**Cloud Solution Overview**

*This section is to be completed by the designated ITSD Project lead. The information will be referenced by the cloud solution provider in completing the questionnaire.*

**Solution Provider Information**

Solution Name: Click or tap here to enter text.

Contact Name: Click or tap here to enter text.

Vendor Name: Click or tap here to enter text.

Email Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Website: Click or tap here to enter text.

**Project Lead Information**

Project Lead Name: Click or tap here to enter text.

Department/Division Represented: Click or tap here to enter text.

Email Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

**Authentication Requirements:** Click or tap here to enter text.

**Legal, regulatory, or industry compliance requirements:** Click or tap here to enter text.

**Cloud Provider Questionnaire**

*This section is to be completed by the cloud solution provider.*

1. **Indicate other Federal, State, or Local government agencies that utilize the cloud application or service. Provide the year the agency started using the service. If available, provide agency contact information including name, title, email and phone.**

Click or tap here to enter text.

1. **Indicate the extent to which third parties are responsible for providing the different logical layers of the solution’s infrastructure. Where multiple parties share responsibility for securing, configuring, managing, or obtaining certification of compliance for a given logical layer, indicate all parties that share responsibility.**

|  |  |
| --- | --- |
| Layer Description | Responsible Parties and Role |
| Application | Click or tap here to enter text. |
| Database  | Click or tap here to enter text. |
| Runtime | Click or tap here to enter text. |
| Middleware | Click or tap here to enter text. |
| Operating System | Click or tap here to enter text. |
| Virtualization | Click or tap here to enter text. |
| Server | Click or tap here to enter text. |
| Storage | Click or tap here to enter text. |
| Network | Click or tap here to enter text. |
| Physical Security | Click or tap here to enter text. |

1. **Indicate if all information managed by the application will remain solely within the continental United States and will not be stored in any manner outside the continental United States.**

[ ] Yes, all information will remain within the continental United States

[ ] No, all or some information may not remain within the continental United States

1. **Indicate if the application and its supporting infrastructure will be managed and maintained solely by citizens of the United States and from locations within the continental United States.**

[ ] Yes, the application and its supporting infrastructure will be managed and maintained solely by citizens of the United States and from locations within the continental United States

[ ] No, the application and its supporting infrastructure may be managed and maintained by other than citizens of the United States and/or from locations outside the continental United States

1. **Indicate the application or service’s Service Level Agreement (i.e. 99.95%) with the exception of scheduled maintenance.**

Click or tap here to enter text.

1. **Indicate the scheduled maintenance procedures for the application including:**
	1. The customer notification process including number of days before event and the means of notification Click or tap here to enter text.
	2. The maximum scheduled maintenance outage time Click or tap here to enter text.
	3. The typical day of week, start time, and end time of maintenance processes Click or tap here to enter text.
	4. The frequency of scheduled maintenance Click or tap here to enter text.
2. **Indicate the characteristics of the disaster recovery plan for the application and application infrastructure including:**
3. The circumstances that would trigger activation of the disaster recovery plan Click or tap here to enter text.
4. The frequency of conducting a disaster recovery practice drill to verify the plan’s viability Click or tap here to enter text.
5. The States in which the primary and secondary data centers are located Click or tap here to enter text.
6. The maximum loss of transactional information (in minutes) in the event the disaster recovery plan is activated (recovery point objective)
	1. Best case: Click or tap here to enter text.
	2. Worst case: Click or tap here to enter text.
7. The customer notification process and means of notification in the event the disaster recovery plan is activated Click or tap here to enter text.
8. **Indicate the availability of backups, and/or recovery points should information be lost or corrupted as a result of errors in application processes or upgrade processes.**

Click or tap here to enter text.

1. **Indicate the contractual protections that are in place should the application vendor cease operations.**

Click or tap here to enter text.

1. **If the cloud services are provided by a third party, indicate the contractual protections that are in place if the third party cloud services vendor should cease operations.**

Click or tap here to enter text.

1. **Indicate whether the solution is in compliance with the legal, regulatory, and industry specific requirements listed in section one above. For each compliance requirement, indicate if the compliance is self or independently certified, date of last certification, and if a copy of the attestation / certification can be made available to the State. If no requirements are specified in section one, indicate the extent to which the solution is implemented in compliance with the latest revision of NIST SP800-53. Indicate if the solution has been certified under other recognized standards.**

Click or tap here to enter text.

1. **Indicate the application vendor’s process for responding to legal action by Federal, State, or Local government agencies or private parties requesting access to State information in the custody of the application vendor. Include information on the notification procedures and timeline in effect should this event occur.**

Click or tap here to enter text.

1. **Indicate the application vendor’s security breach notification process including:**
2. The conditions under which the breach notification is triggered Click or tap here to enter text.
3. The means by which the State will be notified of the breach (email, phone, text messaging) Click or tap here to enter text.
4. The maximum timeline from breach discovery to notification: Click or tap here to enter text.
5. The security and audit logs available to the State to assist in ascertaining the scope of the breach Click or tap here to enter text.
6. The availability of funds from the application vendor (breach insurance or other means) to defray costs associated with a breach Click or tap here to enter text.
7. **Indicate if the cloud solution is regularly scanned for vulnerabilities utilizing both static and dynamic scanning method on a periodic basis (quarterly, semi-annually, or annually) and prior to updates to the application. Indicate the process for remediating vulnerabilities found by the scans and the minimum requirements for release of an update or enhancement for production use.**

Click or tap here to enter text.

1. **Indicate if the cloud solution is multi-tenant or single tenant (dedicated).**

Click or tap here to enter text.

1. **Indicate if the cloud solution’s information / data is encrypted at rest.**

Click or tap here to enter text.

1. **Indicate if the cloud solution’s information is encrypted when transmitted, including requiring HTTPS for all web access and encryption of data during application to application communication.**

Click or tap here to enter text.

1. **Indicate if the application provides a native identity, access, and account management feature. If so, indicate if the application provides configuration settings for: This is N/A as it regards Canvas internal authentication which will be unused, per 19.**
2. Password length- 8 characters minimum: Click or tap here to enter text.
3. Password composition (Upper, lower, numeric, special, etc.) Click or tap here to enter text.
4. Password expiration Click or tap here to enter text.
5. Maximum login attempts before lockout Click or tap here to enter text.
6. Lockout time Click or tap here to enter text.
7. Two factor authentication support Click or tap here to enter text.
8. Delegation of account creation, change, and deletion (describe) Click or tap here to enter text.
9. Delegation of feature authorization (describe) Click or tap here to enter text.
10. **If applicable, indicate if the application is capable of integrating with a State managed authentication system, i.e. Active Directory, ADFS, OpenID Connect etc. Indicate the authentication protocols supported by the application or service.**

Click or tap here to enter text.

1. **Indicate the type of interfaces or customizations available to interface the application with applications hosted by the State or hosted by other vendors. Indicate if any specific development tools are required or desirable, i.e. SDKs, libraries, API documentation, etc.**

Click or tap here to enter text.

1. **Indicate if the cloud solution can provide data backup / replication to other cloud service providers or to the State’s Data Center. Include information of the available format(s) of the backup that would make the backup information available to the State.**

Click or tap here to enter text.

1. **Indicate if there is an enterprise pricing model or per account/unit/license available for larger volumes of users.**

Click or tap here to enter text.

1. **Indicate the process for reporting customer issues to the vendor, and issue escalation process. Include information on support response times.**

Click or tap here to enter text.

1. **Indicate any specific workstation requirements including installation of software, browser version(s), supporting software, processor, memory, etc.**

Click or tap here to enter text.