|  |  |
| --- | --- |
| **Department:****Date Completed:** | **University Contact:** |
| **Vendor/Service Provider Name:** | **Vendor/Provider Contact:** |
| **Vendor Service Relationship:** |  |

|  |
| --- |
| **Please identify any regulation(s) that the data accessed, viewed, stored or transmitted by vendor may be subject to. Mark all that apply.** |
| HIPAA \_\_\_\_ FERPA \_\_\_\_ PCI \_\_\_\_ HB5 (Ky Privacy)\_\_\_\_ Export Control\_\_\_\_ Other\_\_\_  |

|  |
| --- |
| **Departmental Worksheet – Part I****Guidelines for departmental consideration – as applicable to the service provided** |
| **Vendor Service Level Agreements (SLA), Contract Language and Documentation** |
| **Question** | **Yes**  | **No** | **Comments** |
| 1. The SLA/contract addresses uptime as well as downtime guarantees that include maintenance parameters. For example, defined preventative maintenance periods.
 |  |  |  |
| 1. The SLA/contract includes performance parameters.
 |  |  |  |
| 1. The SLA/contract includes support/availability and response times.
 |  |  |  |
| 1. The SLA/contract language defines proper destruction processes to ensure that when the contract is over the data is properly returned or destroyed per any regulations or University requirements.
 |  |  |  |
| 1. The SLA/contract includes data security responsibilities and breach notification parameters, including applicable regulation language (i.e., PCI, Kentucky House Bill 5, BAA).
 |  |  |  |
| **Relationship Management** |  |  |  |
| **Question** | **Yes**  | **No** | **Comments** |
| 1. Termination terms and or potential service charges have been addressed.
 |  |  |  |
| 1. All costs including fees, ongoing costs, and rate of inflation caps for long term agreements are included in the contract.
 |  |  |  |
| 1. Details regarding functionality of the services including expectations and notification of changes are addressed.
 |  |  |  |
| 1. Vendor experience, viability, and impact of mergers and acquisitions have been discussed/documented.
 |  |  |  |
| 1. Details regarding outsourcing have been reviewed to include identification of all other 3rd parties that may handle University data. This should include language regarding 3rd party agreements, retention of responsibility, 3rd party responsibility for security of data and a current list of all identified 3rd parties.
 |  |  |  |
| 1. The contract includes details regarding the disclosure of data. This would include details regarding non-disclosure, legal requests and notification to the University. Notifications should also include the expectations for timing of said notification.
 |  |  |  |
| 1. Will this service/product require interfacing with university systems such as PeopleSoft? If so, list all data elements that will be involved (e.g., name, ID, GPA, DOB, phone, etc.).
 |  |  |  |

|  |  |
| --- | --- |
| **Department:** | **University Contact:** |
| **Vendor/Service Provider:** | **Vendor/Provider Contact:** |
| **Vendor Service Relationship:** |  |

**Assessment Completed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Completion date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |
| --- |
| **Vendor Worksheet – Part II****Questions for the vendor – as applicable to the service provided** |
| **Data Management, Infrastructure and Data Security – controls, physical security and continuity** |
| **Question** | **Yes**  | **No** | **Comments** |
| 1. Define the companies view on roles and responsibilities regarding data management and University ownership.
 |  |  |  |
| 1. Will you be able to provide a clear exit strategy that includes data return, format and proper destruction/sanitization? Please describe.
 |  |  |  |
| 1. Will you allow the University to audit, and to see reports or certifications, assessments and scan results preformed on systems, network?
 |  |  |  |
| 1. Please provided required or industry standard certification documentation as pertinent to the regulations of the data involved (i.e., PCI Attestation, HIPAA compliance, FISM, SOC3, ISO27001, etc.)
 |  |  |  |
| 1. Has your company completed the Cloud Security Alliance (CSA) self-assessment or is the company STAR certified?
 |  |  |  |
| 1. Has the company undergone a SSAE 16 audit? Is the company SOC certified? Documentation provided.
 |  |  |  |
| 1. Will university data be encrypted both during storage **and** transmission. This includes all versions - backups. Please explain.
 |  |  |  |
| 1. Will University data be stored within the United States? Storage locations have been identify and are in compliance with applicable regulations or contracts. This includes data back-up, and cloud providers.
 |  |  |  |
| 1. Is two-factor authentication utilized? Please explain your authentication methods. This should include the details of how these methods are used based on employee roles including administrators that may have access to University data.
 |  |  |  |
| 1. Access control policies require approvals, granting of access based on the principle of “least privilege” and changing of default passwords.
 |  |  |  |
| 1. A formalized incident response plan which includes defined breach responsibility, process, format, and timing expectations is in place.
 |  |  |  |
| 1. Describe your firewall and IDS usage and audit logs.
 |  |  |  |
| 1. Regular network penetration and vulnerability testing is conducted. Current results (or attestations) have been provided and results ongoing throughout the terms of this agreement will be provided if requested.
 |  |  |  |
| 1. Procedures in place to obtain, assess, rank and ensure timely patching of system and device vulnerabilities.
 |  |  |  |
| 1. Procedures in place to ensure anti-virus is running and up-to-date on all devices included in the service provided to the University.
 |  |  |  |
| 1. Dataflow documentation depicting all points in the transmission and storage of University data has been provided.
 |  |  |  |
| 1. Information Security Policy and Procedures are available and implemented addressing areas such as user responsibility, network and data security, incident response and system development?
 |  |  |  |
| 18. Business Continuity and DR plans which include  continuous service, data recovery, security and  backups are in place, tested regularly and updated. |  |  |  |
| 19. Employee management policies and procedures  exist including requirements for background checks, awareness training and personnel change  notification. |  |  |  |
| 20. Will your company consent to allow the  University to perform its own inspection including  the right to review the physical security controls,  infrastructure and other inspection documentation? |  |  |  |
| 21. Does your company utilize a formal, industry  standard process for secure development, testing  and coding of software. |  |  |  |
| 22. The preferred method for systematically transferring  University data securely utilizes PGP. Can your  systems support this process? If not, please  explain the method for ensuring data encryption  both during transfer and upon receipt (at rest). |  |  |  |
| 23. Will your service require interfacing or authentication with university systems? Explain  |  |  |  |
| 24. Are you in compliance with the EU  General Data Protection Regulation (GDPR)? Please explain what steps have been taken to comply with  the regulation. |  |  |  |
| 25. Does your company have Cyberliability Insurance?  If so, please provide your limits. |  |  |  |
| 26. Has your company experienced a data breach within  the last 3 years? If so, please describe the nature of  the occurrence, length of time and resolution. |  |  |  |
| 27. To your knowledge, has any 3rd party contractor  involved in the service provided to us, experienced a data breach? If so, please identify the  service provided, the nature and resolution of the  breach. |  |  |  |
| **Relationship Management** |
| **Question** | **Yes**  | **No** | **Comments** |
| 1. Please provide details regarding any outsourcing. Include identification of all other third parties that may handle University data.
 |  |  |  |
| 1. How do you ensure the security controls of third party vendors that may handle or access University data?
 |  |  |  |
| 1. Please provide details on your availability and maintenance schedule and process.
 |  |  |  |

**For Services that include a mobile application**

|  |
| --- |
| **Mobile App Security – to be used if a mobile application is included in current or future services** |
| **Question** | **Yes**  | **No** | **Comments** |
| 1. Does your company currently offer or plan to offer in the future mobile app solutions related to the services you are currently proposing?
 |  |  |  |
| 1. If so, please explain security previsions specific to this service. This should include data transmission, storage, and backup details.
 |  |  |  |
| 1. Has the mobile application been reviewed by a third party? Please include details regarding application development controls including 3rd party application code reviews by external companies and the frequency of the review process.
 |  |  |  |
| 1. Does the company’s contract include details regarding testing procedures to ensure that device considerations are being addressed?
 |  |  |  |
| 1. Has the mobile application been designed based on industry standard security guidelines provided by both NIST and OWASP? The scope for these would include server side controls, transport layer protection, data leakage, authorization / authentication controls, broken cryptography, client side injection, session handling and binary protections.
 |  |  |  |
| 1. Does the company have procedures to address handling public user reviews and complaints regarding the mobile application?
 |  |  |  |
| 1. Does the company’s mobile application include layered security controls for the app? This would include the use of internal security controls to protect stored data for example a pin number to gain access to the application itself that would go beyond access to the device’s OS.
 |  |  |  |
| 1. Does the company’s mobile application include a time out feature to ensure data protection?
 |  |  |  |
| 1. How long has the company made this mobile application available to the general public? How many updates has it received since its initial roll out?
 |  |  |  |
| 1. Does the company have procedures regarding the turn-around time for bug reports?
 |  |  |  |
| 1. Does the company’s mobile application allow for external storage? If so what security controls are included to protect this data?
 |  |  |  |
| 1. Can the company’s mobile application be accessed by other applications? If so what security controls are included to protect this data?
 |  |  |  |