## GENERAL

| | |
|---|---|
| Effective | September 10, 2015 |
| Author / Maintainer | Director, Information Security |
| Responsibility / Owner | Executive Vice-President, Media Technology and Infrastructure Services |
| Approver(s) | Executive Vice-President, Media Technology and Infrastructure Services |
| Related to Policy | 2.5.1: Use of Technology Assets Policy |

## OBJECTIVE

The objective of this Directive is to ensure that the selection, adoption, acquisition, implementation and oversight of all external cloud-based solutions by CBC/Radio-Canada are founded on informed business decisions that consider the benefits, costs and risks involved.

It also offers direction on selecting, adopting, acquiring, implementing and overseeing externally hosted cloud-based solutions that meet the Corporation's current and future business needs without jeopardizing the Corporation's information and resources.

## SCOPE

| | |
|---|---|
| Audience | Any person or business unit within CBC/Radio-Canada that has a business need to adopt or acquire a cloud-based solution. |
| Processes | The selection, adoption, acquisition, implementation and oversight of cloud-based solutions. |
| Systems | All cloud-based solutions |

## DEFINITIONS

Cloud-based Solution: An internet based service that is externally hosted or managed by a third party and supports the on-demand provision of information technology capabilities.

Compromised Information: Information that is lost, corrupted, viewed or made public without proper authorization.

Requester: Any person within CBC/Radio-Canada who wishes to select, adopt, acquire or implement a cloud-based solution. This person must have the appropriate Delegation of Signing Authority (DSA) to approve the adoption and acquisition of the cloud-based solution.

Solution Owner: The person within CBC/Radio-Canada who assumes the ownership of a cloud-based solution. This person must have the appropriate DSA.

## STATEMENTS

All Requesters must make informed business decisions that consider the benefits, costs, and risks involved for the Corporation.

1. **Assessing Currently Implemented Cloud-based Solutions**

   Before selecting, adopting or acquiring any cloud-based solution, the Requester must first verify whether an existing solution meeting his/her business needs already exists at CBC/Radio-Canada by consulting the Media and Enterprise Technology Services (METS) Information Security Department.

   Should an appropriate solution already exist, the Requester must contact the associated Solution Owner. The Solution Owner may grant or deny access, based on administrative and/or operational considerations. If access is granted, the Requester must proceed as instructed by the Solution Owner, who is responsible for ensuring compliance with this Directive.

2. **Selecting and Adopting a New Cloud-based Solution**

   a) If no solution meeting the Requester's business needs exists within the Corporation, or in the event that access to an existing solution is not granted by its Solution Owner, the Requester must contact the METS Information Security Department for assistance in selecting a new solution and becoming a Solution Owner.

   b) With the assistance of the METS Information Security Department, the Requester must complete the Cloud-based Solutions Checklist by providing the following information:

      i) Service Level and Monitoring: Identify the service level and performance monitoring required by business needs and evaluate them against the service level and the performance monitoring provided by the service provider.

If the solution requires a negotiated contract, both the Requester and the METS Information Security Department must agree on the service level and performance monitoring requirements to be included within the agreement.

ii) Business Continuity: If the service is deemed a critical business function for which a prolonged service interruption cannot be tolerated, consult the Business Continuity Program Manager, as assigned by the Emergency Operations Teams, to establish business continuity measures.

iii) Incident Management: In order to manage incidents (such as service interruption and security or privacy breaches), develop and maintain a list of key contacts within CBC/Radio-Canada, as well as a list of the provider's operational contacts.

iv) Information Classification: Identify the sensitivity level of the information collected, used, stored and processed by the cloud-based solution, as defined by 2.9.7: Information Classification Policy.

## 3. Assessing Information Security and Privacy Requirements

Based on the sensitivity level of the information that may be collected, used, stored and processed while using the proposed cloud-based solution (as defined by 2.9.7: Information Classification Policy), the Requester must ensure that the proper security and privacy teams are involved in assessing the cloud-based solution, as required by the table below. The METS Information Security Team will assist in determining whether security and/or privacy risk assessments are required:

**Assessment Requirement Table**

| **Sensitivity level of information collected, used, stored, and processed** (based on 2.9.7: Information Classification Policy) | **Security Risk Assessment (SRA)** | **Privacy Impact Assessment (PIA)** |
|---|---|---|
| **Unrestricted** (if made public would likely have insignificant impact) | Not required | Not required |
| **Internal Use** (if compromised would likely have minor impact) | Not required | Not required |
| **Confidential** (if compromised would likely have moderate impact) | Required:<br><br>Contact the METS Information Security Department for assistance | Required for personal information:<br><br>Contact the Access to Information and Privacy (ATIP) Office for assistance |
| **Restricted** (if compromised would likely have major or severe impact) | Required:<br><br>Contact the METS Information Security Department for assistance | Required for personal information:<br><br>Contact the Access to Information and Privacy (ATIP) Office for assistance |

**Acquiring and Implementing a New Cloud-based Solution**

a) The Requester must provide the Cloud-based Solutions Checklist to the METS Information Security Department, and attach the Cloud-based Solutions Checklist to the Expense Report or Procurement Checklist that accompanies the Purchase Requisition in SAP.

b) For a negotiated contract, the Requester must contact Supply Management Services (SMS) and Legal Services to ensure that the contract includes the key contractual elements required for cloud-based solutions.

c) SMS must ensure that purchase orders and expenditures for all new cloud-based solutions are completed using either the Expense Report or Procurement Checklist and that the Cloud-based Solution Checklist is complete, authorized by the appropriate DSA, and attached to the request.

d) Once the cloud-based solution has been adopted, acquired and implemented by the Requester, he/she will then become the Solution Owner of the cloud-based solution.

## 4. Interpretation and Application

a) The Solution Owner must:

i) ensure that all measures identified by the SRA or the PIA are implemented internally or by the provider, and remain active as long as the solution is in use;
ii) set up measures to manage or delegate the management of subscriptions, as well as the assignment and unassignment of user access; and
iii) oversee the decommissioning of the solution.

If the Solution Owner delegates some or all of his/her responsibilities to an employee, another sector, or an external party, he/she is still ultimately accountable for ensuring compliance with this Directive.

b) The METS Information Security Department is responsible for overseeing the application of this Directive.

c) The Executive Vice-President, Media Technology and Infrastructure Services oversees CBC/Radio-Canada's appropriate use and governance of cloud-based solutions, approves this Directive and ensures the proper allocation of resources to support this Directive. Once a year, his/her team reviews the Implemented Cloud-based Solutions List to identify opportunities to consolidate cloud-based solutions or expand access to them to other individuals or Departments within the Corporation.

## APPENDIX A – Key Information Security Elements for Negotiated Cloud-based Solution Contracts

This Appendix presents key Information Security elements related to external cloud-based solutions that should be included in all contracts negotiated with providers.

- Right to audit the provider's security measures and mechanisms
- Right to obtain the standard auditing report CSAE 3416 (also known as SSAE16, or formally SAS70)
- Right to perform additional auditing based on an "Agreed-upon procedure engagement" (also known as 9110)
- Right to request information security assessments
- Right to access Business Continuity/Disaster Recovery processes and testing results
- Requirements related to service level and performance monitoring (to be determined based on business needs)
- Requirements related to incident management, such as contacts and expected time for taking action when an incident occurs
- Specific measures related to the intention of the provider, as identified by the Security Risk Assessment
- A clause ensuring that the provider promptly notifies in the case of breaches that potentially affect the availability, confidentiality or integrity of CBC/Radio-Canada's information
- A clause ensuring that the terms of termination permit the transfer of data back to the organization and that the cloud provider securely deletes information within reasonable timeframes