Bibliothèque et Archives nationales Québec

POLITIQUE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION (P-3)

Adoptée par le conseil d'administration le 22 octobre 2020

POLITIQUE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Adoption :	
Conseil d'administration	12 décembre 2013

Modifications :	
Conseil d'administration	22 septembre 2016
Conseil d'administration	22 octobre 2020

Table des matières

POLITIQUE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

PRÉAMBULE

Le monde n'a plus de frontières et l'espace numérique est à la merci d'actions malveillantes dont le vol d'informations personnelles et autres actions frauduleuses, la cyberintimidation et la perte de données. L'exercice des activités de BAnQ n'échappe pas au contexte actuel où les attaques de toute nature se développent et se complexifient.

BAnQ détient de l'information de nature variée : renseignements personnels et information ayant une valeur légale, administrative, économique et patrimoniale. BAnQ reconnaît l'influence grandissante du numérique, son importance pour l'accomplissement de ses missions et la nécessité de son intégration aux processus de travail et de gestion. Dans ce contexte, il est indispensable pour BAnQ de se doter d'une politique en matière de sécurité de l'information qui puisse s'adapter aux changements constants de son environnement, particulièrement de son environnement technologique.

La présente politique témoigne de l'engagement et de la détermination de BAnQ à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information qu'elle détient, quel que soit son support ou son moyen de communication et tout au long de son cycle de vie. Elle permet à BAnQ de veiller à préserver sa réputation, à respecter la législation et à réduire les risques en protégeant l'information créée, reçue, traitée et conservée par BAnQ au cours de ses activités.

Tout en s'inscrivant dans le cadre du plan de gestion des risques stratégiques de BAnQ, la présente politique est élaborée conformément aux exigences légales (notamment, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, la Directive sur la sécurité de l'information gouvernementale et le Cadre gouvernemental de gestion de la sécurité de l'information) et selon les meilleures pratiques.

La présente politique énonce des principes directeurs qui encadrent la sécurité de l'information au sein de BAnQ et précise les rôles et responsabilités des différents intervenants en vue d'assurer la gestion de la sécurité de l'information. Enfin, la présente politique se fonde sur les principes de prévention et de responsabilisation personnelle et collective des membres de la communauté de BAnQ et de ses fournisseurs et partenaires externes.

1. DÉFINITIONS

À moins de mention contraire ou que le contexte n'indique un sens différent, les définitions de l'article 1 de la Directive encadrant le corpus règlementaire (D-1) s'appliquent à la présente politique.

De plus, dans le cadre de l'application de la présente politique, on entend par :

a) « ACTIF INFORMATIONNEL » : une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information ou une ressource informationnelle, une installation ou un ensemble de ces éléments, acquis ou constitués par BAnQ**;**

b) **« AUTHENTICITÉ » :** la propriété d'un document dont on peut prouver qu'il est bien ce qu'il semble être, qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu, et qu'il a été produit ou reçu au moment où il semble l'avoir été;

c) **« CONFIDENTIALITÉ » :** la propriété d'une information de n'être accessible qu'aux personnes autorisées à en prendre connaissance ;

d) **« CONTINUITÉ DES SERVICES » :** la capacité de BAnQ d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini;

e) **« CYCLE DE VIE DE L'INFORMATION » :** l'ensemble des étapes que franchit une information, de sa création jusqu'à sa conservation ou sa destruction en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, en conformité avec le calendrier de conservation de BAnQ**;**

f) **« DISPONIBILITÉ » :** la propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée**;**

g) **« DOCUMENT » :** un ensemble constitué d'information portée par un support. L'information y est délimitée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou d'un autre système de symboles. Sont assimilés à un document tout objet numérique et toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite;

h) **« GESTION DES RISQUES EN SÉCURITÉ DE L'INFORMATION » :** l'évaluation périodique des risques et des mesures de protection des actifs informationnels afin d'assurer une adéquation entre les risques, les menaces et les mesures de protection et d'atténuation déployées**;**

i) **« INCIDENT » :** un événement qui porte atteinte, ou qui est susceptible de porter atteinte, à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité;

j) **« INFORMATION » :** un renseignement consigné sur un support quelconque ou communiqué dans un but de transmission des connaissances;

k) **« INTÉGRITÉ » :** la propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité;

l) **« RENSEIGNEMENT CONFIDENTIEL » :** tout renseignement dont l'accès est assorti d'une ou plusieurs restrictions prévues par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Par exemple, ces restrictions peuvent viser l'administration de la justice et la sécurité publique, les décisions administratives, les négociations entre organismes publics ou la vérification;

m) **« RENSEIGNEMENT PERSONNEL » :** tout renseignement qui concerne une personne physique et permet de l'identifier;

n) **« RISQUES POUR LA SÉCURITÉ DE L'INFORMATION » :** tout événement comportant un degré d'incertitude qui pourrait porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité de l'information et qui pourrait avoir des conséquences sur la prestation des services, sur la vie, la

santé ou le bien-être des personnes, sur la protection de leurs renseignements personnels, le respect de leur vie privée, ou sur l'image de BAnQ;

o) « SÉCURITÉ INFORMATIONNELLE » : l'ensemble de mesures de sécurité physiques, informatiques et administratives et de mesures d'urgence mises en place dans une organisation en vue d'assurer la protection de l'ensemble de ses actifs informationnels. Plus particulièrement, la sécurité informationnelle assure l'intégrité, la confidentialité, l'authenticité et la fiabilité des actifs informationnels ainsi que l'imputabilité et la non-répudiation des incidents. Ces mesures s'ajoutent aux règles spécifiques permettant d'assurer la sécurité des documents patrimoniaux et archivistiques, qui ne sont pas traitées dans la présente politique ;

p) « SÉCURITÉ PHYSIQUE » : les mesures physiques prises pour assurer la protection des personnes et des biens, notamment pour empêcher tout accès non autorisé aux équipements, installations et documents, et les protéger contre toute forme de menace physique ou accidentelle;

q) « UTILISATEUR » : tout membre de la communauté de BAnQ, à l'exclusion de ses usagers, utilisant ou ayant accès aux actifs informationnels de BAnQ. Sont également des utilisateurs les fournisseurs et partenaires externes de BAnQ lorsqu'ils utilisent les actifs informationnels de BAnQ ou y accèdent dans le cadre de contrats ou de partenariats conclus avec elle.

2. OBJECTIFS

La présente politique vise à :

a) protéger et sécuriser l'information tout au long de son cycle de vie;

b) assurer une utilisation et un traitement des renseignements personnels et des renseignements confidentiels conformes à la législation en vigueur;

c) encadrer et mettre en place des mesures de gestion et de contrôle assurant la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information;

d) responsabiliser les différents utilisateurs quant à l'importance de leurs actions individuelles pour assurer la sécurité de l'information;

e) mettre en œuvre la reddition de comptes en matière de sécurité de l'information prévue par le plan de gestion des risques stratégiques de BAnQ;

f) favoriser une démarche de gestion des risques et des incidents actualisée et vérifiée de façon périodique;

g) assurer la pérennité d'une information fiable.

Plus généralement, la présente politique vise également à assurer le respect des principes directeurs de la sécurité de l'information gouvernementale et leur intégration dans les documents normatifs de BAnQ encadrant la sécurité de l'information.

3. CHAMP D'APPLICATION

La présente politique s'adresse à tous les utilisateurs et s'applique à tous les actifs informationnels possédés, détenus, utilisés ou traités par BAnQ, que leur conservation soit assurée par elle-même ou par un tiers.

4. CADRE JURIDIQUE

Le cadre juridique de la présente politique est notamment composé de :

a) la *Charte des droits et libertés de la personne*, RLRQ, c. C-12;

b) la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1;

c) le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, c. A-2.1, r. 2;

d) la *Loi sur les archives*, RLRQ, c. A-21.1;

e) la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1;

f) la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03;

g) la Directive sur la sécurité de l'information gouvernementale, décret 7-2014 du 15 janvier 2014;

h) le Cadre gouvernemental de gestion de la sécurité de l'information;

i) le Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;

j) les conventions collectives en vigueur à BAnQ.

Ce cadre juridique est complété par les éléments suivants du corpus règlementaire de BAnQ :

a) la Politique de gestion intégrée des risques;

b) la Politique en matière d'accès à l'information et de protection des renseignements personnels de BAnQ;

c) la Politique de gestion intégrée des documents administratifs de BAnQ;

d) le Code d'éthique des employés;

e) la Directive encadrant le corpus règlementaire (D-1).

5. PRINCIPES DIRECTEURS

5.1 Protection de l'information

5.1.1 Les actifs informationnels détenus par BAnQ sont essentiels à ses activités et à la réalisation de ses missions et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate.

5.1.2 La sécurité de l'information doit être assurée tout au long de son cycle de vie. Le niveau de protection et les moyens mis en œuvre pour assurer la protection de l'information doivent être proportionnels à la valeur de l'information, à son importance et à sa nature confidentielle ainsi qu'aux risques auxquels elle est exposée.

5.1.3 Toute information détenue par BAnQ doit faire l'objet de mesures de sécurité visant à :

- assurer sa disponibilité en tout temps et de la manière requise par une personne autorisée;
- assurer son intégrité de manière qu'elle ne soit pas détruite ou altérée de quelque façon sans autorisation et que le support sur lequel elle se trouve lui procure la stabilité et la pérennité voulues;
- en limiter l'accès ou la divulgation aux seules personnes autorisées à en prendre connaissance, de façon à garantir une utilisation stricte, contrôlée et confidentielle lorsque cela est nécessaire;
- permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif (authentification), sauf en ce qui concerne l'information qui est publique.

5.1.4 Toute information confidentielle doit être préservée de toute divulgation, de tout accès et de toute utilisation non autorisés.

5.2 Responsabilité

5.2.1 L'efficacité des mesures de sécurité de l'information repose sur l'attribution claire de responsabilités aux utilisateurs à tous les niveaux et exige que chacun réponde de ses actes.

5.2.2 Elle nécessite la mise sur pied d'un processus de gestion interne de la sécurité de l'information permettant une reddition de comptes adéquate.

5.3 Évolution

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, des pratiques gouvernementales ainsi que de l'évolution des menaces et des risques.

5.4 Meilleures pratiques

BAnQ adhère aux principes de partage des meilleures pratiques en matière de sécurité de l'information, s'appuie sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et a recours à des barèmes de comparaison avec des organismes ou des établissements similaires.

5.5 Proactivité

La sécurité de l'information requiert la mise sur pied de mesures proactives et de méthodes de détection d'usage abusif ou inapproprié de l'information, qui doivent cependant respecter les droits et libertés fondamentaux.

5.6 Éthique

Le cadre de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant notamment la responsabilisation collective et individuelle, conformément au Code d'éthique des employés.

5.7 Sensibilisation et formation du personnel

BAnQ s'engage à mettre en place et maintenir un programme d'accueil et de formation continue de son personnel afin de sensibiliser les utilisateurs à l'importance de la sécurité des actifs informationnels et aux conséquences d'une atteinte à leur sécurité et de les former de façon qu'ils puissent assumer leur rôle et leurs obligations en cette matière.

5.8 Cadre de gestion

La présente politique s'articule autour de trois axes de gestion fondamentaux : la gestion des risques, la gestion des accès et la gestion des incidents.

6. GESTION DES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION

6.1 Principes

6.1.1 La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global du plan de gestion des risques stratégiques de BAnQ.

6.1.2 L'engagement de la direction de BAnQ ainsi que la collaboration de tous les utilisateurs sont nécessaires à la bonne gestion des risques liés à la sécurité de l'information.

6.1.3 BAnQ adopte une approche basée sur le risque acceptable, laquelle vise à permettre de protéger l'information tout au long de son cycle de vie.

6.1.4 BAnQ vise le maintien d'un équilibre entre l'accès aux outils permettant la prestation de travail et la sécurité de l'information.

6.2 Mesures de gestion des risques

Afin d'atteindre ses objectifs en matière de gestion des risques liés à la sécurité de l'information, BAnQ doit :

6.2.1 créer et tenir à jour une catégorisation des actifs informationnels qu'elle possède, détient ou utilise afin de connaître la nature et la valeur de l'information à protéger;

6.2.2 déterminer et instaurer des mesures et un niveau de protection de l'information permettant de minimiser les risques en fonction :

a) de la nature et de la valeur de l'information à protéger;

b) des vulnérabilités exploitables décelées : probabilités d'accident, d'erreur ou de malveillance;

c) d'une évaluation qualitative et quantitative des conséquences de la matérialisation de ces risques;

d) du niveau de risque acceptable par BAnQ;

6.2.3 adopter une procédure d'acceptation des risques en matière de sécurité informatique assurant que toute dérogation à une norme de sécurité informatique en vigueur à BAnQ soit décelée, justifiée, documentée et qu'elle fasse l'objet d'une acceptation de risques;

6.2.4 guider l'acquisition, le développement et l'exploitation des systèmes d'information en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans son environnement;

6.2.5 déclarer les risques à portée gouvernementale conformément à la Directive sur la sécurité de l'information gouvernementale.

7. GESTION DES ACCÈS

7.1 Principes

7.1.1 La sécurité de l'information est assurée par des mesures d'encadrement et de contrôle adéquats restreignant strictement l'accès à l'information ainsi que la divulgation et l'utilisation de celle-ci aux personnes autorisées. Ces mesures doivent porter une attention particulière à la protection de la disponibilité, de l'intégrité et de la confidentialité des données ainsi qu'à la protection des renseignements personnels et des renseignements confidentiels.

7.1.2 La gestion des accès s'effectue conformément au corpus règlementaire et aux procédures adoptées afin de mettre en œuvre la présente politique.

7.2 Registre d'autorité

BAnQ se dote d'un registre d'autorité conforme aux exigences de la Directive sur la sécurité de l'information gouvernementale. Y sont notamment consignées les informations suivantes :

- les noms des détenteurs de l'information;
- les systèmes d'information qui leur sont assignés;
- les rôles et les responsabilités des principaux intervenants en sécurité de l'information;
- les accès à l'information autorisés au sein de BAnQ.

7.2.1 Constitution et mise à jour

Le registre d'autorité est :

- élaboré et mis à jour par le conseiller organisationnel en sécurité de l'information (le « **COSI** »);
- mis à jour de façon continue, notamment par l'ajout de tout nouveau système d'information ou de toute évolution majeure d'un système d'information existant et par la consignation de sa catégorisation et de son détenteur;
- mis à jour conformément aux normes adoptées afin de mettre en œuvre la présente politique;
- transmis pour information au président-directeur général et au comité sur la sécurité de l'information par le directeur général des ressources informationnelles au besoin, au minimum tous les deux ans.

7.2.2 Respect du registre d'autorité

Les détenteurs de l'information veillent au respect du registre d'autorité par les utilisateurs qui relèvent de leur responsabilité.

8. GESTION DES INCIDENTS

8.1 Principes

8.1.1 Afin d'assurer la continuité des services à la suite d'incidents et d'incidents de sécurité de l'information à portée gouvernementale, BAnQ doit disposer d'un processus de gestion des incidents liés à la sécurité de l'information et d'un plan de relève des composantes critiques pour assurer la prestation des services jugés prioritaires lors d'un sinistre.

8.1.2 Le responsable organisationnel de la sécurité de l'information (le « **ROSI** ») doit être avisé lors de la survenance de tout incident lié à la sécurité de l'information.

8.2 Registre d'incidents

8.2.1 Les incidents sont répertoriés dans un registre d'incidents. Y sont notamment consignées les informations suivantes :

- la nature de l'incident;
- ses effets;
- les mesures prises pour le retour à la normale et le suivi;
- l'analyse et la classification des incidents selon leur gravité.

8.2.2 Ce registre est tenu à jour par le COSI.

9. RÔLES ET RESPONSABILITÉS

La présente politique établit les obligations en matière de sécurité de l'information attribuées aux différents intervenants mentionnés ci-dessous.

9.1 Président-directeur général

Le président-directeur général est le premier responsable de la sécurité de l'information. À ce titre, il a la responsabilité de :

- s'assurer du respect des lois et des règles en matière de sécurité de l'information déterminées par le Secrétariat du Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques liés à la sécurité de l'information;
- s'assurer de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par BAnQ;
- s'assurer que les mesures de sécurité de l'information en vigueur répondent adéquatement aux risques encourus;
- désigner les principaux intervenants en sécurité de l'information, dont le ROSI;
- veiller à ce que le COSI désigne, parmi les employés de niveau cadre, les détenteurs de l'information aux fins de l'application de la présente politique;
- s'assurer de la création et de la mise à jour du registre d'autorité;
- nommer les membres du comité sur la sécurité de l'information;
- créer toute instance interne qu'il juge pertinente pour la mise en œuvre des mesures liées à la sécurité de l'information;
- superviser la reddition de comptes en matière de sécurité de l'information auprès du conseil d'administration et des autorités gouvernementales.

9.2 Directeur général des ressources informationnelles

Le directeur général des ressources informationnelles assure la gouvernance de la sécurité de l'information en collaboration avec le ROSI.

Il a la responsabilité de :

- recommander au ROSI et au comité sur la sécurité de l'information les orientations stratégiques et les priorités d'intervention;

- transmettre le registre d'autorité au président-directeur général et au comité sur la sécurité de l'information;

- voir à l'adoption, par sa direction générale, de procédures de mise en œuvre des exigences de la présente politique concernant l'acceptation des risques en matière de sécurité informatique;

- s'assurer de la prise en charge des exigences en matière de sécurité de l'information dans l'exploitation des systèmes d'information, ainsi que lors de la réalisation de projets de développement et de l'acquisition de systèmes d'information;

- s'assurer de la réalisation périodique d'audits de sécurité de l'information indépendants ainsi que de tests d'intrusion et de vulnérabilité, et en dégager des priorités;

- assurer la mise en œuvre du plan de relève informatique lorsque cela est nécessaire;

- nommer les intervenants suivants dont les rôles et responsabilités sont définis dans le Cadre gouvernemental de gestion de la sécurité de l'information et dans la présente politique :

    - le COSI;

    - le responsable de l'architecture de sécurité de l'information (RASI);

    - le responsable du développement ou de l'acquisition de systèmes d'information (RDASI);

    - le coordonnateur organisationnel de gestion des incidents (COGI).

Le directeur général des ressources informationnelles est le responsable de la gestion des technologies de l'information (RGTI). À ce titre, il a la responsabilité de :

- contribuer à l'élaboration et à la mise en œuvre de directives contribuant à assurer la sécurité de l'information numérique;

- mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par BAnQ, y compris les plans de relève informatique en cas de sinistre;

- instaurer un cadre normatif de développement assurant la prise en charge des exigences en matière de sécurité de l'information lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

9.3 Responsable organisationnel de la sécurité de l'information (ROSI)

Le ROSI a la responsabilité de :

- agir, auprès de BAnQ, comme porte-parole du dirigeant principal de l'information désigné par le gouvernement en communiquant les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information;

- assister le président-directeur général dans la détermination des orientations stratégiques et des priorités d'intervention;

- représenter le président-directeur général en matière de déclaration des incidents liés à la sécurité de l'information à portée gouvernementale;

- soumettre au comité sur la sécurité de l'information, pour consultation, les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes relatifs à la sécurité de l'information ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;

- rend compte au conseil d'administration en matière de sécurité de l'information;

- assurer la coordination et la cohérence des actions en matière de sécurité de l'information menées par les différents intervenants qui assument au sein de BAnQ des rôles et responsabilités en matière de sécurité de l'information en vertu de la présente politique;

- s'assurer de la contribution de BAnQ au processus de gestion des risques et des incidents liés à la sécurité de l'information à portée gouvernementale;

- s'assurer de la mise en œuvre de processus officiels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ayant mis ou qui auraient pu mettre en péril la sécurité de l'information;

- coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information.

9.4 Secrétaire général

Le secrétaire général a la responsabilité de :

- assurer la gouvernance de la sécurité de l'information en collaboration avec le ROSI;

- par délégation du président-directeur général, coordonner avec le ROSI la reddition de comptes en matière de sécurité de l'information dans le cadre du plan de gestion des risques stratégiques;

- veiller à la transmission de l'information nécessaire à l'exercice des fonctions du conseil d'administration, du comité de vérification et des finances, du conseil de direction et du directeur de la vérification interne;

- veiller à l'inclusion des éléments requis par la présente politique dans tout contrat conclu avec un fournisseur ou partenaire externe.

Le secrétaire général est le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP). À ce titre, il a la responsabilité de :

- veiller au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;

- communiquer au directeur général des ressources informationnelles les problèmes et les préoccupations concernant la sécurité en matière de protection des renseignements personnels et des renseignements confidentiels;

- contribuer à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

Le secrétaire général est le responsable de l'éthique (RE). À ce titre, il a la responsabilité de :

- veiller à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information afin d'assurer la régularisation des conduites et la responsabilisation individuelle.

9.5 Conservateur et directeur général des Archives nationales

Le conservateur et directeur général des Archives nationales est le responsable de la gestion documentaire (RGD). À ce titre, il a la responsabilité de :

- collaborer à la conception des systèmes informatiques, administratifs ou autres et s'assurer qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires pour permettre une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois;

- collaborer étroitement avec les détenteurs de l'information ainsi qu'avec le COSI en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information.

9.6 Directeur des ressources humaines

Le directeur des ressources humaines a la responsabilité de :

- veiller à ce que la procédure d'accueil des employés de la Direction des ressources humaines informe tout nouvel employé de l'existence des éléments du corpus règlementaire en matière de sécurité de l'information qui lui sont directement applicables.

9.7 Directeur de la vérification interne

Le directeur de la vérification interne est le responsable de la vérification interne (RVI). Il a la responsabilité d'évaluer, examiner ou vérifier, notamment :

- l'application, la validité et l'efficacité des plans d'action, des règles et des contrôles de sécurité élaborés et mis en œuvre en matière de sécurité de l'information;

- l'adéquation de l'intégration de la sécurité de l'information dans les processus organisationnels.

9.8 Directeur de la gestion immobilière et de la sécurité

Le directeur de la gestion immobilière et de la sécurité est le responsable de la sécurité physique (RSP). À ce titre, il a la responsabilité de :

- mettre en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentiels ou des supports d'information confidentielle;

- concevoir et mettre en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de BAnQ;

- s'assurer de la mise au rebut sécuritaire des supports de l'information;

- s'assurer que les salles des serveurs et salles de télécommunication sont uniquement accessibles aux utilisateurs autorisés;

- élaborer et mettre en œuvre des directives, des guides et des procédures propres à son domaine d'intervention et nécessaires afin d'assurer la sécurité de l'information.

9.9 Conseiller organisationnel en sécurité de l'information

Le COSI a la responsabilité de :

- soutenir le ROSI, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus formels liés à la sécurité de l'information;

- mettre en œuvre les orientations internes découlant des directives gouvernementales et des éléments du corpus règlementaire en matière de sécurité de l'information ainsi que les pratiques généralement admises à cet égard;

- désigner, parmi les employés de niveau cadre, les détenteurs de l'information aux fins de l'application de la présente politique;

- tenir à jour le registre d'incidents;

- élaborer et mettre à jour le registre d'autorité;

- produire les bilans et les plans d'action en matière de sécurité de l'information;

- participer, au besoin, aux négociations des ententes de service et des contrats et formuler des recommandations quant à l'intégration de dispositions contractuelles garantissant le respect des exigences en matière de sécurité de l'information;

- assister les détenteurs de l'information relativement à la catégorisation de l'information relevant de leur responsabilité et à la réalisation des analyses de risques de sécurité de l'information;

- contribuer à la mise en œuvre des processus officiels en matière de sécurité de l'information;

- définir et instaurer des indicateurs de performance en matière de sécurité de l'information sous forme de tableau de bord sommaire sur l'état de sécurité des actifs et, au besoin, au minimum annuellement, informer le directeur général des ressources informationnelles et le comité sur la sécurité de l'information à ce sujet.

9.10 Détenteurs de l'information

Les détenteurs de l'information sont désignés par le COSI. Leurs noms et les systèmes d'information qui leur sont assignés sont consignés au registre d'autorité.

Tout détenteur de l'information a la responsabilité de :

- participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans en matière de sécurité de l'information;

- catégoriser l'information relevant de sa responsabilité en fonction de sa valeur et selon les critères de disponibilité, d'intégrité et de confidentialité;

- veiller à ce que les mesures de sécurité de l'information adoptées soient mises en place et appliquées et qu'elles répondent adéquatement aux risques encourus;

- agir comme maître d'œuvre des analyses de risques et s'assurer de la prise en charge des risques résiduels;

- veiller au respect du registre d'autorité par les utilisateurs qui relèvent de sa responsabilité.

9.11 Responsable de l'architecture de sécurité de l'information

Le responsable de l'architecture de sécurité de l'information (RASI) a la responsabilité de :

- concevoir et mettre en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;

- arrimer les solutions retenues aux processus organisationnels en matière de sécurité de l'information;

- participer à la conception et à l'évaluation des composantes de sécurité de l'information des solutions conçues ou acquises par BAnQ.

9.12 Responsable de la continuité des services

Le responsable de la continuité des services (RCS) a la responsabilité de :

- coordonner l'élaboration du plan de continuité des services de BAnQ, assurer sa gestion, coordonner sa mise en œuvre et assurer sa mise à jour;

- assurer la planification et la coordination des tests initiaux et récurrents.

9.13 Responsable du développement ou de l'acquisition de systèmes d'information

Le responsable du développement ou de l'acquisition de systèmes d'information (RDASI) a la responsabilité de :

- concevoir, réaliser et documenter les fonctionnalités de sécurité de l'information à intégrer aux systèmes d'information, ainsi qu'en assurer le bon fonctionnement.

9.14 Dirigeants et cadres

Tout dirigeant ou cadre a la responsabilité de :

- voir à l'application de la présente politique au sein de l'unité administrative dont il est responsable;

- sensibiliser les utilisateurs relevant de son autorité à la présente politique et à leurs responsabilités dans ce domaine afin que les exigences en matière de sécurité de l'information soient respectées dans leurs activités quotidiennes, dans tout processus et tout contrat.

De plus, les dirigeants et cadres qui détiennent des renseignements personnels ou confidentiels, notamment les détenteurs de l'information, sont responsables de :

- élaborer des mesures, des mécanismes et des normes visant à protéger ces renseignements dans leurs champs respectifs d'activité, conformément à la Politique sur l'accès à l'information et la protection des renseignements personnels de BAnQ.

9.15 Utilisateurs

Tout utilisateur qui accède à une information est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

Tout utilisateur doit :

- respecter la présente politique ainsi que tout autre élément du corpus règlementaire ou procédure qui en découle;

- respecter les mesures de sécurité de l'information mises en place, sans les contourner, ni modifier leur configuration ou les désactiver;

- informer sans délai la Direction générale des ressources informationnelles de tout incident de sécurité de l'information (piratage d'un système informatique ou intrusion, vol d'identité, utilisation de virus informatique, etc.) dont il a connaissance.

De plus, tout membre du personnel de BAnQ doit :

- signaler sans délai à son supérieur immédiat tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information.

De plus, tout fournisseur ou partenaire externe qui, dans le cadre d'un mandat confié par BAnQ, utilise ses actifs informationnels ou y accède doit :

- respecter et s'assurer que ses employés respectent la présente politique;

- signaler à BAnQ tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information.

10. COMITÉS

10.1 Comité de vérification et des finances

Le comité de vérification et des finances a pour responsabilité de :

- superviser le processus de gestion des risques liés à la sécurité de l'information et surveiller l'application de la politique;

- rendre compte à ce sujet au conseil d'administration lorsque cela est nécessaire.

10.2 Comité sur la sécurité de l'information

Le comité sur la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information à BAnQ.

10.2.1 Composition

Ce comité est présidé par le président-directeur général ou son représentant.

Le président-directeur général nomme les membres de ce comité, qui doit notamment comprendre :

- le directeur général des ressources informationnelles;

- le ROSI;
- le secrétaire général;
- le conservateur et directeur général des Archives nationales;
- le directeur de la vérification interne;
- le directeur de la gestion immobilière et de la sécurité;
- le COSI;
- les détenteurs de l'information.

10.2.2 Mandat

Le comité sur la sécurité de l'information a pour mandat de :

- examiner les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'organisation, ainsi que tout projet ou proposition d'action en sécurité de l'information et formuler des recommandations à ce sujet;
- analyser les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information et formuler des recommandations à ce sujet.

10.3 Comité de continuité des services

10.3.1 Composition

Ce comité est présidé par le responsable de la continuité des services ou son représentant.

Il est composé des membres suivants, auxquels peut s'ajouter toute autre personne dont le comité juge qu'elle est en mesure d'assurer un soutien adéquat dans le cadre de ses prises de décision :

- le responsable organisationnel de la sécurité de l'information;
- le responsable de la continuité des services;
- le conseiller organisationnel en sécurité de l'information;
- les détenteurs de l'information;
- le coordonnateur organisationnel de gestion des incidents.

10.3.2 Mandat

Le comité de continuité des services a pour mandat de :

- procéder à l'évaluation des dommages;

- recommander au comité de crise ministériel l'adoption d'une déclaration de sinistre;
- assurer la mise en œuvre du plan de mobilisation;
- assurer la coordination avec les intervenants extérieurs à BAnQ.

11. TABLEAU DES PRINCIPAUX RÔLES ET RESPONSABILITÉS

	Politique	**Reddition de compte en matière SI**	**Registre d'autorité**	**Tableau de bord de l'état de sécurité des actifs**	**Orientations et stratégies**	**Procédure d'acceptation des risques**	**Autres procédures et directives appropriées**	**Registre d'incidents**	**Processus en matière de sécurité de l'information**
Conseil d'administration (« CA »)	Adopte	Prend acte							Prend acte en matière de gestion des risques
Comité de vérification et des finances (« CVF »)	Surveille son application et rend compte au CA	Prend acte, examine et recommande			Prend acte	Prend acte	Prend acte		Supervise le processus de gestion des risques et rend compte au CA
Conseil de direction	Approuve								
Président-directeur général	Approuve	Supervise	Veille à confection et prend acte		Détermine				
Directeur général des ressources informationnelles (« DGRI »)	Élabore		Informe PDG et CSI	Prend acte	Recommande à ROSI et à CSI	Adopte	Adopte ou voit à adoption par le conseil de direction		Veille à mise en oeuvre
Responsable organisationnel de la sécurité de l'information (« ROSI »)		Élabore et informe le CSI et le CA			Assiste PDG			Prend acte	Veille à mise en oeuvre
Secrétaire général (« SG »)	Appuie le DGRI	Coordonne l'information du CA et du CVF			Coordonne l'information du CA et du CVF	Coordonne l'information du CA et du CVF	Appuie Coordonne l'information du CA et du CVF		Contribue Coordonne l'information du CA et du CVF

	Politique	Reddition de compte en matière SI	Registre d'autorité	Tableau de bord de l'état de sécurité des actifs	Orientations et stratégies	Procédure d'acceptation des risques	Autres procédures et directives appropriées	Registre d'incidents	Processus en matière de sécurité de l'information
Conservateur et directeur général des Archives nationales							Élabore et collabore dans son champ d'intervention		
Directeur de la vérification interne	Observe, évalue et commente				Observe, évalue et commente				
Directeur de la gestion immobilière et de la sécurité							Élabore et collabore dans son champ d'intervention		
Conseiller organisationnel de la sécurité de l'information (« COSI »)	Met en œuvre		Élabore et met à jour	Prépare et informe le CSI et le DGRI	Met en oeuvre	Élabore et met en oeuvre	Élabore et met en oeuvre	Tient à jour et informe le ROSI	Contribue et appuie le ROSI
Détenteurs de l'information	Contribue		Veillent au respect		Participe	Catégorisent information et analysent les risques	Collaborent		
Dirigeants et cadres			Veillent à application						
Comité sur la sécurité de l'information	Examine et recommande	Prend acte, examine et recommande	Prend acte	Prend acte	Prend acte, examine et recommande		Prend acte, examine et recommande		Prend acte, examine et recommande

12. SANCTIONS

12.1 Sanctions applicables

Quiconque contrevient à une disposition de la présente politique est passible de sanctions disciplinaires, administratives ou légales proportionnelles à la gravité de son acte.

12.1.1 Membres du personnel

Dans le cas de membres du personnel, l'application des sanctions prévues au présent article doit se faire conformément aux conventions collectives de travail auxquelles BAnQ est partie ou aux politiques de gestion.

12.1.2 Fournisseurs et partenaires externes

Dans le cas de fournisseurs ou de partenaires externes, BAnQ pourra résilier le contrat qui la lie à ce cocontractant sans intervention judiciaire et intenter des procédures judiciaires afin de réclamer tout dommage, le cas échéant.

12.2 Consultation d'experts et avis aux autorités judiciaires

12.2.1 Les autorités responsables de l'application des sanctions prévues à la présente politique peuvent, si elles le jugent pertinent, s'adjoindre des experts dans des domaines spécifiques, notamment en informatique, afin de faire la lumière sur les faits et circonstances entourant les contraventions à la présente politique.

12.2.2 BAnQ peut transmettre à toute autorité judiciaire les renseignements qui la portent à croire qu'une infraction à une loi en vigueur a été commise.

13. RESPONSABLE DE LA POLITIQUE

Le directeur général des ressources informationnelles est responsable de la mise en œuvre de la présente politique.

14. ENTRÉE EN VIGUEUR ET RÉVISION

14.1 Entrée en vigueur

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration.

14.2 Révision

La révision et la mise à jour de la présente politique sont effectuées au besoin, au minimum tous les trois ans.