**Detailed ASP Vendor Risk Assessment 1**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ASP Vendor Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unit

With respect to the ASP vendor the following shall be assessed after giving consideration to the magnitude of the ASP service being considered using the “High Level Risk Assessment Form”.

|  |  | Impact on Risk |
| --- | --- | --- |
| Considerations: | Y/N | High | Med. | Low |
|  |  |  |  |  |
| Does the Vendor have and adhere to a written and comprehensive set of information and security policy documents dealing with the protection of information and assets?  |  |  |  |  |
| Have these documents been reviewed by the University? |  |  |  |  |
| Does the Vendor have a senior level person responsible for the initiation and implementation of information security?  |  |  |  |  |
| Have we spoken with this senior security official and confirmed their role? |  |  |  |  |
| Will known incidents of a breach in information, software, or physical security be reported to the University? |  |  |  |  |
| Are third party service providers utilized to provide any aspect of the service? Provide a description of all pertinent third party services used to provide the service to the University. |  |  |  |  |
| Does the Vendor have in place asset control policies and procedures that assure their right of ownership, management, and licensing of information assets, software assets, and physical assets used to provide service to the University? |  |  |  |  |
| Are there procedures and controls associated with vendor disposal of server and primary and secondary storage devices? |  |  |  |  |
| Are there procedures and controls that assure full data backup? |  |  |  |  |
| Are full data backup’s maintained onsite? |  |  |  |  |
| Are full data backup’s maintained offsite? |  |  |  |  |
| Are backups maintained offsite by a third party?  |  |  |  |  |
| Does the vendor have a contract(s) in place with the third party vendor with respect to their responsibilities and access to the backups? |  |  |  |  |
| Are there procedures and controls to ensure aged backups are securely destroyed? |  |  |  |  |
| Is the vendor insured for losses of information, software, and physical assets? (Provide list of type and levels of insurance carried.) |  |  |  |  |
| Does the Vendor have policies, procedures, and controls in place to ensure that background checks are completed on those individuals that will be administering the systems used by the University? |  |  |  |  |
| Are employee reference checks completed? |  |  |  |  |
| Are employee criminal background checks completed? |  |  |  |  |
| Are employees required to sign and adhere to a non-disclosure or confidentiality agreement? |  |  |  |  |
| Are employees bonded? |  |  |  |  |
| At the location where the work of the University will be conducted by the Vendor are the Vendor’s facilities physically protected from unauthorized access?  |  |  |  |  |
| Are all accesses logged? |  |  |  |  |
| Are all logs protected and regularly reviewed? |  |  |  |  |
| Are there documented disaster recovery plans? |  |  |  |  |
| Do staff participate regularly in testing these disaster recovery plans? |  |  |  |  |
| Does the Vendor have documented policies and procedures that are adhered to for the management and operation of all information processing facilities?  |  |  |  |  |
| Do these policies and procedures include appropriate operating instructions, change control, incident response procedures, segregation of duties, and environments for development, testing, staging and production versions of the software? |  |  |  |  |
| Does the Vendor own it’s own facilities where the work of the University is being conducted? |  |  |  |  |
| Are the Vendor facilities adequately protected from natural disasters like flood, fire, tornado, ice storms?  |  |  |  |  |
| Are data facilities monitored? Are these monitoring systems regularly review and tested? |  |  |  |  |
| Are environmental protection systems in place for the data centre to monitor for and protect against fire, loss of air conditioning, loss of commercial power, humidity?  |  |  |  |  |
| Are these systems tested regularly, and if so at what frequency? |  |  |  |  |
| Are failover systems, hot swap equipment replacements and or hot sites employed to ensure continuous availability of the service and access to its data and information by the University? |  |  |  |  |
| Is any of the equipment used in handling the University’s data or information housed with a third party? |  |  |  |  |
| Is any of the equipment used in handling the University’s data or information owned with a third party? (Provide details) |  |  |  |  |
| Can this equipment be monitored and maintained remotely?  |  |  |  |  |
| Is the connection to remote equipment protected from electronic intrusion? |  |  |  |  |
| Are safeguards in place to prevent unauthorized interception or damage to the network, power, or telecommunications cabling of the vendor?  |  |  |  |  |
| Is network cabling, monitors and wireless systems adequately shielded to prevent compromise of network security? |  |  |  |  |
| When equipment is replaced by the vendor is there a policy and standard process for identifying and removing all data and information? |  |  |  |  |
| Does the Vendor have a projection of future capacity requirements and are these being planned for?  |  |  |  |  |
| Is system capacity, performance, and response time monitored for the application service the University will be using? |  |  |  |  |
| Is antivirus software deployed and maintained current on the application service, and servers the University will be using? |  |  |  |  |
| Are remote users to the vendors systems virus protected? |  |  |  |  |
| Are new systems being contemplated and if so does the vendor have established and documented test results that must be met prior to acceptance?  |  |  |  |  |
| Does the Vendor have procedures for restarting and recovering systems? |  |  |  |  |
| What priority does the system the University uses have in this restart and recovery procedure?  |  |  |  |  |
| Are major system modifications planned for the next 12 months? (Provide information on each planned modification.) |  |  |  |  |
| Does the Vendor have policies and procedures for ensuring the protection of data in transit?  |  |  |  |  |
| Does that protection extend to any offsite storage location transmissions of the Vendor?  |  |  |  |  |
| Are transactions authenticated with non-repudiation? |  |  |  |  |
| Are access codes encrypted while in transit and in storage? |  |  |  |  |
| Are electronic transactions protected during transmission? |  |  |  |  |
| Are periodic reviews of router and firewall logs performed? |  |  |  |  |
| Does the Vendor have policies and procedures that are adhered to and ensure only authorized staff of the University have access to the service, data, and information of the University? |  |  |  |  |
| Does the University have the ability to review all access authorizations granted? |  |  |  |  |
| Can the University review all accesses gained to our application and data by vendor developers and vendor support personnel? |  |  |  |  |
| What is the minimum length of a password?  |  |  |  |  |
| Do passwords expire? (Please indicate how often.) |  |  |  |  |
| Does the Vendor have procedures for a password reset request? (Please attach details) |  |  |  |  |
| Are inactive users automatically logged off after a set period of time? (Provide details on length of time to log out.) |  |  |  |  |
| Can the University review all vendor authorized external access connections to the University’s service, data, and information?  |  |  |  |  |
| Are controls in place to prevent unauthorized changes to the application, data, or information? |  |  |  |  |
| Does the Vendor have established policies and procedures which are monitored for adherence to ensure compliance with all legal and regulatory agencies? |  |  |  |  |
| Are there procedures in place to ensure compliance with Saskatchewan Privacy Law, with Canadian Privacy law? |  |  |  |  |
| Are there any domestic or foreign laws, regulations or policies that the vendor comes under that could prevent the vendor from meeting University needs with respect to access and use of information, software, and or physical assets? |  |  |  |  |
| Is the Vendor subject to the United States Patriot Act?  |  |  |  |  |
| Does this have implications for the University with respect to its data and information stored with the Vendor? |  |  |  |  |
| Is the Vendor required to retain all personal information irrespective of the University’s instruction to destroy all such personal information? |  |  |  |  |
| Does the Vendor’s software exist in escrow? |  |  |  |  |
| Are there rights the University will have to access and use any escrowed software? |  |  |  |  |

Assessment Completed By: Authorization to Implement:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Date

1. The expectations, questions and ideas contained within this Detailed Vendor Assessment are drawn from BITS Financial Services Roundtable, “BITS IT Service Provider Expectations Matrix, January 2004”, BITS, Washington, DC, copyright 2004.