RENSEIGNEMENTS GÉNÉRAUX

Date d'entrée en vigueur	10 septembre 2015
Auteur/réviseur	Directeur, Sécurité de l'information
Responsable	Vice-président principal, Infrastructure et Services technologiques médias
Approbateur(s)	Vice-président principal, Infrastructure et Services technologiques médias
Politique qui s'y rapporte	Politique 2.5.01 – Utilisation des biens technologiques

OBJECTIF

La présente directive vise à s'assurer que la sélection, l'adoption, l'acquisition, la mise en œuvre et la supervision de toutes les solutions infonuagiques externes par CBC/Radio-Canada sont fondées sur des décisions opérationnelles éclairées qui tiennent compte des avantages, des coûts et des risques qui en découlent.

Elle donne aussi des indications pour la sélection, l'adoption, l'acquisition, la mise en œuvre et la supervision de solutions infonuagiques hébergées à l'externe qui répondent aux besoins opérationnels actuels et à venir de CBC/Radio-Canada, sans compromettre l'information ni les ressources de la Société.

PORTÉE

Auditoire	Toute personne ou tout secteur de CBC/Radio-Canada qui doit du point de vue opérationnel adopter ou acquérir une solution infonuagique.
Processus	La sélection, l'adoption, l'acquisition, la mise en œuvre et la supervision de solutions infonuagiques.
Systèmes	Toutes les solutions infonuagiques

DÉFINITIONS

Solution infonuagique : service en ligne hébergé à l'extérieur ou géré par un tiers qui permet la fourniture de capacités technologiques.

Information compromise : information perdue, corrompue, vue ou rendue publique sans autorisation appropriée.

Demandeur : toute personne au sein de CBC/Radio-Canada qui souhaite sélectionner, adopter, acquérir ou mettre en œuvre une solution infonuagique. Cette personne doit être titulaire d'une délégation du pouvoir de signature (DPS) pour être en mesure d'approuver l'adoption et l'acquisition de la solution infonuagique.

Responsable de la solution : la personne à CBC/Radio-Canada qui assume la responsabilité d'une solution infonuagique. Cette personne doit être titulaire de la DPS appropriée.

ÉNONCÉS

Tous les demandeurs doivent prendre des décisions opérationnelles éclairées qui tiennent compte des avantages, des coûts et des risques qui en découlent pour la Société.

1. **Évaluation des solutions infonuagiques utilisées actuellement**

   Avant de sélectionner, d'adopter ou d'acquérir une solution infonuagique, le demandeur doit vérifier s'il n'existe pas déjà une solution à CBC/Radio-Canada qui répond à ses besoins en consultant la liste des solutions infonuagiques déjà mises en œuvre, qui est tenue à jour par le service de la Sécurité de l'information des Services technologiques d'entreprise et aux médias (STEM).

   Au cas où il existerait déjà une solution appropriée, le demandeur doit communiquer avec le responsable de la solution en question. Celui-ci peut autoriser ou refuser l'accès en fonction de considérations administratives ou opérationnelles. Si l'accès est autorisé, le demandeur doit suivre les instructions fournies par le responsable de la solution, qui est chargé de faire respecter la présente directive.

2. **Sélection et adoption d'une nouvelle solution infonuagique**

   a) S'il n'existe aucune solution répondant aux besoins opérationnels du demandeur, ou si l'accès à une solution existante n'est pas autorisé par le responsable de la solution, le demandeur doit communiquer avec le service de la Sécurité de l'information des STEM afin d'obtenir de l'aide pour sélectionner une nouvelle solution et devenir un responsable de la solution.

   b) Avec l'aide du service de Sécurité de l'information des STEM, le demandeur doit remplir la liste de vérification des solutions infonuagiques en fournissant l'information suivante :

      i) Niveau de service et surveillance : Déterminer le niveau de service et le suivi du rendement exigés par les besoins opérationnels et les évaluer par rapport au niveau de service et au suivi du rendement assurés par le fournisseur de service.

Si la solution nécessite un contrat négocié, le demandeur et le service de la Sécurité de l'information des STEM doivent s'entendre sur les exigences en matière de niveau de service et de suivi du rendement à inclure dans l'entente.

ii) Continuité des activités : Si le service est jugé être une fonction opérationnelle critique, dont une interruption prolongée ne peut être tolérée, consulter le gestionnaire du Programme de continuité des activités désigné par l'équipe d'opérations d'urgence afin de déterminer les mesures de continuité des activités.

iii) Gestion des incidents : Afin de gérer les incidents (comme les interruptions de service ou les atteintes à la vie privée), dresser et tenir à jour une liste des principaux contacts au sein de CBC/Radio-Canada, ainsi qu'une liste des contacts opérationnels du fournisseur.

iv) Classification de l'information : Déterminer le niveau de sensibilité de l'information recueillie, utilisée, stockée et traitée par la solution infonuagique, comme le définit la politique 2.9.7 sur la classification des documents.

3. Évaluation des exigences en matière de sécurité de l'information et de respect de la vie privée

En fonction du niveau de sensibilité de l'information recueillie, utilisée, stockée et traitée à l'aide de la solution infonuagique proposée (comme le définit la politique 2.9.7 sur la classification des documents), le demandeur doit s'assurer que les équipes appropriées en matière de sécurité et de protection des renseignements personnels participent à l'évaluation de la solution infonuagique conformément au tableau ci-dessous. L'équipe du service de la Sécurité de l'information des STEM vous permettra de déterminer si des évaluations du risque pour la sécurité et des facteurs relatifs à la vie privée sont nécessaires :

Tableau d'évaluation des exigences

Niveau de sensibilité de l'information recueillie, utilisée, stockée et traitée (Selon la politique 2.9.7 : politique sur la classification des documents)	**Évaluation du risque pour la sécurité (ERS)**	**Évaluation des facteurs relatifs à la vie privée (EFVP)**
Sans restriction (incidences négligeables si le document est rendu public)	Non requise	Non requise
Utilisation interne (incidences mineures si l'information était compromise)	Non requise	Non requise
Confidentiel (incidences modérées si l'information était compromise)	Requise : Communiquer avec le service de la Sécurité de l'information des STEM	Requise pour les renseignements personnels : Pour obtenir de l'aide, communiquer avec le bureau de l'accès à l'information et à la protection des renseignements personnels (AIPRP)
Diffusion restreinte (incidences majeures ou critiques si l'information était compromise)	Requise : Communiquer avec le service de la Sécurité	Requise pour les renseignements personnels :

	de l'information des STEM	Pour obtenir de l'aide, communiquer avec le bureau de l'accès à l'information et à la protection des renseignements personnels (AIPRP)

Acquisition et mise en œuvre d'une nouvelle solution infonuagique

a) Le demandeur doit fournir la liste de vérification des solutions infonuagiques au service de la Sécurité de l'information des STEM, et également joindre la liste au rapport de dépenses ou à la liste de vérification de l'Approvisionnement qui accompagne la demande d'achat dans SAP.

b) Pour les contrats négociés, le demandeur doit communiquer avec le Service de gestion des approvisionnements (SGA) et le Service juridique pour s'assurer que le contrat comprend les principaux éléments contractuels nécessaires pour les solutions infonuagiques.

c) Le SGA doit s'assurer que les bons de commande et les formulaires de dépenses associés à toutes les nouvelles solutions infonuagiques sont remplis à l'aide du rapport de dépenses ou de la liste de vérification de l'Approvisionnement, et que la liste de vérification des solutions infonuagiques est dûment remplie, autorisée par le titulaire de la délégation du pouvoir de signature approprié et jointe à la demande.

d) Une fois la solution infonuagique adoptée, acquise et mise en œuvre par le demandeur, celui-ci devient alors le responsable de la solution infonuagique.

4. Interprétation et application

a) Le responsable de la solution doit :

i) S'assurer que toutes les mesures déterminées à l'aide de l'ERS ou de l'EFVP sont mises en œuvre à l'interne ou par le fournisseur et qu'elles demeurent en vigueur tant que la solution est utilisée;
ii) Prendre des mesures pour gérer la gestion des inscriptions, ou en déléguer la gestion, ainsi que l'attribution ou la suppression de l'accès des utilisateurs; et
iii) Superviser la mise hors service de la solution.

Si le responsable de la solution délègue certaines ou toutes ses responsabilités à un employé, à un autre secteur ou à un tiers de l'externe, il demeure entièrement responsable de garantir la conformité à la présente directive.

b) Le service de la Sécurité de l'information des STEM est chargé de superviser l'application de la présente directive.

c) Le Vice-président principal, Infrastructure et Services technologiques medias supervise l'utilisation et la gouvernance appropriées des solutions infonuagiques par CBC/Radio-Canada, approuve la présente directive et s'assure de l'attribution appropriée des ressources nécessaires pour appuyer la présente directive. Une fois par an, son équipe passe en revue la liste des solutions infonuagiques mises en œuvre pour cerner les possibilités de consolider les solutions infonuagiques ou en élargir l'accès à d'autres personnes ou services au sein de la Société.

ANNEXE A – Éléments clés relatifs à la sécurité de l'information pour les contrats négociés de solutions infonuagiques

Cette annexe présente des éléments clés relatifs à la sécurité de l'information pour les solutions infonuagiques externes qui doivent être inclus dans tous les contrats négociés avec des fournisseurs.

- Le droit de vérifier les mesures et les mécanismes en matière de sécurité.
- Le droit d'obtenir le rapport de vérification standard CSAE 3416 (également appelé SSAE16 ou SAS70 auparavant).
- Le droit de procéder à des vérifications additionnelles en vertu d'une « mission d'application de procédés convenus » (également appelé 9110).
- Le doit de demander des évaluations de la sécurité de l'information.
- Le droit d'accéder aux processus de continuité des activités/reprise après sinistre, ainsi qu'aux résultats des essais.
- Des exigences liées au suivi du niveau de service et de rendement à déterminer en fonction des besoins opérationnels).
- Des exigences liées à la gestion des incidents, comme les personnes-ressources et le délai de réaction prévu en cas d'incident.
- Des mesures particulières liées à l'intention du fournisseur, comme le détermine l'évaluation du risque pour la sécurité.
- Une garantie voulant que le fournisseur nous avise promptement en cas d'atteintes à la sécurité qui auraient des conséquences éventuelles sur la disponibilité, la confidentialité ou l'intégrité de l'information de CBC/Radio-Canada.
- Une garantie voulant que les modalités de résiliation autorisent le transfert des données à l'organisation et que le fournisseur de la solution supprime l'information en toute sécurité dans un délai raisonnable.