Centre de services scolaire des Découvreurs Québec	MANUEL DE GESTION	CODIFICATION Nº 03.11.11
ENTRÉE EN VIGUEUR 29 mai 2019	**SECTEUR** Direction générale	**NATURE** Politique
APPROBATION Par : C.C. Date : 28 mai 2019		**AMENDEMENT** 27 octobre 2026 (C.A.)

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

1. PRÉAMBULE

Les encadrements légaux et réglementaires en matière de sécurité de l'information imposent des obligations importantes aux organismes publics, notamment aux centres de services scolaires. Afin de se conformer à ces exigences, le Centre de services scolaire des Découvreurs (ci-après le « CSSDD ») adopte la présente Politique, en assure la mise en œuvre, la mise à jour et l'application. Les dispositions de cette Politique sont complétées par un Cadre de gestion de la sécurité de l'information définissant les processus et les mécanismes nécessaires pour assurer une gestion efficace et conforme de la sécurité de l'information au sein de l'organisation.

Le CSSDD reconnaît que l'information et les technologies qui la soutiennent constituent des ressources stratégiques essentielles à la réalisation de sa mission et à la prestation de ses services. En raison de leur valeur administrative, juridique et financière, les actifs informationnels doivent faire l'objet d'une évaluation continue et de mesures de protection adaptées tout au long de leur cycle de vie.

Une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces actifs peut avoir des répercussions sur la vie, la santé ou le bien-être des personnes, compromettre la protection des renseignements personnels et le respect de la vie privée, nuire à la prestation des services à la population ainsi qu`à la réputation du CSSDD et du gouvernement.

2. OBJECTIFS

La présente Politique établit les orientations générales en matière de gestion des actifs informationnels, dans le respect des droits et obligations du CSSDD pour contribuer à l'atteinte des objectifs de sécurité de l'information et plus spécifiquement pour:

- Assurer la protection des actifs informationnels tout au long de leur cycle de vie, quel que soit le support ou l'emplacement;

- Préserver la confidentialité de l'information en veillant à ce qu'elle ne soit ni accessible ni divulguée à des personnes non autorisées;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation;
- Assurer la disponibilité de l'information pour qu'elle soit accessible au moment opportun et utilisable par les personnes autorisées;
- Assurer une gestion proactive des risques de cybersécurité afin de prévenir, détecter et répondre aux cybermenaces susceptibles d'affecter les actifs informationnels du CSSDD;
- Établir les lignes directrices, les rôles et les responsabilités des intervenants en matière de sécurité de l'information;
- Identifier et classifier les actifs informationnels selon leur niveau de criticité et en assurer l'évaluation continue et la protection appropriée;
- Assurer la conformité aux lois, règlements et autres encadrements applicables;
- Assurer le respect de la vie privée des individus en protégeant adéquatement leurs renseignements personnels;
- Promouvoir une culture organisationnelle axée sur la sécurité de l'information.

3. CADRE LÉGAL ET NORMATIF

Le présent document repose sur des fondements légaux et normatifs, tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

La Politique relative à la sécurité de l'information s'inscrit principalement dans un contexte régi par :

- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03);
- *La Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1);
- La *Loi sur l'instruction publique* (RLRQ, c. I-13.3);
- La *Loi sur les archives* (RLRQ, chapitre A-21.1);
- La *Directive gouvernementale sur la sécurité de l'information* (Gouvernement du Québec 2021);
- Le *Cadre gouvernemental de gestion de la sécurité de l'information* (Gouvernement du Québec 2021);
- La *Politique gouvernementale de cybersécurité* (Gouvernement du Québec, 2020);
- Le *Règlement sur les incidents de confidentialité* (RLRQ, A-2.1, r. 3.1);
- La *Charte des droits et libertés de la personne* (RLRQ, c. C-12);
- Le *Code civil du Québec* (RLRQ, c. CCQ-1991);
- Le *Code criminel* (L.R.C 1985, c. C-46);

- Le *Modèle de classification de sécurité des données numériques gouvernementales* (Gouvernement du Québec, 2024);
- Le Cadre de gestion de la sécurité de l'information – CSSDD;
- Toute autre loi, règlement, directive ou norme applicable.

4. DÉFINITION

Actif informationnel

Information, document, système d'information, équipement informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitué par le CSSDD pour mener à bien sa mission, quel que soit leur support de conservation électronique, technologique ou papier.

Code d'accès

Mécanisme d'identification et d'authentification permettant d'identifier de façon unique un utilisateur et de valider son identité lors de l'accès à un actif informationnel au moyen d'un identifiant, d'un mot de passe ou de tout autre dispositif d'authentification**.**

Confidentialité

Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

Cybersécurité

Capacité, pour un système en réseau, de se protéger et de résister à des événements de sécurité de l'information et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient.

Cycle de vie de l'information

Ensemble des étapes que parcourt une information, de sa création 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 du CSSDD.

Disponibilité

Propriété qu'ont les données, l'information et les systèmes d'information et de communication, d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Incident de sécurité de l'information

Événement avéré où une menace a exploité une vulnérabilité, causant un impact négatif sur la confidentialité, l'intégrité ou la disponibilité des informations. C'est la matérialisation d'un risque, pouvant entraîner des perturbations, des pertes ou des violations des actifs informationnels.

Intégrité

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiées, ni altérées, ni détruites sans autorisation.

Risques liés à la sécurité de l'information

Tout événement lors du traitement, l'utilisation ou l'entreposage comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, l'intégrité et la disponibilité de l'information et causer un préjudice.

Système d'information

Système constitué d'actifs informationnels et des procédures permettant d'acquérir, de conserver, de traiter et de diffuser les éléments d'information pertinents au fonctionnement du CSSDD.

Technologies de l'information

Regroupent les techniques, principalement, de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.

5. CHAMP D'APPLICATION

Personnes visées :

La présente Politique vise, sans exception, toute personne physique ou morale appelée à utiliser les actifs informationnels du CSSDD, notamment :

- Le personnel à l'emploi du CSSDD;
- Les élèves inscrits au CSSDD et, le cas échéant, leurs parents ou titulaires de l'autorité parentale;
- Les membres des instances et des comités du CSSDD;
- Les stagiaires, les bénévoles, les consultants, les partenaires, les fournisseurs et tout autre tiers œuvrant pour le CSSDD.

Actifs visés :

Cette Politique vise tous les actifs informationnels :

- Appartenant au CSSDD;
- Détenus, utilisés ou administrés par un tiers pour le compte ou au nom du CSSDD ;
- Quel que soit le support de conservation électronique, technologique ou papier.

Activités visées :

Cette Politique concerne l'ensemble des activités entrant dans le cycle de vie de l'information, à savoir : la création, la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des actifs informationnels du CSSDD qu'elles soient réalisées dans les locaux du CSSDD, dans un autre endroit ou à distance.

6. RÔLES ET RESPONSABILITÉS

La présente Politique attribue la gestion de la sécurité de l'information à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

Conseil d'administration

Le Conseil d'administration adopte la Politique relative à la sécurité de l'information. Il prend connaissance annuellement des redditions de comptes relatives à la sécurité de l'information**.**

Direction générale

La direction générale assume la responsabilité première de la sécurité de l'information au sein de l'organisation. À ce titre, elle est responsable de l'application de la présente politique. Elle veille à la mise en place d'une gouvernance efficace en matière de sécurité de l'information et s'assure que les mesures requises sont déployées afin de satisfaire aux exigences légales, réglementaires et gouvernementales.

Elle soumet à l'approbation du Bureau de direction les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans ainsi que les redditions de comptes en matière de sécurité de l'information.

Elle désigne le chef de la sécurité de l'information organisationnelle (CSIO) et le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI), auxquels elle confie les responsabilités prévues à leur mandat respectif.

Chef de la sécurité de l'information organisationnelle (CSIO)[1]

Le chef de la sécurité de l'information organisationnelle assume la responsabilité de la gestion globale de la sécurité de l'information au sein du CSSDD. Il conseille la direction générale sur les enjeux et les orientations en matière de sécurité de l'information. Il élabore et recommande les stratégies, les cadres de gestion, les directives et les mesures visant à assurer la sécurité des actifs informationnels de l'organisation. Il recommande à la Direction générale toute modification requise à la présente politique lorsque le contexte l'exige.

Il met en œuvre les décisions émanant du Chef gouvernemental de la sécurité de l'information (CSGI) et veille à l'application des encadrements en vigueur. Il assure le suivi des risques, des incidents de sécurité et des plans d'amélioration et en rend compte à la Direction générale.

Le Chef de la sécurité de l'information organisationnelle (CSIO) est responsable de la diffusion de la présente Politique.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI agit sur le plan opérationnel. Il intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO de l'organisation, plus particulièrement en matière de

[1] Annexe 1 : La structure de gouvernance de la sécurité de l'information gouvernementale

gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente l'organisation auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) au CSSDD en soutien au CSIO. Il collabore avec le CSIO de son organisation à l'élaboration des divers éléments stratégiques et tactiques en sécurité de l'information.

Comité de sécurité de l'information

Le Comité de sécurité de l'information assiste le Chef de la sécurité de l'information organisationnelle (CSIO) dans la mise en œuvre de la gouvernance de la sécurité de l'information et des mesures requises pour assurer la protection des actifs informationnels du CSSDD. Il agit également comme instance de concertation et de recommandation auprès du CSIO.

Plus particulièrement, le Comité prend connaissance des orientations, politiques, directives, cadres de gestion, plans d'action, bilans, projets et initiatives en matière de sécurité de l'information. Il examine les actions proposées, en valide la pertinence et la faisabilité dans le contexte organisationnel et formule, au besoin, des recommandations afin de soutenir leur mise en œuvre. Il favorise également l'adhésion des différents milieux aux initiatives de sécurité de l'information.

Le Comité est informé des principaux enjeux liés à la sécurité de l'information, notamment les vulnérabilités, les incidents de sécurité et toute autre situation susceptible d'affecter la protection des actifs informationnels. À cet égard, il contribue à l'analyse de ces enjeux et formule des recommandations visant à soutenir la prise de décision et l'amélioration continue des pratiques en matière de sécurité de l'information.

Il participe également à la planification et au suivi des activités de sensibilisation, de formation et des campagnes de simulation d'hameçonnage destinées à promouvoir une culture de sécurité de l'information au sein de l'organisation.

Le responsable de la protection des renseignements personnels (RPRP)

Le RPRP veille au respect des lois applicables en matière de protection des renseignements personnels. Il met en œuvre les politiques et pratiques de gouvernance des renseignements personnels et assure la gestion des incidents de confidentialité.

Direction du secrétariat général et des communications

La Direction valide la Politique relative à la sécurité de l'information et contribue à sa mise à jour en fonction des exigences légales, réglementaires et organisationnelles.

Elle assure la gouvernance de l'information en matière de gestion documentaire et de cycle de vie de l'information. À ce titre, elle veille à l'application du calendrier de conservation, des règles de gestion documentaire ainsi que des mécanismes encadrant la conservation, le transfert, l'archivage et la destruction de l'information.

Elle coordonne la classification des actifs informationnels afin d'assurer leur gestion adéquate tout au long de leur cycle de vie et l'application des mesures de protection requises.

Direction du service des technologies de l'information

La Direction du service des technologies de l'information contribue à la mise en œuvre de la présente Politique et des mesures de sécurité de l'information relevant de ses responsabilités. Elle veille à l'intégration des exigences de sécurité de l'information dans l'exploitation, l'acquisition, le développement et l'évolution des systèmes d'information.

À ce titre, elle :

- Collabore avec le CSIO à l'identification des risques, des vulnérabilités, des menaces et des besoins en matière de sécurité de l'information;
- Met en œuvre les mesures administratives, physiques et technologiques requises pour protéger les systèmes d'information;
- Assure la prévention, la détection, la gestion et le traitement des incidents de sécurité de l'information relevant de son champ de responsabilité;
- Applique les mesures de réaction appropriées lors d'une menace ou d'un incident, y compris l'interruption ou la suspension temporaire de services ou de systèmes d'information lorsque la situation l'exige;
- Fournit l'expertise et le soutien technique requis à la Direction générale ou à la Direction du Service des ressources humaines dans le traitement des situations impliquant une contravention réelle ou présumée à la présente Politique.

Direction du service des ressources humaines

En matière de sécurité de l'information, la Direction doit :

- S'assurer que les employés ont été informés de l'existence de cette Politique et de l'obligation de s'y conformer;
- Contribuer à la sensibilisation et à la formation des membres du personnel en matière de sécurité de l'information;
- Imposer les sanctions appropriées lors de la violation des politiques, règlements, directives et codes de conduite touchant à la sécurité de l'information.

Direction du service des ressources matérielles

La Direction du Service des ressources matérielles participe, en collaboration avec le CSIO, à l'identification et à l'évaluation des risques liés aux infrastructures physiques. Elle contribue à la mise en œuvre des mesures de sécurité physique nécessaires à la protection des actifs informationnels du CSSDD.

Gestionnaire – Responsable d'actifs informationnels

Le gestionnaire détenant l'autorité au sein de son unité est le responsable des actifs informationnels. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité. Le responsable doit :

- Informer et sensibiliser à la présente Politique le personnel relevant de son autorité, ainsi que toute autre personne ayant accès aux actifs informationnels sous sa responsabilité, notamment les consultants, les partenaires et les fournisseurs et s'assurer de leur compréhension ainsi que de leur adhésion;
- S'assurer de la participation des employés aux activités de formation et de sensibilisation en matière de sécurité de l'information;
- S'assurer que les droits d'accès aux systèmes d'information dont il est responsable sont accordés, modifiés et révoqués selon les fonctions exercées;
- Participer activement aux activités de révision périodique des accès et en confirmer la pertinence, l'exactitude et le maintien;
- Participer à la classification de l'information relevant de son unité et à l'analyse des risques;
- S'assurer que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité;
- Signaler tout événement, incident ou menace liés à la sécurité de l'information;
- Intervenir auprès du personnel en cas de pratiques non conformes;
- Collaborer à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information;
- Soutenir une culture de sécurité de l'information en encourageant les comportements sécuritaires et en intégrant la sécurité de l'information aux pratiques quotidiennes de travail.

Utilisateurs

La responsabilité de la sécurité de l'information au CSSDD incombe à tous les utilisateurs des actifs informationnels. Toute personne qui accède à une information, la consulte ou la traite est responsable de l'utilisation qu'elle en fait et doit prendre les mesures nécessaires pour en assurer la protection.

À cette fin, l'utilisateur doit :

- Se conformer à la présente Politique et à toute autre directive du CSSDD en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- Préserver la confidentialité de ses renseignements d'authentification, notamment son identifiant, son code d'accès et son mot de passe, et ne pas les divulguer, les partager ou permettre leur utilisation par une autre personne.
- Utiliser uniquement les droits d'accès qui lui sont attribués ainsi que les informations et les systèmes d'information mis à sa disposition, dans le cadre de ses fonctions et aux fins pour lesquelles ils lui sont accordés;
- Participer, au besoin, à la classification de l'information de son secteur;
- Signaler sans délai à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant compromettre la protection des actifs informationnels du CSSDD;

- Respecter les mesures de sécurité mises en place, ne pas les contourner, les modifier ou les désactiver ;
- Collaborer à toute intervention visant à identifier, signaler, gérer ou atténuer une menace ou un incident de sécurité de l'information.

7. PRINCIPES DE SÉCURITÉ DE L'INFORMATION

La sécurité de l'information repose sur trois principes fondamentaux : la confidentialité, l'intégrité et la disponibilité de l'information.

- Confidentialité : La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. Elle a pour but de s'assurer qu'une information ou une donnée est accessible uniquement par les personnes autorisées. La confidentialité de l'information doit aussi être assurée tout au long de son cycle de vie. Afin de garantir la confidentialité, des mesures de contrôle doivent être mises en place.

- Intégrité : L'intégrité des données consiste à garantir que les données n'ont été modifiées d'aucune façon au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'intégrité des données, des mesures de sécurité physiques et d'accès logiques doivent être mises en place.

- Disponibilité : La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès opportun et ininterrompu aux informations contenues dans ce système ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière requise par un utilisateur autorisé. Afin d'aider à assurer cette disponibilité, des mesures de contrôles doivent être mises en place.

8. CLASSIFICATION DES ACTIFS INFORMATIONNELS

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie, raison pour laquelle il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation. La classification des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des actifs dans le but d'en déterminer le niveau de protection. Cette classification est réalisée conformément au Modèle de classification de sécurité des données numériques gouvernementales. Une réévaluation de la classification attribuée doit être effectuée de façon périodique par le responsable de l'actif.

9. CADRE DE GESTION

La présente Politique est soutenue par un Cadre de gestion de la sécurité de l'information qui définit l'organisation de la sécurité de l'information au sein du CSSDD ainsi que les mécanismes nécessaires à sa mise en œuvre. Ce cadre comprend, entre autres, les volets suivants :

- La gestion des identités et des accès (GIA);
- La gestion des vulnérabilités;
- La gestion des risques;
- La gestion des incidents;
- La gestion de la reprise et de la continuité des activités.

10. FORMATION ET SENSIBILISATION

La sécurité de l'information repose, entre autres, sur l'adoption de comportements sécuritaires et la responsabilisation individuelle. À cet égard, tous les utilisateurs doivent être formés et sensibilisés :

- À la sécurité de l'information et à l'utilisation sécuritaire des actifs informationnels du CSSDD;
- Aux conséquences d'une atteinte à la sécurité des actifs informationnels;
- À leur rôle et à leurs responsabilités en la matière.

Le CSSDD s'engage à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière. L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation.

11. SANCTIONS

Tout employé qui contrevient au cadre légal, à la présente Politique ou aux mesures de sécurité de l'information qui en découlent s'expose à des sanctions déterminées selon la nature, la gravité et les conséquences de la contravention, en vertu de la législation, des conventions collectives pour le personnel syndiqué et des règlements sur les conditions de travail pour le personnel cadre.

Les élèves de tous les niveaux d'enseignement sont également assujettis à la présente Politique. En cas de non-respect de celle-ci, ils peuvent faire l'objet de mesures conformément aux règles de conduite en vigueur dans leur établissement.

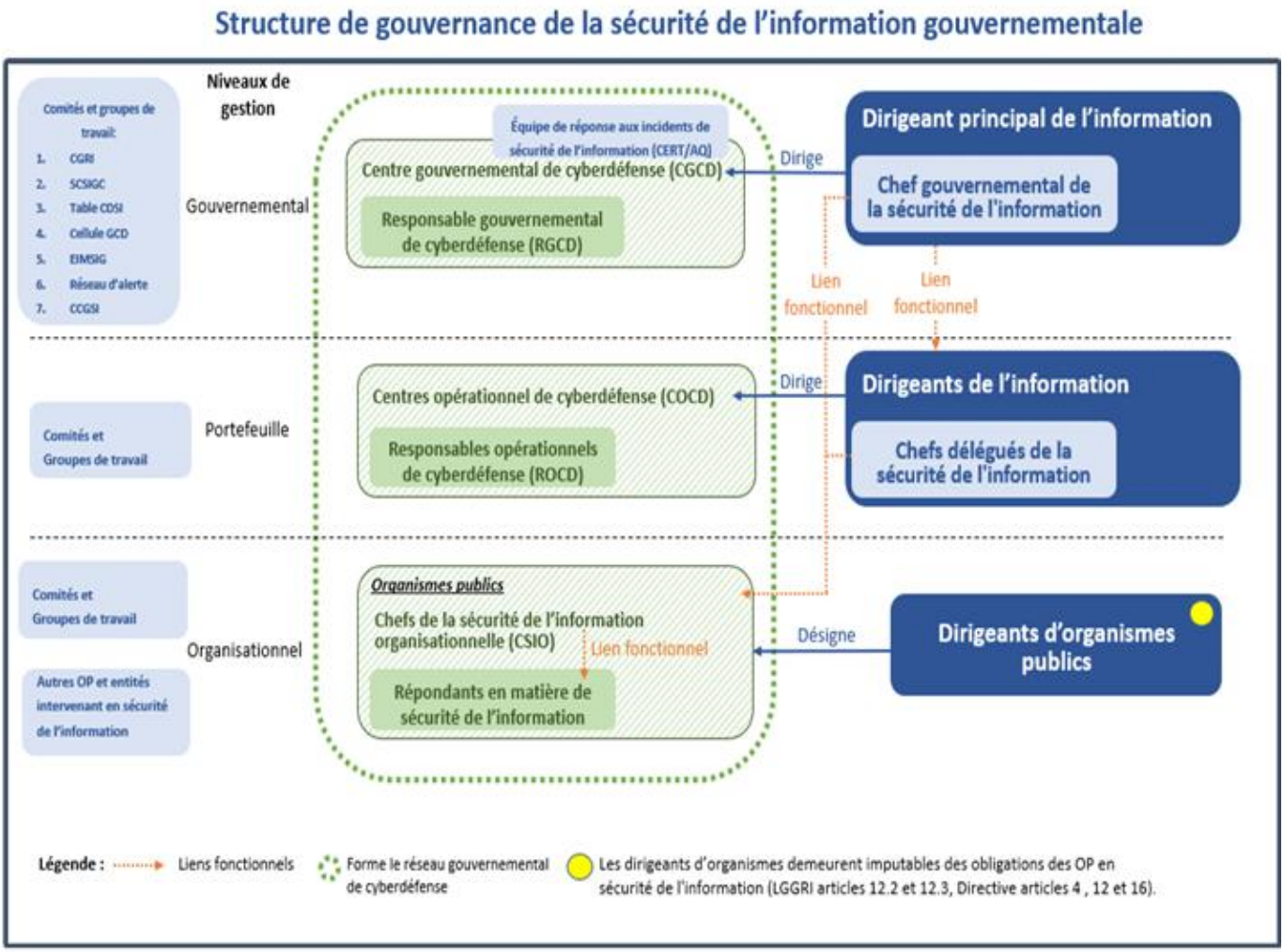
Toute autre personne visée par la présente Politique est passible des sanctions prévues en vertu des dispositions de la législation applicable en la matière.

12. ENTRÉE EN VIGUEUR

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

ANNEXE 1 – Structure de gouvernance de la sécurité de l'information gouvernementale

Figure 1



Source : Gouvernement du Québec, *Cadre gouvernemental de gestion de la sécurité de l'information (2021)*.