Adoption	Résolutions
2007-02-22	CA-257-2505

Modifications	Résolutions
2018-05-28	CA-349-4067

Abrogation	Résolutions

1. Préambule

L'École de technologie supérieure reconnaît que les ressources informationnelles sont au cœur de ses opérations et qu'elles doivent être protégées afin de lui permettre de réaliser sa mission.

La mise en place de mesures relatives à la protection de l'information est donc essentielle et permettra d'assurer la disponibilité, l'intégrité, la confidentialité et le respect du cycle de vie des ressources informationnelles de l'école.

2. Champ d'application

La présente Politique vise les ressources informationnelles, quel que soit leur support et qui:

- Appartiennent à l'ÉTS et sont détenues par elle;
- Appartiennent à l'ÉTS, mais sont détenues par un tiers;
- Utilisées par un tiers et détenues par lui au bénéfice ou pour et au nom de l'ÉTS.

La présente Politique encadre également les actions des Utilisateurs qui ont ou pourraient avoir accès à des ressources informationnelles visées par la présente Politique.

3. Définitions

Ressource informationnelle : Information, quel que soit son canal de communication (téléphone analogique ou numérique, télécopie, voix, etc.) ou son support (papier, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par l'ÉTS.

Catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder en termes de disponibilité, d'intégrité et de confidentialité.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Continuité des services : Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Cycle de vie de l'information : L'ensemble des étapes que franchit une information et qui vont de sa création ou réception, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'ÉTS.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Document : Ensemble constitué d'information portée par un support. L'information est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et 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 transcrits sous l'une de ces formes ou en un autre système de symboles.

Est assimilée au document 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.

Détenteur de l'information : Un employé désigné par le directeur général, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, dont le rôle est, notamment, d'assurer la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

Dirigeant principal de l'information (DPI) : Personne nommée par le gouvernement au sein du Conseil du trésor et dont le rôle et les responsabilités sont énoncés dans la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.*

École de technologie supérieure ou ÉTS : Désigne l'institution d'enseignement et de recherche, ainsi que le CENTECH et toute autre personne morale qui pourraient exister présentement ou dans le futur et qui seraient sous le contrôle de l'ÉTS.

Incident de sécurité de l'information à portée gouvernementale : Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale qui nécessite une intervention concertée sur le plan gouvernemental.

Information : Renseignements consignés sur un support quelconque pour être conservés, traités ou communiqués comme éléments de connaissance.

Intégrité : Fiabilité d'un document, qu'il s'agisse d'un original, d'une reproduction ou d'une représentation comparable, qui garantit que l'information y est demeurée intacte, qu'elle n'a pas été altérée frauduleusement ou par inadvertance.

Plan de continuité : Ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité de l'ÉTS.

Registre d'autorité de la sécurité de l'information : Registre dans lequel sont notamment consignés les noms des détenteurs de l'information, les systèmes qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

Registre d'incident : Recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

Renseignement confidentiel : Renseignements dont l'accès est assorti d'une ou de plusieurs restrictions dont celles prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et qui comprend notamment les renseignements personnels.

Risque de sécurité de l'information : Risque d'interruption ou de réduction de la qualité des services, ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ainsi que sur l'image de l'ÉTS.

Risque de sécurité de l'information à portée gouvernementale : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale, qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

Services communs de sécurité de l'information : Services utilisés par plusieurs organismes publics, dont la gestion est centralisée.

Technologie de l'information : Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Unité : L'un ou l'autre des départements, services administratifs, ainsi que l'une ou l'autre des unités de recherche.

Utilisateur : Toute personne autorisée à accéder à une ressource informationnelle de l'ÉTS ou sous sa responsabilité, notamment les membres du personnel de l'ÉTS, les étudiants, les diplômés, les retraités, les consultants, les fournisseurs et toutes personnes morales qui bénéficient de services provenant de l'ÉTS dont entre autres l'Association des étudiants et des étudiantes de l'ÉTS, Réseau ÉTS, le CENTECH, les syndicats affiliés et la COOP.

4. Cadre légal

La présente Politique est adoptée en vertu de l'article 7a) de la *Directive sur la sécurité de l'information gouvernementale*, qui découle de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du Gouvernement*, RLRQ C. G-1.03.

Elle s'inscrit dans un contexte régit plus largement par :

- La *Loi concernant le cadre juridique des technologies et l'information*, RLRQ, ch. C-1.1;
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, ch. A-2.1;
- La *Loi sur les archives*, RLRQ, ch. A-21.1;

- Le *Cadre gouvernemental de gestion de la sécurité de l'information* (juin 2014);
- Le *Règlement relatif à la gestion des documents et des archives* de l'ÉTS;
- Le *Règlement sur la sécurité des personnes, des biens et des STI* de l'ÉTS;
- La *Politique sur les données institutionnelles* de l'ÉTS;
- La *Directive sur la divulgation de renseignements confidentiels en vue d'assurer la protection des personnes* de l'ÉTS.

5. Objectif

La présente Politique a pour objectif d'assurer la sécurité de l'information tout au long de son cycle de vie, et plus précisément :

- d'assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- d'assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- de limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité lorsque requis;
- de permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif;
- de permettre l'attribution des rôles et responsabilités des différents intervenants en matière de sécurité de l'information à l'ÉTS, en conformité avec le cadre gouvernemental de gestion de la sécurité de l'information.

Elle a de plus pour objectif d'assurer le respect des principes directeurs de la sécurité de l'information gouvernementale et leur intégration dans les documents normatifs encadrant la sécurité de l'information et qui sont :

- **Rôles et responsabilités** : L'efficacité des mesures de sécurité de l'information exige l'attribution claire de rôles et de responsabilités aux différents intervenants et une reddition de comptes adéquate.
- **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, ainsi que de l'évolution des menaces et des risques.
- **Universalité** : Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.
- **Éthique :** Le cadre de gestion de la sécurité de l'information doit reposer sur des considérations éthiques visant à assurer la régulation des conduites et la responsabilisation individuelle.

6. Mise en œuvre de la gestion de la sécurité de l'information

Le directeur du Service des technologies de l'information élabore un cadre de gestion de la sécurité de l'information, composé principalement de directives et de procédures adoptées par les instances appropriées, et qui permet :

- la mise en œuvre des processus formels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès et la gestion des incidents;
- d'encadrer les déclarations devant être effectuées au DPI et au CERT/AQ;
- d'assurer la réalisation d'audits de sécurité et de tests d'intrusion et de vulnérabilité;
- d'assurer la mise en place d'un registre d'autorité de la sécurité de l'information;
- d'assurer l'intégration dans les ententes et contrats conclus par l'ÉTS de clauses garantissant le respect d'exigences de sécurité de l'information;
- de favoriser l'utilisation de services communs de sécurité de l'information déterminés par le Conseil du trésor;
- de définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.

7. Rôles et responsabilités des principaux intervenants

7.1 Dirigeant de l'organisme public

Le directeur général occupe la fonction de dirigeant de l'organisme public.

En tant que premier responsable de la sécurité de l'information relevant de son autorité, il doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor. À ce titre, il :

- s'assure de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par l'organisation ;
- s'assure de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- désigne les Détenteurs de l'information.

7.2 Responsable Organisationnel de la Sécurité de l'information (ROSI)

Le directeur du développement stratégique et des ressources ou son mandataire assume le rôle de Responsable Organisationnel de la Sécurité de l'information (ROSI) au sein de l'ÉTS. Il joue ainsi le rôle de porte-parole du Dirigeant Principal de l'Information (DPI). Il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information. Il assiste le dirigeant de l'organisme public pour ce qui est de la détermination des orientations stratégiques et des priorités d'intervention. De plus, il le représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. En collaboration avec le secrétaire général, il a, en outre, comme responsabilités :

- de soumettre à la consultation du comité chargé de la sécurité de l'information, les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information ;
- d'assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein de l'ÉTS par d'autres intervenants dont les Détenteurs de l'information, ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique ;
- de s'assurer de la contribution de son organisation au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale ;
- de définir et de mettre en oeuvre les 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 gouvernementale ;
- de s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information ;
- de coordonner l'élaboration et la mise en oeuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information.

7.3 Conseiller organisationnel en sécurité de l'information

Le directeur du Service des technologies de l'information, ou son mandataire, assume le rôle de conseiller organisationnel en sécurité de l'information (COSI). Il apporte son soutien au ROSI en contribuant notamment à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus de sécurité de l'information.

À titre de COSI, il a en outre comme responsabilités :

- de mettre en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard ;
- de produire les bilans et les plans d'action de sécurité de l'information ;
- de participer aux négociations des ententes de service et des contrats et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information ;
- de tenir à jour le registre d'autorité de la sécurité de l'information ;
- d'assister les Détenteurs de l'information dans le processus de catégorisation de l'information relevant de leur responsabilité, en collaboration avec le Bureau de la gestion des documents et des archives ;
- d'assister les Détenteurs de l'information dans la réalisation des analyses de risques de sécurité de l'information ;
- de contribuer à la mise en œuvre des processus officiels de sécurité de l'information de son organisation.

7.4 Coordonnateur organisationnel de gestion des incidents (COGI)

Le responsable Conception de solutions-client assume le rôle de conseiller organisationnel de gestion des incidents (COGI). Il participe également de manière active au réseau d'alerte gouvernemental.

À titre de COGI, il a en outre comme responsabilités :

- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information;
- de s'assurer de la coordination des membres CERT/AQ qui lui sont rattachés et de mettre en oeuvre les stratégies de réaction appropriées ;
- de contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en oeuvre les solutions appropriées ;
- de contribuer à la mise en oeuvre du processus gouvernemental de gestion des incidents de sécurité de l'information ;
- d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications ;
- de collaborer étroitement avec le ROSI et de lui fourni le soutien technique nécessaire à l'exercice de ses responsabilités.

8. Rôles et responsabilités des autres intervenants

8.1 Cadres supérieurs

Les cadres supérieurs ou leurs mandataires assument la fonction de Détenteurs de l'information. Ils sont à ce titre notamment chargés 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 ;
- catégoriser l'information relevant de leur responsabilité selon sa valeur au niveau de la disponibilité, de l'intégrité et de la confidentialité ;
- veiller à ce que les mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées ;
- s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels.

8.2 Bureau de la gestion documentaire et des archives

Le responsable du Bureau de la gestion documentaire et des archives agit comme responsable de la gestion documentaire. À ce titre il :

- collabore à la conception des systèmes informatiques, administratifs ou autres et s'assure 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 ;
- collabore étroitement avec les Détenteurs de l'information ainsi qu'avec le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en oeuvre des mesures de sécurité de l'information, indépendamment de son support;
- assiste les Détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité en collaboration avec l'officier de la sécurité de l'information;
- détermine les normes de mise au rebut sécuritaire des supports de l'information.

8.3 Secrétaire général

Le secrétaire général ou son mandataire, agit à titre de responsable de l'accès à l'information et de la protection des renseignements personnels.

Il veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. À ce titre, il :

- communique au ROSI les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles ;
- contribue à assurer la cohérence et l'harmonisation des interventions avec 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 à portée gouvernementale;
- veille 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.

8.4 Bureau de la prévention et de la sécurité

Le responsable de la prévention et de la sécurité veille à la mise en place des mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Plus particulièrement, il :

- conçoit et met en oeuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de son organisation ;
- élabore et met en oeuvre des procédures et directives propres à son domaine d'intervention.

8.5 Service de la gestion des actifs immobiliers

Le directeur du Service de la gestion des actifs immobiliers voit à la disposition sécuritaire des supports de l'information. À ce titre, il :

- s'assure de la mise au rebut sécuritaire des supports de l'information selon les normes établies par le Bureau de la gestion des documents et des archives ;
- élabore et met en œuvre des procédures et directives propres à son domaine d'intervention.

8.6 Service des technologies de l'information

Le Service des technologies de l'information remplit plusieurs fonctions dans le cadre de la mise en place de mesures de sécurité de l'information.

8.6.1 Gestion des technologies de l'information

- contribue à l'élaboration et à la mise en oeuvre de directives qui visent à assurer la sécurité de l'information numérique ;
- met en oeuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par son organisation, dont les plans de reprise informatique en cas de sinistre ;
- met en place un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

8.6.2 Développement ou de l'acquisition de systèmes d'information

En collaboration avec le Service des affaires juridiques et le Bureau de la gestion des documents et des archives, conçoit, réalise et documente les fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, à intégrer aux systèmes d'information. Il s'assure également de leur bon fonctionnement.

8.6.3 Architecture de sécurité de l'information

- conçoit et met en oeuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information ;
- arrime les solutions retenues aux processus organisationnels de sécurité de l'information ;
- participe à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires développées ou acquises par son organisation.

9. Vérification interne

Le directeur du développement stratégique et des ressources ou son mandataire évalue, examine ou vérifie, notamment :

- l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre ;
- l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

10. Utilisateurs

Tout Utilisateur qui interagit avec des ressources informationnelles est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

À cette fin, il doit :

- se conformer à la présente Politique et au cadre de gestion de la sécurité de l'information qui en découle ;
- utiliser les droits d'accès qui lui sont attribués et les ressources informationnelles mises à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés ;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ou les désactiver ;
- signaler au Service des technologies de l'information tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information de l'ÉTS, selon les procédures établies dans le cadre de la gestion de la sécurité de l'information.

11. Comités

11.1 Comité chargé de la sécurité de l'information

Le Comité chargé de la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information à l'ÉTS.

11.1.1 Mandat

Le mandat de ce comité est :

- d'examiner et formuler des recommandations concernant les orientations, les politiques, les directives, les procédures, les cadres de gestion, les plans d'action et les bilans de l'organisation, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information ;
- d'analyser et formuler des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'ÉTS.

11.1.2 Composition

Ce comité est présidé par le directeur général ou son mandataire.

Les membres sont :

- Le ROSI ou son mandataire ;
- Le COSI ou son mandataire ;
- Le secrétaire général ;
- Les Détenteurs de l'information ;
- Un représentant des unités responsables des ressources informationnelles visées ;
- Un représentant du Service des technologies de l'information ;
- Un représentant pour l'accès à l'information et de la protection des renseignements personnels ;
- Le responsable du Bureau de la gestion des documents et des archives ou son mandataire
- Le responsable du Bureau de la prévention et de la sécurité ou son mandataire.

11.2 Comité de crise ministériel

En cas d'incident critique de sécurité de l'information, le Comité de crise ministériel est le groupe décisionnel appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services.

Le Comité de gestion de crise (CGC) prévu au Plan des mesures d'urgence de l'ÉTS agit comme Comité de crise ministériel.

11.2.1 Mandat

Le mandat de ce comité est:

- de mettre en œuvre le Plan des mesures d'urgence lorsque requis ;
- d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information ;
- d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants ;
- de décider du déploiement ou non des plans de continuité des services ;
- de proposer des orientations à suivre ou des actions à poser en cas de sinistre ;
- de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation ;
- de communiquer avec les médias.

11.2.2 Composition

Ce comité est présidé par le directeur général ou son mandataire.

Les membres sont ceux du Comité de gestion de crise (CGC) prévu au Plan des mesures d'urgence, auxquels s'ajoutent :

- Le responsable de la protection des renseignements personnels ;
- Le responsable de la prévention et de la sécurité ou son mandataire ;
- Le directeur du Service des communications ;
- Un représentant du Service des technologies de l'information.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision.

11.3 Comité de continuité des services d'un organisme public

Ce comité se réunit lorsqu'un incident survient.

11.3.1 Mandat

Le mandat de ce comité en cas d'incident est :

- de procéder à l'évaluation des dommages ;
- de recommander au Comité de crise ministériel l'adoption d'une déclaration de sinistre ;
- d'assurer la mise en oeuvre du plan de mobilisation ;
- d'assurer la coordination avec les intervenants de l'extérieur de l'ÉTS.

11.3.2 Composition

Ce comité est présidé par le ROSI.

Les membres sont :

- Les Détenteurs de l'information ;
- Le COSI ;
- Le COGI.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision. Il est présidé par le responsable de la continuité des services ou son mandataire.

12. Sanctions

Toute personne qui contrevient au cadre légal, à la présente Politique, au cadre de gestion de la sécurité de l'information qui en découle et aux mesures de sécurité de l'information en vigueur s'expose à des sanctions administratives ou disciplinaires.

13. Diffusion et mise à jour

Le secrétaire général est responsable de la diffusion et de la mise à jour de la présente Politique.

14. Dispositions finales

La présente Politique entre en vigueur à la date de son adoption par le conseil d'administration.