** | Will users of the hosted service be authenticated by UF systems? | | |  |  |
| **2.2** | Will users be authenticated by the hosting service provider? | | |  |  |
|  | **2.2.1** | | Will userids assigned by the service provider match UF Gatorlink userids? |  |  |
| **2.2.2** | | Will each user have a unique userid? |  |  |
| **2.2.3** | | Can the service provider's system be configured to require strong passwords? |  |  |
| **2.2.4** | | Can UF dictate password criteria as needed to ensure compliance with UF security standards? |  |  |
| **2.2.5** | | Can the service provider's system be configured to expire user passwords periodically in accordance with UF security standards? |  |  |
| **2.2.6** | | Does the service provider provide a function to enable users to change their own password securely? |  |  |
| **2.2.7** | | Can accounts be locked after a UF defined number of unsuccessful login attempts? |  |  |
| **2.2.8** | | Can the service provider's system deauthenticate users after a UF defined period of inactivity? |  |  |
| **2.2.9** | | Does the hosted service provide a logout on-demand option? |  |  |
| **2.2.10** | | Are passwords entered in a non-display field? |  |  |
| **2.2.11** | | Are passwords encrypted during network transit? |  |  |
| **2.2.12** | | Are passwords encrypted in storage? |  |  |
| **2.2.13** | | Are all attempted and successful logins logged, include date/time, userid, source network address, and are maintained for at least one year? |  |  |
| **3.0 AUTHORIZATION – Logical Access Control** | | | | **YES** | **NO** |
| **3.1** | Will users be authorized by a UF based system (LDAP, NDS, AD, Peoplesoft roles)? | | |  |  |
| **3.2** | Will users be authorized by the hosting service provider's system? | | |  |  |
|  | **3.2.1** | Does the service provider’s system offer the ability to restrict access within the application based on roles assigned to authorized users? | |  |  |
| **3.2.2** | Will the service provider's system provide easy to read security reports that identify users and their access levels for periodic review? | |  |  |
| **3.2.3** | Can the authorization process be configured to automatically disable user accounts or access privileges after a UF defined period of non-use? | |  |  |
| **3.3** | Can the service provider’s security controls detect and report unauthorized access attempts? | | |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **4.0 DATA SECURITY** | | | **YES** | **NO** |
| **4.1** | Is all network transfer of UF Restricted Data encrypted when traversing the service provider's network and the UF network or non-UF networks? | |  |  |
| **4.2** | Is all network transfer of UF Restricted Data encrypted between multiple service providers’ systems (e.g. web and database servers)? | |  |  |
| **4.3** | Is all physical transfer of UF Restricted Data encrypted (e.g. backups to tape, disk, DVD)? | |  |  |
| **4.4** | Will any UF Restricted Data be stored, temporarily or otherwise, be stored on end-user workstations, portable devices, or removable media? | |  |  |
|  | **4.4.1** | If so, will the data be stored encrypted using a strong encryption methodology? |  |  |
| **4.5** | If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? | |  |  |
| **4.6** | Does the service provider's software provide appropriate controls to ensure data integrity (e.g. input validation, checksums of stored data, transaction redo logs)? | |  |  |
| **4.7** | Will the service provider's developers and systems administration staff who have access to UF Restricted Data, have unique account IDs assigned to them? | |  |  |
| **4.8** | Are the duties of the service provider’s technical staff separated to ensure least privilege and individual accountability? | |  |  |
|  | **4.8.1** | Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? |  |  |
| **4.9** | Is the activity of service provider's technical staff logged when performing system maintenance? | |  |  |
|  | **4.9.1** | If so, are activity logs maintained for at least one year? |  |  |
| **4.10** | Is user-level access to UF Restricted Data logged, monitored, and possible security violations investigated? | |  |  |
|  | **4.10.1** | Can this log data be made available to UF? |  |  |
|  | **4.10.2** | Does this log data specify the data element or data record accessed and the action taken upon the data (e.g. View, Modify, Delete)? |  |  |
| **4.10.3** | Can the log data support after-the-fact investigations detailing who, when, and how data or systems were accessed? |  |  |
| **4.10.4** | Will the service provider's system provide easy to read access audit reports for periodic review? |  |  |
| **4.10.5** | Will access to the audit reports be logged and strictly controlled? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.0 RECOVERABILITY** | | **YES** | **NO** |
| **5.1** | Is the service provider fully aware of the UF Unit’s recoverability objectives? |  |  |
| **5.2** | Does the service provider have and follow a data and system backup plan commensurate with the UF Unit’s recoverability objective? |  |  |
| **5.3** | Does the service provider have an adequate hardware maintenance contract or hot spare inventory to meet the sponsoring UF Unit’s recoverability objective after a hardware failure? |  |  |
| **5.4** | Does the service provider have the capability to execute a recovery from a security incident, complete system failure or destruction within the time-frame of the UF Unit’s recoverability objective? |  |  |
| **5.5** | To what extent does the hosting service provider ensure system availability consistent with the UF Unit’s recoverability objectives? (e.g. backup power systems, redundant network paths, use of virtual machines, etc) | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6.0 OPERATIONAL CONTROLS** | | | **YES** | **NO** |
| **6.1** | Does the service provider outsource hosting of their application and data storage servers to a third-party? | |  |  |
| **6.2** | 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? | |  |  |
| **6.3** | 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? | |  |  |
| **6.4** | Does the service provider maintain and apply host security standards on their servers and verify them whenever changes in configuration are introduced into the system? | |  |  |
| **6.5** | Does the service provider have and exercise a process to maintain current patch levels of software running on their systems? | |  |  |
| **6.6** | Does the service provider implement anti-malware controls on servers? | |  |  |
| **6.7** | Does the service provider practice effective electronic data destruction procedures when hardware is recycled for repair or removed for disposal? | |  |  |
| **8.6.1** | If the service provider outsources information destruction services, is the outsourced destruction service a NAID Certified Operation?  see: http://www.naidonline.org/certified\_members.html |  |  |
| **8.6.2** | If the service provider outsources information destruction services, please specify the name and address of the outsourced vendor: | | |
| **6.8** | What process will be provided to purge old records from service provider systems? | | | |
| **6.9** | Does the service provider have an information security audit or evaluation program for their operation? | |  |  |
| **6.10** | What methods are used to ensure the expertise of service provider employees who have access to UF Restricted Data? | | | |
| **6.11** | What methods are used to ensure that service provider employees, who have access to UF Restricted Data, have been properly vetted? (e.g. law enforcement background checks) | | | |
| **6.12** | Does the service provider have an effective procedure for timely termination of access of their staff and UF users (upon notification) who no longer need access to the service provider’s system? | |  |  |
| **6.13** | What methods are used by service provider staff for remote access to systems that store UF Restricted Data? | | | |
| **6.14** | What administrative access will UF IT workers have to hosted service on vendor systems? | | | |
| **6.15** | To what extent does the service provider test its software for security vulnerabilities, including conducting software penetration tests? | | | |
| **6.16** | Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **7.0 INCIDENT RESPONSE** | | **YES** | **NO** |
| **7.1** | Does the service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted UF data to the UF Unit contact or, if appropriate, law enforcement? |  |  |
| **7.2** | Are security incidents monitored and tracked until resolved? |  |  |
| **7.3** | Is incident information and common vulnerabilities or threats shared with owners of interconnected systems or data hosting customers? |  |  |
| **7.4** | Will a third party ever have access to the service provider's hardware or systems that store UF Restricted Data? |  |  |
| **7.5** | Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise? |  |  |
| **7.6** | What process does the service provider have in place to identify security breaches on vendor managed systems (e.g. file integrity checks)? | | |
| **7.7** | In the case of a security breach or unexpected exposure of UF Restricted Data, what are the hosting service provider’s incident response procedures? | | |
| **7.8** | What is the service provider's process for disclosing to UF any data requests, such as subpoenas or warrants, from a third party? | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8.0 APPLICATION SECURITY** | | | **YES** | **NO** |
| **8.1** | 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 (e.g. TSP-Secure, SAMM, Microsoft SDL, OWASP, NIST SP800-64 rev 2, )? If so, please specify. | |  |  |
|  | **8.1.1** | Are security components identified and represented during each phase of the software development life -cycle? |  |  |
| **8.2** | Does the service provider have change management policies in place? | |  |  |
|  | **8.2.1** | Is a pre-determined maintenance window used to apply changes? |  |  |
| **8.2.2** | How much lead-time will the service provider give UF of upcoming changes? | | |
|  | **8.2.3** | How are customers notified of changes? | | |
|  | **8.2.4** | Does the service provider have a process to test their software for anomalies when new operating system patches are applied? |  |  |
|  | **8.2.5** | Has a technical and/or security evaluation been completed or conducted when a significant change occurred? |  |  |
| **8.3** | Are source code audits performed regularly? | |  |  |
|  | **8.3.1** | Are source code audits performed by someone other than the person or team that wrote the code? |  |  |
| **8.4** | Is access to the service provider's application restricted to encrypted channels (e.g. https)? | |  |  |
| **8.5** | Describe the session management processes used by the hosted service's applications. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **9.0 TESTING AND VALIDATION** | | | **YES** | **NO** |
| **9.1** | Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? | |  |  |
| **9.2** | Can the hosting service provider make available a test evaluation instance of their service or application that can be used by UF IT security staff to validate the information security assertions made by the vendor? | |  |  |
| **9.2.1** | Can the test evaluation instance include access at both the user-level interface and management-level interface? |  |  |