DDSB Ignite Learning

PROCEDURE

CORPORATE SERVICES

Technology Approval Process (Cloud Services): Privacy and Security Assessment Guide

Adopted under the Privacy Policy

1.0 Objective

1.1 As the digital landscape moves further from on premise hosting, Cloud Services provide financial and production benefits to the Durham District School Board ("DDSB") by reducing costs and increasing production and ease of use. The DDSB recognizes that the financial and production benefits of Cloud Services must be balanced with ensuring security and privacy of information in the custody, or under the control of the DDSB, and be consistent with legislative requirements, including the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 and its regulations, as amended ("MFIPPA"), *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3 and its regulations, as amended ("PHIPA"), and the *Education Act*, R.S.O. 1990, c. E.2 and its regulations, as amended (the "Education Act").

1.2 The objective of the *Technology Approval Procedure (Cloud Services): Privacy and Security Assessment Guide* (this "Procedure") is to assist DDSB employees in assessing and implementing Cloud Services by outlining specific issues that should be raised and considered before Vendor selection is finalized to adequately protect the security and privacy of information in the custody or under the control of the DDSB.

1.3 This Procedure can be used to assist DDSB employees as well as Vendors in responding to Requests for Proposals and evaluating collocation, managed hosting, Cloud and Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Desktop-as-a-Service (DaaS), and Backend-as-a-Service (BaaS) Providers.

1.4 This Procedure is to be interpreted and applied in accordance with the DDSB's commitment to promoting and upholding Indigenous rights and human rights in all its learning and working environments. This includes anti-colonial, anti-discriminatory and anti-racist approaches and actions to provide services and employment that are safe, welcoming, respectful, inclusive, equitable, accessible and free from discrimination and harassment consistent with the DDSB's Indigenous Education Policy, Human Rights, Anti-Discrimination and Anti-Racism Policy, Safe and Respectful Workplace and Harassment Prevention Policy and related procedures.

2.0 Scope

2.1 This Procedure applies to:

2.1.1 All DDSB employees with a responsibility for Cloud Services procurement, assessment, approval, implementation, and management.

2.1.2 All Vendors, Cloud Services Providers and their supply chains that provide Cloud Services to the DDSB.

2.1.3 Outsourced provisions of Cloud Services (e.g., software as a service, platform as a service, cloud hosting).

2.1.4 Outsourced provisions of information technology functions and consulting where personnel are managed by the Cloud Service Provider.

3.0 Applying the Cloud Service Assessment Guide

3.1 When assessing Cloud Services for Vendor selection, there are nine areas to consider, detailed in Appendix A: General, Data Encryption, Access Privileges, Regulatory Compliance, Data Provenance, Data Segregation, Data Recovery, Monitoring and Reporting, and Business Continuity. These nine areas align to areas of security risk associated with Cloud Services.

3.2 When applying this Procedure, ensure each criterion is relevant and necessary to the Cloud Service's use. Additional evaluation assessment guide, questions, and information not set out in this Procedure may be included in a Cloud Services assessment to reflect unique requirements. Similarly, portions of this Procedure may not apply to a particular Cloud Service.

3.3 Not all Vendors or CSPs will be required to pass every piece of assessment guide in order to be selected. Factors, such as the sensitivity of the data stored, will dictate how strict or lenient these assessment guide should be implemented. For example, storage of PI and PHI will require a stricter application of the assessment guide.

3.4 DDSB employees must ensure they work only with trusted Vendors and CSPs that can address Cloud Service security challenges. In moving from using just one Cloud Service to using several Cloud Service from different providers, the DDSB also must manage all these issues across multiple operators, each with different infrastructures, operational policies, and security skills. This complexity of trust requirements drives the need for a ubiquitous, highly reliable method to secure our data as it moves to, from and around the Cloud Service.

4.0 Responsibilities

4.1 **Information Technology Services ("ITS") and Legal Services**

ITS and Legal Services are jointly responsible for the administration of this Procedure.

4.2 **Innovative Education**

4.3 The Innovative Education ("IE") team is responsible for reviewing all Cloud Services requested for approval by education staff that fall under the "Educational" category (used for in-person or online classrooms) to determine the following:

4.3.1 If the technology requested has pedological value;

4.3.2 Privacy considerations that require further review by IT Services;

4.3.3 Whether the technology would be redundant because the DDSB already uses a similar or alternate approved "standard" technology; and

4.3.4 Guidelines concerning how technology will be deployed in classrooms.

Questions relating to requests for Educational Cloud Services approval can be sent to innovative.education@ddsb.ca

5.0 Reference Documents

5.1 **DDSB Policies**
Personnel – Privacy
Purchasing Policy

5.2 **DDSB Procedures**
Technology Approval Process
Personnel – Privacy
Purchasing Procedure
Purchasing Regulation

5.3 **Other Documents**
Education Act, R.S.O. 1990, c. E.2
Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56
Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A

Appendix:

Appendix A: Cloud Service Assessment Guide
Appendix B: Definitions

Effective Date

2023-06-02

Appendix A: Cloud Service Assessment Guide

1. **General Considerations**.

   General considerations include what the Vendor is offering and a summary of some of the basic questions that should be asked.

   a. A detailed description of the DDSB information that the Vendor requires to perform their tasks and an acknowledgement that DDSB is the Information Owner.

   b. Does the CSP have an allowance to audit either the application or network infrastructure? What notice is required to do non-intrusive vs. intrusive scans or other vulnerability assessments?

   c. What allowances does the Vendor provide to access or request any security related configuration files, developed application code, or policy or quality assurance and testing documents?

   d. What internal software/hardware/infrastructure audits does the Vendor perform and what actions do they take upon locating a security issue?

   e. Explain how the Vendor designates a customer contact in the event of a breach or security issue?

   f. Does the Vendor use DDSB Confidential Information for any other purposes, whether metadata (in part) or whole for other services?

   g. Description of scheduled maintenance times and customer notification processes. Any maintenance history provided is helpful.

   h. Explain the Vendor's levels of customer support for your Cloud Services offering beyond knowledge base, FAQs, or message boards. Are there additional costs associated for this support? If so, note those costs.

   i. Define the Vendor's trouble ticket severity levels. How are they assigned and how are they escalated? Is escalation automatic based on a metric or customer initiated?

   j. Service Level Agreement for uptime. Targets should be 99.99% if possible but may vary. For DDSB guidance:

      i. 99.999% uptime translates to 5.39 minutes per year of downtime

      ii. 99.99% uptime translates to less than 53 minutes per year downtime

      iii. 99.9% uptime translates to almost 9 hours per year downtime

      iv. 99.5% uptime translates to almost 44 hours per year downtime

      v. 99% uptime translates to almost 90 hours (87.6 or 3.65 days) per year downtime

   k. Mobile device access capabilities and any security controls for protecting linking to lost or stolen customer mobile devices containing data.

l. Review the Vendor Personnel hire, orientation, and security training process and any non-compete or data/customer confidentiality agreements you have them sign.

2. Data Encryption

Both data in transit and data at rest require encryption to adhere to most governmental regulations. Types of encryption and protocols should be assessed.

a. Data in transit and file uploads or transfers must be secured with encryption protocols. Those protocols utilized should be explained by the Vendor.

b. For data in transit, CSPs should be using Transport Layer Security (TLS 1.2) from an established, reliable and secure independent certificate authority (CA). The TLS 1.2 CA needs its authentication practices audited annually by a trusted third-party auditor. The CA needs its authentication practices audited annually by a trusted third-party auditor.

c. For data in transit, TLS should deliver at minimum 256-bit encryption based on the new 2048-bit global root. And it should require a rigorous authentication process. The certificate issuing authority should maintain military-grade data centers and disaster recovery sites optimized for data protection and availability.

d. For data at rest, what encryption technology is utilized for data storage?

e. For data at rest, how are encryption keys for stored data managed?

f. Particularly for data backup and recovery, what technology is used to encrypt data backups and how are those keys managed?

g. If databases are utilized, to what level is encryption applied?

3. Access Privileges

CSPs should be able to demonstrate they enforce adequate hiring, training, oversight and access controls to enforce administrative delegation.

a. A description of the physical security measures in place within the Vendors data centers. Describe both the physical data center access as well as server room and physical host access.

b. How are the logical and physical data center services secured from other users and from external threats?

c. What level of support does the Vendor provide for Single-Sign-On (SSO) or authentication utilizing DDSB identity management infrastructure?

d. A detailed description of those authentication methods.

e. Any support for two-factor authentication?

f. What level of administrative privileges and controls does DDSB IT Services have over the system or software and its users?

4. Regulatory Compliance

Information Owners are accountable for their own data even when it is in a Public Cloud Storage Service and should ensure their CSPs are ready and willing to undergo audits and provide proof of such audits.

a. What is the Vendor's and any 3rd party's compliance requirements to SSAE 16/SAS70-II, SOX, PCI-DSS, ISAE3402, SOC1, 2 or 3, Safe Harbor, or other regulatory certification requirements?

b. Can the Vendor describe the commitment to their and any 3rd party utilized to remain in such compliance?

c. Will the Vendor attach their latest compliance audit performed by a recognized qualified 3rd party and commit to maintaining that described level of security?

d. What ISO standards do the Vendors adhere too?

5. Data Provenance

When selecting a CSP, ask where their datacenters are located and if they can commit to specific privacy requirements.

a. A description of how often is infrastructure/hardware/software upgraded, hardened and patched and what communications/requirements are there with the customer?

b. Describe the automated Information Lifecycle (Configuration Upgrade and Control) Management capabilities of Cloud Service offering and the benefits clients receive from this functionality.

c. What are any options for dedicated storage, dedicated hardware firewalls and load balancers to connect to the Public Cloud Storage Service offerings in the Vendor's facilities?

d. Can you share networks, VPNs, firewalls and load balancers between the Vendors dedicated and Public Cloud Storage Service environments?

e. Explain your data and sensitive documents handling and destruction practices for customer data.

f. Define where geographically data is stored and ensure that it complies with MFIPPA, PHIPA and the Education Act.

6. Data Segregation

Most Public Cloud Storage Services are shared environments, and it is critical to make sure hosting providers can guarantee complete data segregation for secure multi-tenancy.

a. Provide an overview of the dedicated single-tenant and shared (multi-tenant) Cloud Services provided by the CSP.

b. Notation if the data center components are provided by Vendor or by another third party

and a description of maintenance or transfer of those services.

c. As a customer, how are we responsible for entering or transferring data?

d. Explain how data is either physically or logically separated such that one account cannot see data from any other account.

7. Data Recovery

Ensuring that the hosting provider can do a complete restoration in the event of a disaster.

a. Describe the SAN and/or NAS storage options connected to the Cloud Service.

b. Describe the backup and archival process and length of time backups are available.

c. Does the CSP perform test restores?

d. Does the CSP have any file or directory versioning capability or capabilities short of restoring from a backup?

e. Location of backups and key management and storage for any backup encryption keys.

f. What archival backup/restore/versioning is part of the agreement and what actions require any additional service fees?

g. Explain any shadowing or redundancy the Vendor has across multiple datacenters or repositories, the geographic location of those data repositories and whether the data repositories controlled by the Vendor.

h. An explanation of the Vendor disaster recovery plan with maximum downtime limits.

i. Does the Cloud Service offer persistent Cloud images (longer than 2-week retention) or offer back up in the Cloud Service longer than 1-month retention?

j. Does the Cloud Service backup allow file based restore, without requiring clients to mount a full historic copy of their virtual machine?

8. Monitoring and Reporting

Monitoring and logging Public Cloud Storage Service activity is difficult to do. DDSB employees should ask for proof that their hosting providers can support investigations.

a. Explain how the Vendor monitors and reports upon notification of abuse or investigation. This might include notices to the Information and Privacy Commissioner of Ontario, criminal or civil investigations and additional requests made by either an outside entity or the DDSB.

b. Explain the dashboards and analytics that are in place for customer use.

c. Explain any real-time monitoring that the customer might deploy that the Vendor has developed.

d. Explain what additional reporting, training, aggregate, industry, research, or other reporting

information or data might be available as part of a customer subscription.

e. Define and secure documentation on Vendor's policy in case of a data breach.

9. Business Continuity

Businesses come and go, and DDSB employees should ask hard questions about the portability of their data to avoid lock-in or potential loss if the business fails.

a. Does the Vendor have a formal Risk Analysis plan that is reviewed annually?

b. Does the Vendor have a disaster recovery plan?

c. What tests does the Vendor perform to audit their disaster recovery plan?

d. What are the contract stipulations for potential customer losses or for transfer of data and support to another organization should the business fail?

Appendix B: Definitions

In this Procedure,

1. "**Cloud Service**" means a specific service offering computing, networking, application, or storage function made available to users on demand via the Internet from a Cloud Service Provider as opposed to being provided from an organization's own on-premise servers and equipment.

2. "**Cloud Service Provider**" or "**CSP**" means a company that offers components of cloud computing. CSPs use their own data centres and compute resources to host cloud computing–based infrastructure and platform services for customer organizations. The CPS may also be, but not necessarily, the Vendor.

3. "**Confidential Information**" means all information of the DDSB that is of a confidential nature, including all confidential information in the custody or control of the DDSB, regardless of whether it is identified as confidential or not, and whether recorded or not, and however fixed, stored, expressed or embodied, which comes into the knowledge, possession or control of the Vendor and CSP in connection with an agreement with the DDSB. For greater certainty, Confidential Information shall:

    i. include: (i) all new information derived at any time from any such information whether created by the DDSB, the Vendor, CSP, or any third-party; (ii) all information (including Personal Information) that the DDSB is obliged, or has the discretion, not to disclose under provincial or federal legislation or otherwise at law; but

    ii. not include information that: (i) is or becomes generally available to the public without fault or breach on the part of the Vendor or CSP of any duty of confidentiality owed by the Vendor or CSP to the DDSB or to any third-party; (ii) the Vendor or CSP can demonstrate to have been rightfully obtained by the Vendor or CSP, without any obligation of confidence, from a third-party who had the right to transfer or disclose it to the Vendor nor CSP free of any obligation of confidence; (iii) the Vendor or CSP can demonstrate to have been rightfully known to or in the possession of the Supplier at the time of disclosure, free of any obligation of confidence when disclosed; or

    iii. (iv) is independently developed by the Vendor or CSP; but the exclusions in this subparagraph shall in no way limit the meaning of Personal Information or the obligations attaching thereto under the DDSB's agreement with the Vendor or at law;

4. "**Data Segregation**" means the process of separating certain sets of data from other data sets so that different access policies can be applied to those different data sets. The goal of doing so is only allowing the individuals who are authorized to view certain data sets access to that data.

5. "**Information Owner**" means the DDSB employee who creates information or is delegated responsibility for the information.

6. "**Personal Information**" or "**PI**" means recorded information about an identifiable individual. As defined by MFIPPA this may include, but is not limited to:

    a. Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual

orientation or marital or family status of the individual, Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

b. Any identifying number, symbol or other particular assigned to the individual,

c. The address, telephone number, fingerprints or blood type of the individual,

d. The personal opinions or views of the individual except if they relate to another individual,

e. Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

f. The views or opinions of another individual about the individual, and

g. The individual's name if it appears with other PI relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

7. "**Personal Health Information**" or "**PHI**" means information about an individual that pertains to health care, including information about an individual's physical or mental health, receipt of health care services and health number.

8. "**Subcontractor**" means, in the case of each Vendor, any contractor of that Vendor or any of its subcontractors at any tier of subcontracting.

9. "**Vendo**r" means the entity that is, or may be, selected to provide Cloud Services to the DDSB.

10. "**Vendor Personnel**" means individuals who are employed or contracted to the Vendor or the Vendor's consortium.