Cloud Computing Security Policy

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy for Cloud Computing.

Purpose

To ensure that the confidentiality, integrity and availability of the Government of Saskatchewan's information is preserved when stored, processed or transmitted by a third party cloud computing provider.

Scope

This policy applies to all cloud computing engagements. All cloud computing engagements must be compliant with this policy.

Context

Cloud computing is defined by NIST as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It is composed of five essential characteristics including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured services. It can be provided at a low-level as hosted infrastructure (IaaS), at a mid-tier level as a hosted platform (PaaS), or at a high level as a software service (SaaS). Cloud providers can use private, public, or hybrid models.

Policy Statements

The cloud services risk-management framework used by the Government of Saskatchewan has the following activities mandated by this policy:

- Step 1: Perform data classification (Statement of Sensitivity);
- Step 2: Perform Threat Risk Assessment on the solution;
- Step 3: Address threats/risks identified by implementing the proper controls;
- Step 4: Continuously monitor and periodically audit systems and services.

Data Classification

All Government of Saskatchewan information under consideration for use in a cloud computing environment must first be classified by the appropriate Information Owner.

- Security controls will be applied based on the Information Classification.
- Any Government of Saskatchewan Data containing Personally Identifiable Information must ensure data at-rest resides in Canada.

Select Security Controls

Security controls for the proposed solution must be appropriate for the level of data classification. Detailed requirements are specified in *Information Protection Security Controls (IPSC) for Classified Data*. At minimum, the security controls provided by Cloud Service Providers (CSP) must implement the following:

1. **Standards**: CSP must ensure that they are compliant with a widely adopted cloud security standard that is acceptable to government:
   a. ISO/IEC 27017, demonstrated via certification with accreditation;
   b. NIST SP 800-53, demonstrated via certification with accreditation; or
   c. Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification.
2. **Compliance**: CSP must ensure it can demonstrate compliance with a cloud security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. CSP must demonstrate compliance with security obligations if they are not covered anywhere else.
3. **Access Control**: CSP must implement an access control policy and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts. CSP must identify and segregate conflicting duties and areas of responsibility (eg. separation of duties). CSP must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts. CSP must enforce a limit of logon attempts and concurrent sessions as well as multi-factor authentication for privileged access.
4. **Passwords:** CSP must enforce password length, complexity, and history for password-based authentication. CSP must support multi-factor authentication to allow the Province to use it. CSP must support single sign-on technologies for authentication.
5. **Awareness:** CSP must ensure that it conducts security awareness and training for employees.
6. **Logging:** CSP must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. CSP must provide online GUI access to logs. CSP must provide the technical capability to forward the logs to the Province. CSP must correlate, monitor, and alert on logs.
7. **Investigations:** CSP must retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed. CSP must provide adequate investigative support to the Province. CSP must support e-discovery and legal holds to meet needs of investigations and judicial requests.
8. **Time:** CSP must ensure that infrastructure is synchronized with Stratum 1 time servers.
9. **Change Control:** CSP must implement change controls in accordance with reasonable industry practices. CSP must test changes to the environment as part of the change management process. CSP must not utilize production data in test environments.
10. **Configuration/Patch Management/Best Practices**: CSP must have an information security policy based on industry best practices. CSP must harden systems and servers using appropriate industry standards. CSP must secure databases using appropriate industry standards and logically isolate and encrypt Province information. CSP must ensure workstations used in management and provisioning are patched and secured with antivirus. CSP must implement physical security according to industry best practices. CSP must remedy vulnerabilities and patches according to criticality. CSP must ensure that applications and programming interfaces are developed according to industry standards.

11. **BCP/DRP:** CSP must have a business continuity plan and a disaster recovery plan that are reviewed and tested annually. CSP must conduct backups using appropriate industry standards. CSP must have incident management and incident response plans that are reviewed and tested annually.
12. **Asset Disposal:** CSP must dispose of assets according to industry best practices. CSP must dispose of information according to industry best practices.
13. **Threat/Risk Assessments**: CSP must conduct threat and risk assessments on new systems or material changes to existing ones. CSP must support the Province in completing Security Threat and Risk Assessments (STRAs).
14. **Security Testing**: CSP must conduct vulnerability scans for new systems and material changes to existing ones. CSP must conduct web app vulnerability scans for new systems and material changes to existing ones. CSP must conduct penetration tests at least annually.
15. **Security Screening:** CSP must screen individuals prior to authorizing access to information systems. CSP must conduct criminal record checks on employees.
16. **Supply Chain**: CSP must ensure suppliers and contractors meet or exceed CSP's own security policies.
17. **Encryption**: CSP must implement encryption of data in transit and at rest for Province information and provide the technical capability to manage encryption keys.
18. **Logical Separation**: CSP must logically isolate the Province's information and segregate Province traffic from other tenants and management traffic. CSP must implement security devices between zones.
19. **Technical Controls**: CSP must implement firewalls and intrusion prevention. CSP must implement application layer firewalls. CSP must enable Province to enable/configure security controls in the tenancy such as firewall, intrusion prevention, antivirus, and encryption (IaaS). CSP must secure remote access according to industry best practices. CSP must implement distributed denial of service attack protection.
20. **Breach Notification**: CSP must notify the Province within 24 hours of a potential or actual breach or incident that may affect the Province's information. CSP must notify the Province of any changes to security policies, procedures or agreements.

Risk Assessment

A risk management process must be used to balance the benefits of cloud computing with the security risks associated with handing over control to a vendor.

As compliance with one of the cloud security standards acceptable to government is one of the required security controls, a simplified risk assessment process of a successful review by TRB and a successful ISB review of the supplier's Statement of Applicability and recent external auditor's report is sufficient.

All findings by TRB and the TRA must be successfully addressed before approval to proceed may be granted.

Monitor Services

Ongoing security compliance monitoring and auditing of the supplier by the Government of Saskatchewan must be included in contracts with cloud computing providers.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.