A.M., 2024

Arrêté numéro 2024-05 du ministre de la Cybersécurité et du Numérique en date du 12 décembre 2024

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
(chapitre G-1.03)

CONCERNANT le Modèle de classification de sécurité des données numériques gouvernementales

LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE,

VU le paragraphe 3° de l'article 12.6 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) suivant lequel le chef gouvernemental de la sécurité de l'information assume la responsabilité d'établir le modèle de classification de sécurité des données numériques gouvernementales en fonction de leur nature, de leurs caractéristiques, de leur utilisation et des règles qui les régissent, et de le faire approuver par le ministre;

VU que le chef gouvernemental de la sécurité de l'information a, le 12 décembre 2024, établi ce modèle;

VU le deuxième alinéa de l'article 21 de cette loi suivant lequel le ministre de la Cybersécurité et du Numérique peut déterminer des orientations portant sur les principes ou les pratiques à appliquer en matière de gestion des ressources informationnelles, incluant les pratiques pour optimiser l'organisation du travail de même que la nécessité de considérer l'ensemble des technologies offrant un potentiel d'économies ou de bénéfices et des modèles de développement ou d'acquisition disponibles pour répondre aux besoins des organismes publics, dont les logiciels libres;

CONSIDÉRANT qu'il y a lieu, pour le ministre de la Cybersécurité et du Numérique, d'approuver le Modèle de classification de sécurité des données numériques gouvernementales, annexé au présent arrêté, et de déterminer des orientations concernant la classification des données numériques gouvernementales, soient celles déterminées dans ce modèle;

ARRÊTE CE QUI SUIT :

APPROUVE le Modèle de classification de sécurité des données numériques gouvernementales, annexé au présent arrêté.

DÉTERMINE des orientations concernant la classification de sécurité des données numériques gouvernementales, soient celles déterminées dans ce modèle.

Québec, le 12 décembre 2024

Le ministre de la Cybersécurité et du Numérique,
ÉRIC CAIRE

Modèle de classification de sécurité des données numériques gouvernementales

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
(chapitre G-1.03, a. 12.6, par. 3).

CHAPITRE I
DISPOSITIONS INTRODUCTIVES

1. Le présent modèle de classification de sécurité des données numériques gouvernementales permet aux organismes publics de classifier les données numériques gouvernementales qu'ils détiennent afin de leur accorder un niveau de sécurisation adéquat.

Il est au cœur de la démarche globale de sécurisation des données numériques gouvernementales permettant aux organismes publics de réduire, autant que possible, les risques d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de telles données.

Il prend appui sur une analyse des préjudices advenant un bris de confidentialité, d'intégrité ou de disponibilité aux données numériques gouvernementales et tient compte de la nature de ces données, de leurs caractéristiques, de leur utilisation de même que des règles qui les régissent, notamment celles prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

2. Le présent modèle s'inscrit plus généralement dans l'encadrement optimal de la sécurité de l'information et vise les objectifs suivants :

1° soutenir la politique gouvernementale en matière de sécurité de l'information en vigueur, incluant toute modification à celle-ci;

2° assurer une classification uniforme pour l'ensemble des organismes publics à l'aide d'un modèle commun et, conséquemment, une sécurisation adéquate des données numériques gouvernementales à l'échelle de l'Administration publique;

3° faciliter une interopérabilité avec d'autres acteurs de l'écosystème de la sécurité de l'information sur le plan national ou international.

3. Dans le présent modèle, on entend par :

1° « donnée » : toute donnée numérique gouvernementale au sens du paragraphe 1° de l'article 12.10 de la Loi;

2° « donnée non structurée » : donnée stockée sans être organisée de manière prédéfinie, ce qui rend son utilisation plus difficile pour un système d'information, telle une donnée contenue dans un document généré au moyen d'un outil bureautique ou du courrier électronique;

3° « donnée structurée » : une donnée stockée selon un format prédéfini de façon à permettre son interprétation par un logiciel, telle une donnée stockée dans une base de données utilisée par différents systèmes d'information;

4° « Loi » : la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);

5° « objectifs de sécurité » : la confidentialité, l'intégrité et la disponibilité, étant les trois objectifs pour assurer le niveau de sécurité attendu au regard des données.

4. Le présent modèle s'applique aux organismes publics visés à l'article 2 de la Loi.

CHAPITRE II
DÉMARCHE GLOBALE DE SÉCURISATION DES DONNÉES

5. La démarche globale de sécurisation des données que doit suivre un organisme public repose sur l'identification de ses besoins de sécurité et la réalisation des activités suivantes :

1° la classification de sécurité des données conformément au chapitre III;

2° pour chaque donnée visée par un profil de mesures de sécurité ou un marquage, l'application des mesures de sécurité adéquates, notamment celles prévues aux orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi;

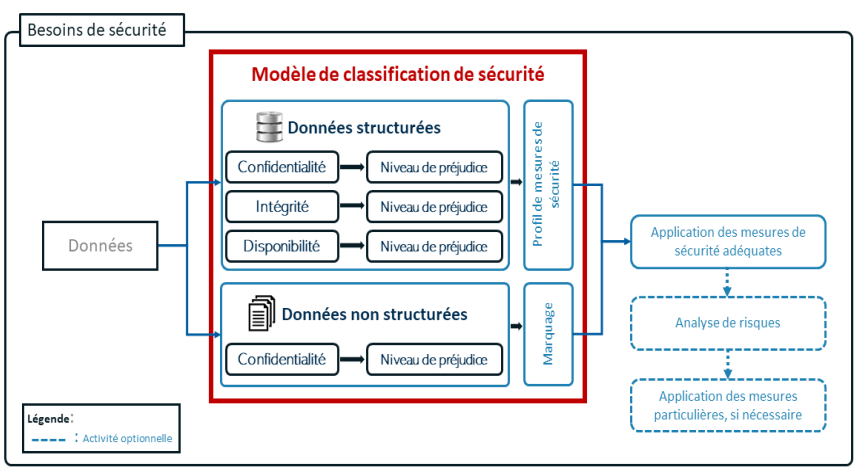
3° le cas échéant, l'analyse de risques au regard d'une donnée visée par la classification afin d'évaluer la pertinence d'appliquer des mesures de sécurité particulières;

4° le cas échéant, l'application de mesures de sécurité particulières que détermine un tel organisme, proportionnelles à la valeur de la donnée concernée et aux risques encourus.

Les mesures visées au premier alinéa à être appliquées par un organisme public doivent minimalement inclure, au regard d'une donnée, toute autre mesure de sécurité prévue à une évaluation des facteurs relatifs à la vie privée que ce dernier a réalisée.

La démarche visée au premier alinéa est illustrée avec la Figure 1 :

Figure 1



CHAPITRE III
CLASSIFICATION DE SÉCURITÉ DES DONNÉES

SECTION I
ÉTAPES POUR LA CLASSIFICATION DE SÉCURITÉ DES DONNÉES

6. Les étapes à suivre pour la classification de sécurité des données sont les suivantes :

1° l'identification du format des données, à savoir s'il s'agit de données structurées ou non, et de la granularité retenue;

2° la détermination de la catégorie d'appartenance au regard de chaque donnée conformément à la section II du présent chapitre;

3° la détermination de la sous-catégorie d'appartenance au regard de chaque donnée conformément à la section III du présent chapitre;

4° l'attribution d'un profil de mesures de sécurité ou, selon le cas, l'application d'un marquage conformément à la section IV du présent chapitre;

5° la tenue d'un registre conformément à la section V du présent chapitre.

La granularité visée au paragraphe 1° du premier alinéa constitue un choix de l'organisme public qui effectue la classification de sécurité des données qu'il détient. Elle peut avoir un niveau de détail fin en visant chacune des données ellesmêmes ou, au contraire, avoir une plus grande amplitude en visant d'autres objets de classification tels un programme, une activité, un service, une opération, un processus, un regroupement d'actifs informationnels ou un actif informationnel, et, par voie de conséquence, en assimilant de tels objets à une donnée. En ce dernier cas, l'organisme public identifie adéquatement les objets de classification choisis, en fait la description et applique le niveau de préjudice le plus élevé qui se rattache à l'une des données se trouvant dans ces objets.

Les étapes visées au premier alinéa sont illustrées à l'Annexe 1 et la classification qui en résulte tient compte de la grille des niveaux de préjudice de l'Annexe 2 et du tableau des données visées par une restriction au droit d'accès de l'Annexe 3, étant entendu que cette dernière annexe est fournie uniquement à titre indicatif de sorte que le niveau de confidentialité minimal et maximal à être déterminé relève de l'organisme public qui en décide.

SECTION II
DÉTERMINATION DE LA CATÉGORIE D'APPARTENANCE

7. Les données structurées ou non, détenues par les organismes publics, appartiennent à l'une ou l'autre des deux catégories suivantes :

1° « **données classifiées** » ou « **classifié** », étant une catégorie comprenant les données suivantes :

a) les renseignements visés par une restriction au droit d'accès en vertu de la section II du chapitre II de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) et identifiés comme étant « classifié » à l'Annexe 3;

b) les données dont une compromission pourrait raisonnablement porter atteinte plus généralement à la sécurité de l'État, incluant la défense et le maintien de la stabilité sociopolitique et socioéconomique;

2° « **données protégées** » ou « **protégé** », étant une catégorie comprenant les données suivantes :

a) les renseignements visés par une restriction au droit d'accès en vertu de la section II du chapitre II de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou en en vertu du chapitre III de cette loi et identifiés comme étant « protégé » à l'Annexe 3;

b) les données concernant une personne physique, une entreprise ou une autre entité et dont une compromission pourrait raisonnablement causer un préjudice.

Advenant qu'une donnée ait, au moment de sa classification, le potentiel d'appartenir à la fois à la catégorie « classifié » et à la catégorie « protégé », la première catégorie prévaut sur la deuxième de sorte que la donnée concernée doit être considérée comme faisant alors partie de la catégorie « classifié ».

SECTION III
DÉTERMINATION DE LA SOUS-CATÉGORIE D'APPARTENANCE

§1. Les sous-catégories d'appartenance

8. Les sous-catégories d'appartenance possibles, au nombre total de 28, sont réparties parmi les deux catégories existantes et par objectif de sécurité, en fonction du niveau de préjudice applicable. La Figure 2 précise la répartition de ces souscatégories, avec leurs dénominations respectives :

Figure 2

Sous-catégories d'appartenance

Objectif de confidentialité		
Niveaux de préjudice	Catégories de données	
	Données protégées	Données classifiées
Très faible	Non classifié	
Faible	Protégé A	Diffusion restreinte
Modéré	Protégé B	Confidentiel
Élevé	Protégé C	Secret
Très élevé		Très secret

Objectif d'intégrité		
Niveaux de préjudice	Catégories de données	
	Données protégées	Données classifiées
Très faible	Très faible	Très faible
Faible	Faible	Faible
Modéré	Modéré	Modéré
Élevé	Élevé	Élevé
Très élevé	Très élevé	Très élevé

Objectif de disponibilité		
Niveaux de préjudice	Catégories de données	
	Données protégées	Données classifiées
Très faible	Très faible	Très faible
Faible	Faible	Faible
Modéré	Modéré	Modéré
Élevé	Élevé	Élevé
Très élevé	Très élevé	Très élevé

Ainsi, selon le cas, une sous-catégorie est dite :

1° « **très faible** » ou « **non classifié** », lorsqu'une compromission pourrait raisonnablement causer un préjudice *très faible* ou ne causerait *aucun* préjudice;

2° « **faible** », « **diffusion restreinte** » ou « **protégé A** », lorsqu'une compromission pourrait raisonnablement causer un *faible* préjudice;

3° « **modéré** », « **confidentiel** » ou « **protégé B** », lorsqu'une compromission pourrait raisonnablement causer un préjudice *modéré*;

4° « **élevé** », « **secret** » ou « **protégé C** », lorsqu'une compromission pourrait raisonnablement causer un préjudice *élevé*;

5° « **très élevé** » ou « **très secret** », lorsqu'une compromission pourrait raisonnablement causer un préjudice *très élevé*.

9. La détermination de la sous-catégorie d'appartenance résulte de l'exercice suivant :

1° l'identification du ou des types de préjudices applicables parmi ceux visés à l'article 10;

2° la détermination du niveau de préjudice pour chaque type de préjudices applicable conformément à l'article 11, en retenant le niveau de préjudice le plus élevé;

a) lorsqu'il s'agit d'une donnée structurée, la détermination d'un tel niveau doit être effectuée pour chacun des trois objectifs de sécurité;

b) lorsqu'il s'agit d'une donnée non structurée, la détermination d'un tel niveau doit être effectuée minimalement pour l'objectif de confidentialité;

3° l'application de la grille de concordance visée à l'article 13, uniquement pour l'objectif de confidentialité.

L'exercice visé au premier alinéa est illustré à l'étape 3 de l'Annexe 1.

§2. Identification des types de préjudices

10. Les dix types de préjudices, avec leur acronyme respectif, qui peuvent raisonnablement survenir advenant une compromission, susceptibles d'être identifiés comme étant applicables au regard d'un objectif de sécurité, sont ceux de la Figure 3 :

Figure 3

Types de préjudices	
T1	Préjudice physique causé aux personnes physiques
T2	Préjudice psychologique causé aux personnes physiques
T3	Perte financière pour des personnes physiques
T4	Perte financière pour des entreprises et autres entités
T5	Agitation ou désordre civil
T6	Perte financière pour l'État
T7	Préjudice causé à l'économie québécoise
T8	Préjudice causé aux services rendus à la population
T9	Préjudice causé à la réputation du Québec
T10	Perte de l'autonomie du Québec

Ces types de préjudices sont plus amplement décrits à l'Annexe 2.

§3. Détermination du niveau de préjudice pour chaque type de préjudices

11. Une fois que les types de préjudices visés à l'article 10 et à l'Annexe 2 sont identifiés, le niveau de préjudice qui se rattache à chacun des types de préjudices doit être déterminé.

Pour l'application du présent modèle, un niveau de préjudice a pour objet de refléter le degré de gravité ou d'importance du préjudice qui pourrait vraisemblablement résulter d'un bris de confidentialité, d'intégrité ou de disponibilité au regard d'une donnée et ce niveau est dit :

1° « **très faible** » lorsqu'une compromission pourrait raisonnablement causer un préjudice *très faible* ou ne causerait *aucun* préjudice;

2° « **faible** » lorsqu'une compromission pourrait raisonnablement causer un préjudice *limité* aux services publics rendus par l'État, à ses actifs informationnels, aux personnes physiques, aux entreprises ou à toute autre entité. Un préjudice *limité*, par exemple, s'entend d'une compromission pouvant entraîner :

a) une dégradation des services publics lesquels demeurent offerts, mais dont leur efficacité est quelque peu réduite;

b) des effets nuisibles mineurs aux actifs informationnels de l'État, aux personnes physiques, aux entreprises ou à toute autre entité;

c) des pertes financières mineures à l'État, aux personnes physiques, aux entreprises ou à toute autre entité;

3° « **modéré** » lorsqu'une compromission pourrait raisonnablement causer un préjudice *grave* aux services publics rendus par l'État, à ses actifs informationnels, aux personnes physiques, aux entreprises ou à toute autre entité. Un préjudice *grave*, par exemple, s'entend d'une compromission pouvant entraîner :

a) une dégradation importante des services publics lesquels demeurent offerts, mais dont leur efficacité est considérablement réduite;

b) un préjudice important aux actifs informationnels de l'État;

c) des pertes financières importantes à l'État, aux personnes physiques, aux entreprises ou à toute autre entité;

d) un préjudice important pour les personnes physiques qui n'implique pas la perte de la vie ou des blessures graves mettant la vie en danger;

4° « **élevé** » lorsqu'une compromission pourrait raisonnablement causer un préjudice *très grave* aux services publics rendus par l'État, à ses actifs informationnels, aux personnes physiques, aux entreprises ou à toute autre entité. Ce niveau ne s'applique qu'à un nombre très restreint de données. Un préjudice *très grave*, par exemple, s'entend d'une compromission pouvant entraîner :

a) une dégradation très importante ou une perte de services publics;

b) un préjudice nuisible aux actifs informationnels de l'État;

c) des pertes financières très importantes à l'État, aux personnes physiques, aux entreprises ou à toute autre entité;

d) un préjudice *très grave* pour les personnes physiques, avec perte de la vie ou blessures très graves mettant la vie en danger;

5° « **très élevé** » lorsqu'une compromission pourrait raisonnablement causer un préjudice *extrêmement grave* à la sécurité de l'État, à l'économie québécoise, à la réputation du Québec ou à son autonomie. Ce niveau ne s'applique qu'à un nombre très restreint de données. Un préjudice *extrêmement grave*, par exemple, s'entend d'une compromission pouvant entraîner :

a) une incapacité pour l'État d'offrir un ou plusieurs services publics essentiels (ex. : santé, alimentaire, transport, énergie, finance);

b) des effets nuisibles irréparables aux actifs informationnels de l'État;

c) un préjudice *extrêmement grave* pour un ensemble de personnes physiques, avec de nombreuses pertes de vie ou des traumatismes psychologiques importants ou mettant la vie de plusieurs personnes physiques en danger, et pouvant compromettre la nature ou nuire de quelque autre façon à l'intérêt public ou, encore, nécessiter l'intervention de l'État.

12. Dans la détermination du niveau de préjudice, une analyse plus approfondie peut permettre de considérer l'une des situations suivantes :

1° situation de **regroupement** : lorsque, dans la situation concernée, un ensemble de données peut être classifié à un niveau de préjudice plus élevé que les parties qu'il forme en raison du préjudice accru que pourrait causer toute compromission à cet ensemble. Dans une telle situation, les répercussions d'une compromission sur les opérations d'un ensemble de données sont plus importantes que les répercussions d'une compromission individuelle;

EXEMPLE : La divulgation non autorisée d'un dossier contenant des renseignements personnels pouvant causer un préjudice modéré à la personne concernée. Si tous les dossiers des ressources humaines d'un organisme public étaient divulgués, le niveau de préjudice pourrait devenir plus élevé pour l'État.

2° situation d'**inférence :** lorsque, dans la situation concernée, des données d'un certain niveau de préjudice peuvent compromettre des données plus sensibles. Il s'agit d'une situation où d'autres données plus sensibles pourraient être déduites à partir de données déjà classifiées;

EXEMPLE : Des dossiers comportant des renseignements personnels qui donnent certaines indications sur le rôle de l'employé au sein d'un organisme public chargé de prévenir, détecter ou réprimer le crime tels les corps policiers et, par le fait même, sur la nature de certaines activités de cet organisme, ce qui pourrait compromettre les intérêts de l'organisation, voire de l'État.

3° situation d'**interdépendance :** lorsque, dans la situation concernée, la perte ou la dégradation de données peut influer sur d'autres données.

EXEMPLE : Le niveau de préjudice résultant d'un bris d'intégrité des données d'un système de contrôle des accès physiques peut être supérieur si ce système donne accès à une zone contenant des données plus sensibles.

§4. Application d'une grille de concordance pour l'objectif de confidentialité

13. La grille de concordance à être utilisée, dans la détermination de la sous-catégorie d'appartenance d'une donnée au regard de l'objectif de confidentialité, est celle de la Figure 4 :

Figure 4

Grille de concordance - confidentialité		
Niveaux de préjudice	Catégories de données	
	Données protégées	Données classifiées
Très faible	Non classifié	
Faible	Protégé A	Diffusion restreinte
Modéré	Protégé B	Confidentiel
Élevé	Protégé C	Secret
Très élevé		Très secret

Pour les fins de cet objectif de sécurité et au regard d'une donnée de la catégorie « **protégé** », il est entendu que, lorsque le niveau de préjudice qui se rattache à une telle donnée est dit « **très élevé** », cette donnée appartient à la souscatégorie « **protégé C** », tout comme une donnée de la même catégorie d'appartenance se rattachant à un niveau de préjudice « **élevé** » du fait que les mesures de sécurité à être appliquées seront alors les mêmes.

SECTION IV
PROFIL DE MESURES DE SÉCURITÉ ET MARQUAGE

§1. Attribution d'un profil de mesures de sécurité à chaque donnée structurée

14. Un profil de mesures de sécurité doit être attribué à chaque donnée structurée afin de couvrir les trois objectifs de sécurité.

Un profil de mesures de sécurité emporte, pour un organisme public, l'obligation d'appliquer à une telle donnée les mesures de sécurité adéquates qui y sont liées, notamment celles prévues aux orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi, auquel profil peuvent s'ajouter, selon le cas, des mesures de sécurité particulières.

La dénomination d'un profil de mesures de sécurité se compose des trois dénominations des sous-catégories d'appartenance concernées, dans l'ordre suivant : « confidentialité, intégrité, disponibilité ».

En voici des exemples :

— *Exemple no 1 :* « Protégé A, Élevé, Faible » ou « PaEF » en abrégé

— *Exemple no 2 :* « Protégé A, Élevé, Modéré » ou « PaEM » en abrégé

— *Exemple no 3 :* « Protégé B, Modéré, Modéré » ou « PbMM » en abrégé

— *Exemple no 4 :* « Protégé B, Modéré, Faible » ou « PbMF » en abrégé

— *Exemple no 5 :* « Protégé C, Élevé, Faible » ou « PcEF » en abrégé

— *Exemple no 6* : « Protégé C, Élevé, Élevé » ou « PcEE » en abrégé

— *Exemple no 7 :* « Non Classifié, Faible, Élevé » ou « NcFE » en abrégé

— *Exemple no 8 :* « Diffusion restreinte, Modéré, Faible » ou « DrMF » en abrégé

— *Exemple no 9 :* « Diffusion restreinte, Élevé, Modéré » ou « DrEM » en abrégé

— *Exemple no 10 :* « Confidentiel, Modéré, Faible » ou « CMF » en abrégé

— *Exemple no 11 :* « Confidentiel, Modéré, Élevé » ou « CME » en abrégé

— *Exemple no 12 :* « Secret, Élevé, Faible » ou « SEF » en abrégé

§2. Application d'un marquage à chaque donnée non structurée

15. Un marquage doit être appliqué à chaque donnée non structurée afin de couvrir l'objectif de confidentialité.

Un marquage emporte, pour un organisme public, l'obligation d'appliquer à une telle donnée les mesures de sécurité adéquates qui y sont liées, notamment celles prévues aux orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi, auquel marquage peuvent s'ajouter, selon le cas, des mesures de sécurité particulières.

Malgré l'article 8, les sous-catégories d'appartenance possibles pour les données non structurées sont au nombre de 8 suivant la Figure 2 visée à cet article.

SECTION V
TENUE D'UN REGISTRE

16. Au fur et à mesure de la classification des données et tout au long du cycle de vie de celles-ci, un organisme public tient un registre dans lequel il consigne minimalement :

1° les objets de classification retenus avec leur description, à savoir s'il s'agit des données elles-mêmes ou d'autres objets tels un programme, une activité, un service, une opération, un processus, un regroupement d'actifs informationnels ou un actif informationnel;

2° les catégories et les sous-catégories d'appartenance obtenues pour chacun des objectifs de sécurité;

3° les types de préjudices identifiés ainsi que les niveaux de préjudice déterminés pour chacun des objectifs de sécurité;

4° les raisons justifiant les niveaux de préjudice déterminés.

L'obligation visée au présent article présente un lien pertinent et direct avec celle de tenir un inventaire des données numériques gouvernementales visée au paragraphe 2° du premier alinéa de l'article 12.12 de la Loi, conformément au règlement pris en vertu du paragraphe 1° de l'article 12.21 de cette loi.

La Figure 5 qui suit présente un exemple du registre visé au présent article :

Figure 5

Objet de classification	Description de l'objet	Catégories d'appartenance	Types de préjudices	Niveaux de préjudice			Profil ou marquage retenu	Justifications
				Confidentialité	Intégrité	Disponibilité		
Base de données du programme de subvention aux restaurateurs	Renseignements financiers de demande d'aide financière, relatifs au financement, aux travaux et au budget de réalisation d'un projet	Protégé	T4	M	M	F	PbMF	Renseignements financiers des entreprises dans le domaine de la restauration (art. 23 LAI) Même si le type de préjudice T7 semble s'appliquer à cette évaluation, les niveaux de préjudice sont estimés à TF ou F
			T6	M	M	F		
			T7	S.O.	S.O.	S.O.		
Questionnaire de bilan de sécurité	Réponses de l'OP au questionnaire permettant de faire une reddition de comptes en matière de sécurité de l'information	Classifié	T6	M	S.O.	S.O.	Confidentiel	Renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne (art. 29 LAI)

CHAPITRE IV
DISPOSITIONS DIVERSES ET FINALES

17. Le présent modèle peut être cité sous le nom de Modèle de classification.

18. Un organisme public peut, à compter de la date d'entrée en vigueur du présent modèle, échelonner la mise en œuvre des dispositions de celui-ci, dans le respect de l'échéancier suivant :

1° le 31 décembre 2025, étant la date maximale à laquelle chaque organisme public doit, au regard de ses données structurées, avoir complété la classification de celles-ci conformément au présent modèle;

2° le 31 mars 2028, étant la date maximale à laquelle chaque organisme public doit, au regard de ses données non structurées, avoir commencé l'application du marquage, dans le respect de la séquence de déploiement, par organisme public ou par groupe d'organismes publics, à être élaborée par le ministère de la Cybersécurité et du Numérique en lien avec les cibles prévues à la Stratégie gouvernementale de cybersécurité et du numérique 2024-2028.

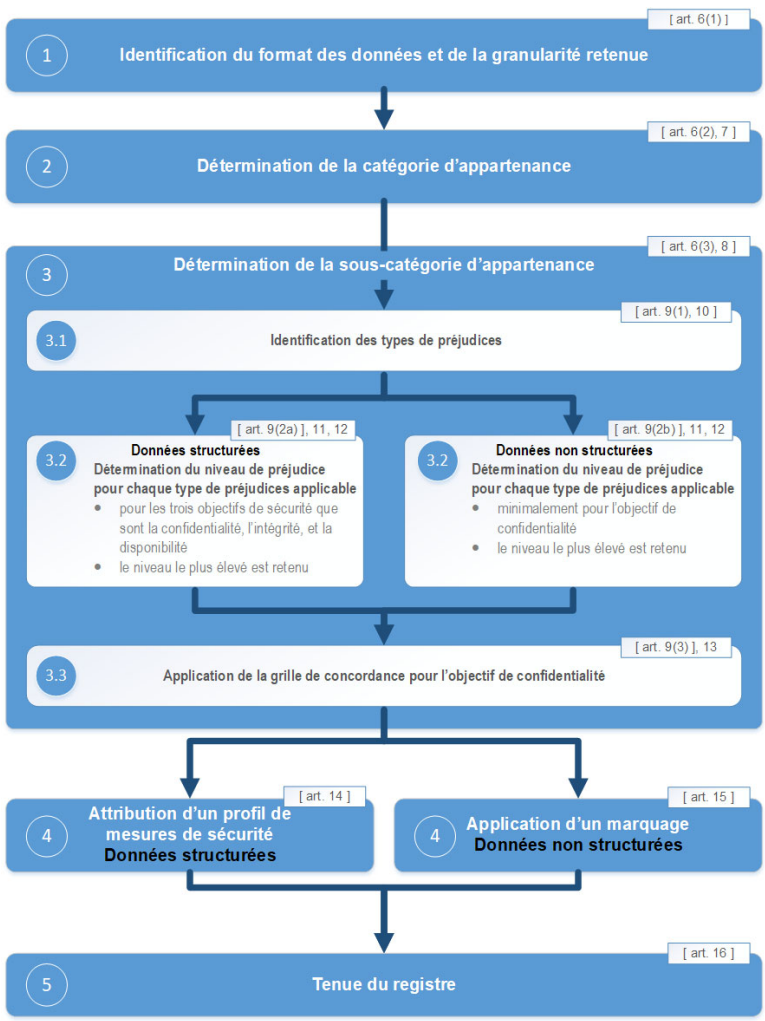
19. Le présent modèle remplace le Guide de catégorisation de l'information, pris par le Conseil du trésor en juillet 2016.

20. Le présent modèle entre en vigueur le 1er janvier 2025.

Établi le 12 décembre 2024 par le chef gouvernemental de la sécurité de l'information

ANNEXE 1
(articles 6 et 9)

ÉTAPES POUR LA CLASSIFICATION DE SÉCURITÉ DES DONNÉES



ANNEXE 2
(articles 6, 10 et 11)

GRILLE DES NIVEAUX DE PRÉJUDICE

Types de préjudices		Niveaux de préjudice				
		Très faible	Faible	Modéré	S'applique à un nombre très restreint de données	
					Élevé	Très élevé
T1	Préjudice physique causé aux personnes physiques	Aucun préjudice ou préjudice très faible	Inconfort physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
T2	Préjudice psychologique causé aux personnes physiques	Aucun préjudice ou préjudice très faible	Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
T3	Perte financière pour des personnes physiques	Aucun préjudice ou préjudice très faible	Stress ou inconfort	Incidence sur la qualité de vie Sécurité financière compromise pour certains	Sécurité financière compromise pour beaucoup	
T4	Perte financière pour des entreprises et autres entités	Aucun préjudice ou préjudice très faible	Incidence sur le rendement	Réduction de la compétitivité Viabilité compromise pour certains	Viabilité compromise pour beaucoup	
T5	Agitation ou désordre civil	Aucun préjudice ou préjudice très faible	Désobéissance civile, obstruction publique	Émeute	Acte de sabotage à l'égard des biens essentiels (infrastructures essentielles)	Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
T6	Perte financière pour l'Etat	Aucun préjudice ou préjudice très faible	Incidence sur le rendement des programmes gouvernementaux	Incidence sur les résultats des programmes	Viabilité des programmes compromise	Viabilité des programmes essentiels compromise
T7	Préjudice causé à l'économie québécoise			Incidence sur le rendement de l'économie québécoise	Perte de compétitivité à l'échelle nationale et internationale	Secteurs économiques clés compromis
T8	Préjudice causé aux services rendus à la population	Aucun préjudice ou préjudice très faible	Incidence sur le rendement d'un service	Incidence sur les opérations d'autres organismes publics	Un ou plusieurs services indispensables à la population ne peuvent être rendus	
T9	Préjudice causé à la réputation du Québec	Aucun préjudice ou préjudice très faible	Perte de la confiance du public	Embarras (au Québec, à une autre province, au Canada ou à l'étranger)	Relations fédérales-provinciales compromises	Relations diplomatiques et internationales compromises
T10	Perte de l'autonomie du Québec			Entrave à l'établissement de politiques gouvernementales importantes	Entrave à l'application efficace de la loi, cessation des activités du gouvernement	Atteinte à la souveraineté canadienne

ANNEXE 3
(articles 6 et 7)

TABLEAU DES DONNÉES VISÉES PAR UNE RESTRICTION AU DROIT D'ACCÈS
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1, «LAI»)

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
Renseignements ayant des incidences sur les relations intergouvernementales	Renseignement d'un autre gouvernement ou d'une organisation internationale (art. 18 LAI)	Facultative	Classifié	Faible	Élevé	Renseignements fournis par le gouvernement du Canada Renseignements obtenus de représentants d'un autre gouvernement inclus dans un rapport de mission Renseignements provenant de l'Agence du Revenu du Canada
	Renseignement dont la divulgation porterait vraisemblablement préjudice à la conduite des relations avec un autre gouvernement ou une organisation internationale (art. 19 LAI)	Facultative	Classifié	Faible	Élevé	Renseignements en lien avec une négociation avec un autre gouvernement (ex. : stratégie de négociation) Renseignements visés par un engagement de confidentialité envers un autre gouvernement
Renseignements ayant des incidences sur les négociations entre organismes publics	Renseignement dont la divulgation entraverait vraisemblablement une négociation en cours avec un autre organisme public (art. 20 LAI)	Facultative	Classifié	Faible	Modéré	Renseignements en lien avec des négociations concernant le budget d'un organisme public Renseignements concernant une négociation pour le partage des coûts entre organismes publics pour la mise en œuvre d'un programme
Renseignements ayant des incidences sur l'économie	Renseignement dont la divulgation révélerait un emprunt, un projet d'emprunt, une transaction ou un projet de transaction, un projet de tarification, un projet d'imposition ou de modification d'une taxe ou d'une redevance (art. 21 LAI)	Facultative	Classifié	Faible	Modéré	Procès-verbaux contenant des renseignements sur des projets de transactions immobilières Renseignements concernant les modalités de l'aide financière relatifs à des transactions avec des entreprises
	Secret industriel et renseignement industriel, financier, commercial, scientifique ou technique appartenant à un organisme public, dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à cet organisme ou de procurer un avantage appréciable à une autre personne, de nuire de façon substantielle à sa compétitivité ou de révéler un projet ou une stratégie d'emprunt, de placement, de gestion de dette ou de gestion de fonds (art. 22 LAI)	Facultative	Classifié	Faible	Modéré	Méthode de calcul d'un organisme public utilisée pour évaluer les retombées économiques Prévisions budgétaires non approuvées d'un organisme public Études de marché pour un organisme public constitué à des fins commerciales Dépenses de publicité, de formation et de déplacement qui permettent de tirer un revenu pour un organisme public constitué à des fins commerciales
	Secret industriel et renseignement industriel, financier, commercial,	Impérative	Protégé	Modéré	Modéré	Les coûts ventilés d'une soumission (salaire, coûts de production, etc.)

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
	scientifique, technique ou syndical de nature confidentielle fourni par un tiers (art. 23 LAI)					États financiers non publics d'un tiers Renseignements financiers contenus dans un formulaire pour une demande d'aide financière, relatifs au financement, aux travaux et au budget de réalisation d'un projet
	Renseignement fourni par un tiers lorsque sa divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers (art. 24 LAI)	Impérative	Protégé	Modéré	Modéré	Les coûts ventilés d'une soumission (salaire, coûts de production, etc.) Fiches techniques soumises dans le cadre d'un processus d'appel d'offres Renseignements concernant une demande de subvention Renseignements concernant une offre d'achat d'un tiers relatif à un immeuble appartenant à l'organisme public Structure de coûts de services d'un tiers
	Renseignement dont la divulgation aurait vraisemblablement pour effet de révéler un mandat ou une stratégie de négociation de convention collective ou de contrat Une étude préparée en vue de l'imposition d'une taxe, d'un tarif ou d'une redevance (art. 27 LAI)	Facultative	Classifié	Faible	Modéré	Une stratégie de négociation de convention collective (possible de refuser pour une période de huit ans à compter du début de la négociation) Une étude préparée en vue de l'imposition d'une taxe, d'un tarif ou d'une redevance (possible de refuser pour une période de dix ans) Renseignement portant sur la classification des employés syndiqués d'un organisme public (évaluation patronale)
Renseignements ayant des incidences sur l'administration de la justice et la sécurité publique	Renseignement détenu dans l'exercice d'une fonction de prévention, de détection ou de répression du crime ou des infractions aux lois ou dans l'exercice d'une collaboration, à cette fin, avec une personne ou un organisme chargé d'une telle fonction (art. 28 LAI) Renseignement obtenu par le service de sécurité interne d'un organisme public désigné par règlement, dans le cadre d'une enquête ayant pour objet de prévenir, détecter ou réprimer le crime ou les infractions aux lois (art. 28 LAI)	Impérative	Protégé ou Classifié	Modéré	Élevé	Enregistrement d'une entrevue dans le cadre d'une enquête criminelle Identité et déclarations des témoins Enquête d'habilitation sécuritaire Méthode utilisée par les policiers pour effectuer une enquête Le coût d'une enquête
	Renseignement dont la divulgation aurait pour effet de porter atteinte à la sécurité de l'État (art. 28.1 LAI)	Impérative	Classifié	Élevé	Élevé	Informations qui servent à faire des liens pour détecter les menaces potentielles ou réelles à la sécurité de l'État

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
	Renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi Renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne (art. 29 LAI)	Impérative	Classifié	Modéré	Élevé	Une description détaillée des objets prélevés sur les lieux d'incendie et que l'on veut soumettre à une expertise Plan de mesures d'urgence Analyse détaillée des risques afférents aux systèmes informatiques Description physique d'un centre de détention comprenant les points de contrôle d'accès et les déplacements des agents lors des rondes d'inspection Vérification d'antécédents dans le cadre de l'exécution d'un contrat
	Renseignement contenu dans une décision rendue dans l'exercice de fonctions juridictionnelles, qui en interdit la communication (huis clos, ordonnance de non-publication, de non-divulgation ou de non-diffusion) Renseignement susceptible de révéler le délibéré lié à l'exercice de fonctions juridictionnelles (art. 29.1 LAI)	Impérative	Protégé	Modéré	Élevé[1]	Témoignages à huis clos Les notes prises par les juges administratifs lors d'une audience
Renseignements ayant des incidences sur les décisions administratives ou politiques	Décret dont la publication est différée, décision résultant des délibérations du Conseil exécutif ou de l'un de ses comités ministériels, décision du Conseil du trésor (art. 30 LAI)	Facultative	Classifié	Faible	Élevé	Décision résultant des délibérations du Conseil des ministres (25 ans) Décision du Conseil du trésor (25 ans) Décret dont la publication est différée en vertu de la Loi sur l'exécutif
	Renseignement dont la divulgation aurait pour effet de révéler une politique budgétaire du gouvernement avant que le ministre des Finances ne la rende publique (art. 30.1 LAI)	Facultative	Classifié	Faible	Modéré	Le budget de dépenses du gouvernement avant que le ministre des Finances ne le rende public
	Opinion juridique portant sur l'application du droit à un cas particulier ou sur la constitutionnalité ou la validité d'un texte législatif ou réglementaire, d'une version préliminaire ou d'un projet de texte législatif ou réglementaire (art. 31 LAI)	Facultative	Protégé ou Classifié	Faible	Modéré	Opinion juridique

[1] En général, il est recommandé d'assigner le niveau **Modéré.** Certains renseignements de ce type de données pourraient être de niveau **Élevé**.

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
	Analyse dont la divulgation risquerait vraisemblablement d'avoir un effet sur une procédure judiciaire (art. 32 LAI)	Facultative	Classifié	Faible	Modéré	Analyse contenue dans un rapport d'enquête administrative Informations concernant le bien-fondé d'une demande d'expertise formulée par un organisme public Évaluation des risques d'accident de travail
	Diverses communications, recommandations, analyses ou avis du Conseil exécutif, d'un de ses membres, du Conseil du trésor ou d'un comité ministériel ou les mémoires ou les comptes rendus des délibérations du Conseil exécutif ou d'un comité ministériel ou une liste de titres de documents comportant des recommandations au Conseil exécutif ou au Conseil du trésor ou l'ordre du jour d'une réunion du Conseil exécutif, du Conseil du trésor ou d'un comité ministériel ou les mémoires des délibérations du comité exécutif d'un organisme municipal, les recommandations qui lui sont faites par ses membres ainsi que les communications entre ses membres (art. 33 LAI)	Impérative	Classifié	Modéré	Élevé	Mémoire destiné au conseil des ministres Avis émanant du Conseil du trésor Une liste de titres de documents comportant des recommandations au Conseil exécutif ou au Conseil du trésor L'ordre du jour d'une réunion du Conseil exécutif, du Conseil du trésor ou d'un comité ministériel
	Document du bureau d'un membre de l'Assemblée nationale, ou produit pour le compte de ce membre par les services de l'Assemblée, ou document d'un cabinet du président l'Assemblée, d'un membre de celle-ci visé dans le premier alinéa de l'article 124.1 de la Loi sur l'Assemblée nationale (chapitre A-23.1) ou d'un ministre visé dans l'article 11.5 de la Loi sur l'exécutif (chapitre E-18), ainsi que d'un document du cabinet ou du bureau d'un membre d'un organisme municipal ou scolaire (art. 34 LAI)	Impérative	Classifié	Modéré	Élevé	Les documents destinés à un ministre Commentaires relatifs à un projet de règlement
	Mémoires de délibérations d'une séance du conseil d'administration ou des membres d'un organisme public dans l'exercice de leurs fonctions (art. 35 LAI)	Facultative	Classifié	Faible	Modéré	Procès-verbal de la réunion du conseil d'administration (partie délibérative) Enregistrement des délibérations du comité exécutif

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
	Version préliminaire ou projet de texte législatif ou réglementaire ou analyse s'y rapportant (art. 36 LAI)	Facultative	Classifié	Faible	Modéré	Version préliminaire d'un projet de loi Ébauche d'un projet de règlement Analyse relative aux impacts d'un projet de loi non déposé à l'Assemblée nationale
	Avis ou recommandation faits depuis moins de dix ans, par un membre d'un organisme public, un membre de son personnel, un membre d'un autre organisme public ou un membre du personnel de cet autre organisme, dans l'exercice de leurs fonctions Avis ou recommandation ayant été faits à un organisme public, à sa demande, depuis moins de dix ans, par un consultant ou par un conseiller sur une matière de sa compétence (art. 37 LAI)	Facultative	Protégé ou Classifié	Faible	Modéré	Avis des fonctionnaires relatif à un projet Recommandation faite par une entreprise à la demande d'un ministère Note interne proposant des scénarios pour solutionner une problématique Pointage décerné à différents projets afin de prioriser leur mise en œuvre Grille synthèse d'évaluation d'une demande de subvention
	Avis ou recommandation faits par un organisme public à un autre, jusqu'à ce que la décision finale sur la matière faisant l'objet de l'avis ou de la recommandation ait été rendue publique par l'autorité compétente (art. 38 LAI)	Facultative	Protégé ou Classifié	Faible	Modéré	
	Avis ou une recommandation fait à un ministre par un organisme qui relève de son autorité (art. 38 LAI)	Facultative	Protégé ou Classifié	Faible	Modéré (pour protégé) Élevé (pour classifié)	Avis produit par un organisme qui relève d'un ministère Recommandations transmises à un autre organisme public
	Analyse produite à l'occasion d'une recommandation faite dans le cadre d'un processus décisionnel en cours (art. 39 LAI)	Facultative	Classifié	Faible	Modéré	Étude de faisabilité Rapport d'analyse Diagnostic organisationnel
	Épreuve destinée à l'évaluation comparative des connaissances, des aptitudes, de la compétence ou de l'expérience d'une personne (art. 40 LAI)	Facultative	Classifié	Faible	Modéré	Examen Questionnaire d'embauche Fiche d'évaluation des aptitudes et cahier-réponse Canevas d'entrevue
Renseignements ayant des incidences sur la vérification	Renseignement dont la divulgation serait susceptible : 1° d'entraver le déroulement d'une opération de vérification;	Facultative	Classifié	Faible	Modéré	Document du vérificateur général en lien avec une vérification en cours Planification d'audit des vérificateurs internes

En vertu de la LAI			En vertu du Modèle de classification			Exemples
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	
	2° de révéler un programme ou un plan d'activité de vérification; 3° de révéler une source confidentielle d'information relative à une vérification; ou 4° de porter sérieusement atteinte au pouvoir d'appréciation accordé au vérificateur général par les articles 38, 39, 40, 42, 43, 43.1 et 45 de la Loi sur le vérificateur général (chapitre V-5.01) (art. 41 LAI)					
Renseignements personnels	Renseignements personnels à caractère public	Non applicable	Protégé	Très faible	Très faible	Nom et coordonnées des employés d'un organisme public Nom et adresse des titulaires de permis de transformation alimentaire Renseignement relatif à une transaction immobilière (registre foncier)
Renseignements personnels	Renseignements personnels, en règle générale (art. 53 LAI ou autres dispositions légales dans le cas d'un régime particulier) Renseignements personnels qui ne sont pas à caractère public	Impérative	Protégé	Faible	Modéré	Nom, adresse et numéro de téléphone d'un citoyen Salaire d'un employé Renseignements relatifs à la situation familiale (ex. : célibataire, mariée, séparée, etc.).
Renseignements personnels	Renseignements personnels sensibles	Impérative	Protégé	Modéré	Élevé[2]	**Modéré :** Renseignements médicaux et numéro d'assurance maladie **Modéré :** Renseignements financiers ou fiscaux (salaire, actif, passif, déclaration de revenus, etc.) **Élevé :** Renseignements en lien avec des enquêtes policières (ex. : délateurs, infiltrations policières, etc.).

[2] Dans certaines situations exceptionnelles, lorsqu'une compromission pourrait raisonnablement causer un préjudice très grave pour les personnes physiques, avec perte de la vie ou blessures très graves mettant la vie en danger, le niveau maximal peut être **Élevé**. À titre d'exemple, les données contenues dans un programme de protection des témoins auraient un niveau de confidentialité **Élevé**, compte tenu du danger imminent de perte de vie des témoins.

84711