# Modèle de classification de sécurité des données numériques gouvernementales

## Présentation à la communauté gouvernementale

Mars 2025

Votre gouvernement

Québec

# Mot de bienvenue

# Agenda

- Objectifs du webinaire
- Présentation détaillée du modèle de classification
  - Réalisation d'une analyse des préjudices;
  - Utilisation du tableau des données visées par une restriction au droit d'accès.
- Guide d'accompagnement du modèle
  - Actualisation des analyses des préjudices du Programme de consolidation des centres de traitement informatique (PCCTI).
- Inventaire des données numériques gouvernementales
  - Référentiel de l'information gouvernementale.
- Soutien et accompagnement
  - Répertoire des outils et guides.
- Calendrier de déploiement du modèle
- Période de questions

# Objectifs du webinaire

- **Clientèle visée**
  - Conseillers en sécurité de l'information;
  - Intervenants impliqués dans la classification de sécurité des données.

- **Objectifs de la présentation**
  - Présenter les concepts fondamentaux du modèle;
  - Décrire le modèle de classification de sécurité;
  - Découvrir les outils pour le soutien et l'accompagnement;
  - Connaître les prochaines étapes.

# Présentation du modèle de classification

# Avant de débuter…

## Préparez votre téléphone pour répondre à nos questions!

Se joindre à

**slido.com**

**#2493 116**

Votre gouvernement

Québec

# Présentation du modèle de classification

## Objectifs du modèle de classification

Assurer une classification uniforme à l'aide d'un modèle commun pour l'ensemble des organismes publics

Assurer l'application de mesures de protection proportionnelles à la valeur de l'information et aux risques encourus

Faciliter l'interopérabilité et la portabilité des données avec les partenaires (fédéraux et autres)

# Présentation du modèle de classification

## Entrée en vigueur

- Le modèle de classification de sécurité des données numériques gouvernementales est en vigueur depuis le 1er janvier 2025 (arrêté 2024-05).
- Le modèle remplace le Guide de catégorisation de l'information, pris par le Secrétariat du Conseil du trésor en juillet 2016.

# Présentation du modèle de classification

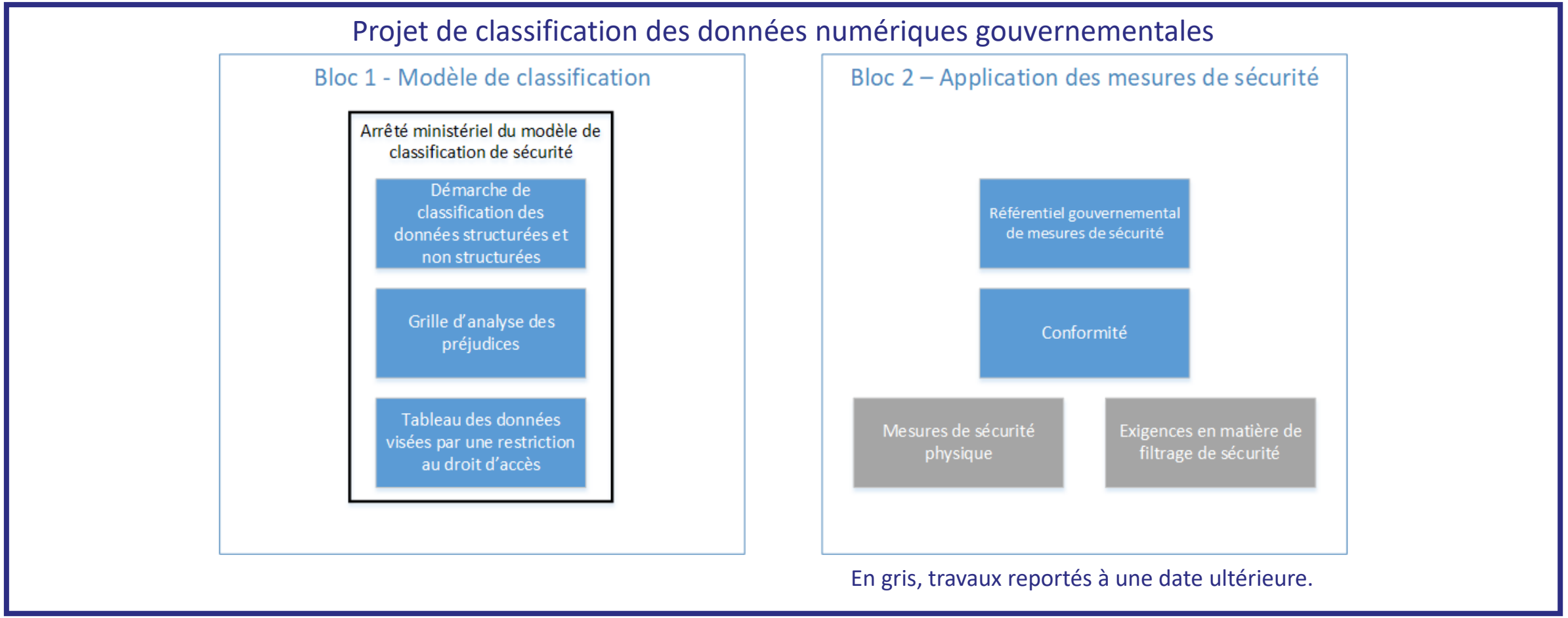
## Cadre légal

- 12.6. Le chef gouvernemental de la sécurité de l'information assume les responsabilités suivantes :
  - 3° **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 le faire approuver par le ministre;

- 12.12. Le gestionnaire des données numériques gouvernementales assume les responsabilités suivantes :
  - 2° **maintenir à jour une consolidation des inventaires** de telles données que doivent tenir les organismes publics conformément au règlement pris en vertu du paragraphe 1° de l'article 12.21 et identifier celles ayant un potentiel de mobilité ou de valorisation;
  - 5° **s'assurer de l'application du modèle de classification de sécurité des données** établi par le chef gouvernemental de la sécurité de l'information […]

# Présentation du modèle de classification

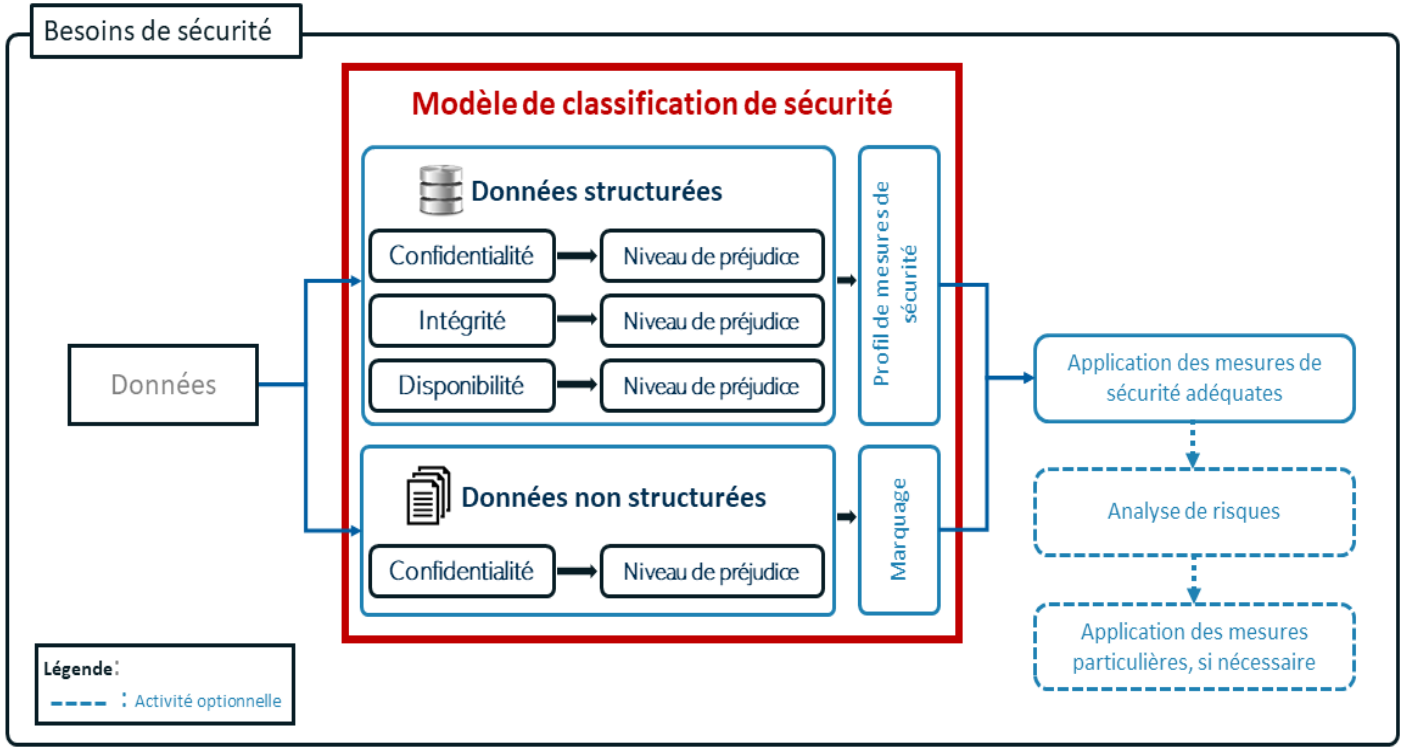
## Projet de classification – Deux volets à réaliser




En gris, travaux reportés à une date ultérieure.

# Présentation du modèle de classification

## Démarche globale de sécurisation des données

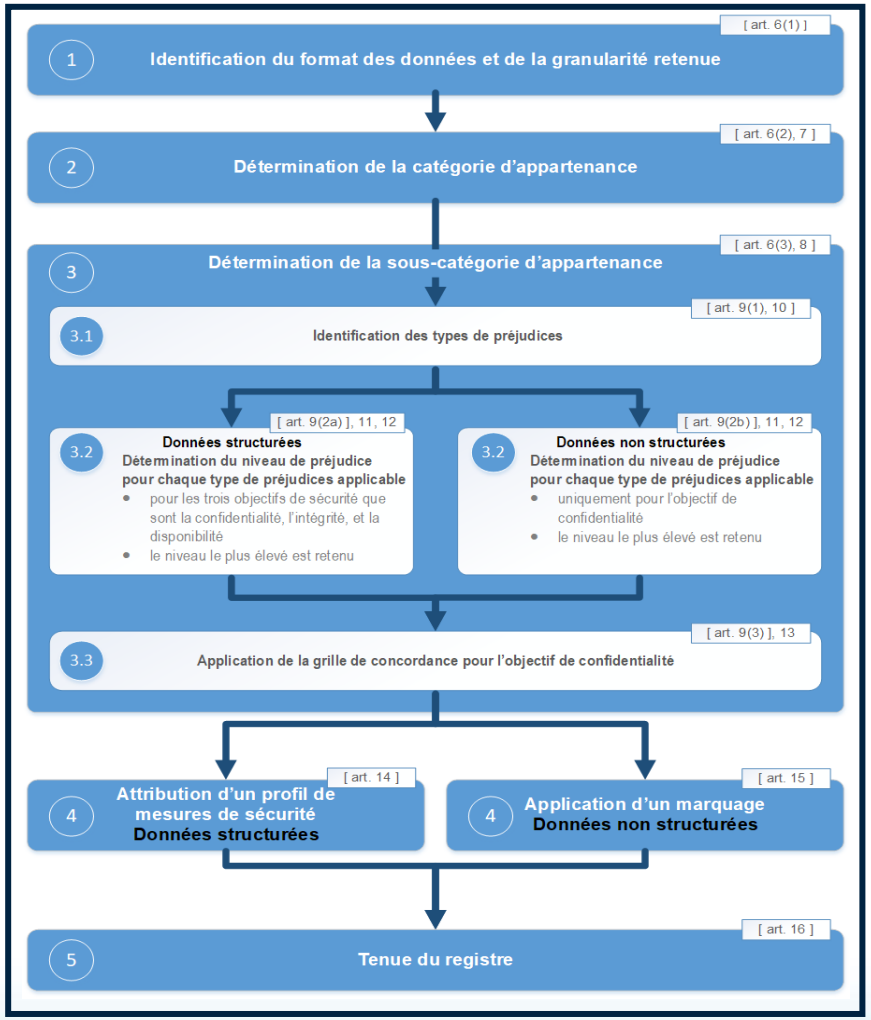



« **donnée structurée** » : une donnée stockée selon un format prédéfini de façon à permettre son interprétation par un logiciel, telle une donnée stockée dans une base de données utilisée par différents systèmes d'information.

« **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 courriel.

# Présentation du modèle de classification

## Étapes pour la classification de sécurité des données



# Présentation du modèle de classification

## Catégories d'appartenance

- « **données classifiées** » ou « **classifié** » est 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.

- « **données protégées** » ou « **protégé** » est 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.

slido

**Vous avez entre les mains des dossiers de citoyens concernant des demandes d’aide financière. S’agit-il de données « protégé » ou « classifié »?**

# Présentation du modèle de classification

## Types de préjudices

| 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 |

**Préjudices aux personnes physiques**

**Préjudices aux entreprises**

**Préjudices à l'État**

# Présentation du modèle de classification

## Grille des niveaux de préjudices

| 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<br>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<br>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'État | 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 |

# Présentation du modèle de classification

## Sous-catégories d'appartenance

**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 |

Les sous-catégories d'appartenance possibles sont réparties entre les deux catégories existantes et par objectif de sécurité, en fonction du niveau de préjudice applicable.

- **Confidentialité** : 8 sous-catégories
- **Intégrité** : 10 sous-catégories
- **Disponibilité** : 10 sous-catégories

# Présentation du modèle de classification

## Attribution d'un profil de mesures de sécurité

- *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

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 et disponibilité ».

# Présentation du modèle de classification

## Application d’un marquage à chaque donnée non structurée

| 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 |

Sous-catégories d’appartenance possibles pour les données non structurées

# Présentation du modèle de classification

## Tableau des données visées par une restriction au droit d'accès*

**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<br>Renseignements obtenus de représentants d'un autre gouvernement inclus dans un rapport de mission<br>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)<br>Renseignements visés par un engagement de confidentialité envers un autre gouvernement |

| 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 personnels** | Renseignements personnels à caractère public | Non applicable | Protégé | Très faible | Très faible | Nom et coordonnées des employés d'un organisme public<br>Nom et adresse des titulaires de permis de transformation alimentaire<br>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)<br>Renseignements personnels qui ne sont pas à caractère public | Impérative | Protégé | Faible | Modéré | Nom, adresse et numéro de téléphone d'un citoyen<br>Salaire d'un employé<br>Renseignements relatifs à la situation familiale (ex. : célibataire, mariée, séparée, etc.). |
| **Renseignements personnels** | Renseignements personnels sensibles | Impérative | Protégé | Modéré | Élevé[1] | **Modéré :**<br>Renseignements médicaux et numéro d'assurance maladie<br>**Modéré :**<br>Renseignements financiers ou fiscaux (salaire, actif, passif, déclaration de revenus, etc.)<br>**Élevé :**<br>Renseignements en lien avec des enquêtes policières (ex. : délateurs, infiltrations policières, etc.). |

[1] 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.

*Tableau conçu en collaboration avec le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité (SRIDAIL)

Votre gouvernement

Québec

slido

Please download and install the Slido app on all computers you use

**Sur un formulaire, vous remarquez le texte dans le rectangle rouge. Cela signifie qu'une fois rempli, le formulaire :**

ⓘ Start presenting to display the poll results on this slide.

# Rappel

## LES FORMATS DE DONNÉES NUMÉRIQUES

- Données structurées (exemple : données stockées dans les bases de données des systèmes de mission des organismes publics)
- Données non structurées (exemple : documents générés par des outils bureautiques et des courriels)

## LES CATÉGORIES ET SOUS-CATÉGORIES D'APPARTENANCE

- **Protégée** : données concernant des personnes physiques, des entreprises et d'autres entités (excluant les données touchant l'État)
  Sous-catégories : Non classifié, Protégé A, Protégé B, Protégé C
- **Classifiée** : données reliées aux intérêts de l'État
  Sous-catégories : Non classifié, Diffusion restreinte, Confidentiel, Secret, Très secret

## LES OBJECTIFS DE SÉCURITÉ

- Confidentialité, intégrité et disponibilité

## LES PROFILS DE MESURES DE SÉCURITÉ ET MARQUAGE

- Attribution d'un profil de mesures de sécurité à chaque donnée structurée
- Application d'un marquage à chaque donnée non structurée

## LES PARTIES CONCERNÉES PAR LES PRÉJUDICES

- Personnes physiques, entreprises et autres entités et l'État

slido

Please download and install the Slido app on all computers you use

**Vous devez produire une nouvelle stratégie de recrutement et de rétention du personnel. Cette stratégie définit des objectifs et des cibles à atteindre par votre direction des ressources humaines. Quel sera le marquage du document?**

ⓘ Start presenting to display the poll results on this slide.

# Guide d’accompagnement du modèle

# Guide d’accompagnement du modèle

## Présentation


Ce guide s’adresse à tous les intervenants de la classification de sécurité de l’information. Il complète l’arrêté ministériel du modèle de classification des données numériques gouvernementales avec des explications additionnelles, des exemples et des astuces.

**À noter :** les explications et les exemples déjà inclus dans l’arrêté ministériel ne sont pas répétés. Il est donc essentiel de consulter l’arrêté ministériel au préalable pour tirer pleinement profit de ce guide.

# Guide d'accompagnement du modèle

## Actualisation des analyses des préjudices du PCCTI

- **Option 1 :** convertir les analyses des préjudices des systèmes dont l'analyse des préjudices PCCTI est terminée. Par « conversion », on fait référence à la possibilité de convertir le profil retenu lors de l'analyse des préjudices du PCCTI en un profil prédéfini jugé équivalent dans le modèle de classification.
  - Procure une économie de temps et d'efforts.

| Niveau de préjudice | Profils du PCCTI | Profils du modèle de classification | |
|---|---|---|---|
| | | Protégé | Classifié |
| Très faible/ Faible | Profil A | PaFF | DrFF |
| Modéré | Profil B | PbMM | CMM |
| Élevé / Très élevé | Profil C | PcEE | SEE |

# Guide d'accompagnement du modèle

## Actualisation des analyses des préjudices du PCCTI

- **Option 2** : réviser les analyses des préjudices des systèmes dont l'analyse des préjudices PCCTI est terminée. Par « révision », on entend la possibilité de réviser le profil obtenu lors de l'analyse de préjudices du PCCTI en un profil dont au moins un des objectifs de sécurité comporte un même niveau de préjudice selon le modèle de classification.
  - Permet de définir les profils plus précisément selon les niveaux de préjudices retenus pour chacun des objectifs de sécurité.
  - N'est pas possible si les informations du PCCTI sont incorrectes, incomplètes ou inexactes. Dans ce cas, une analyse complète du système devra être réalisée.

| Profils PCCTI | Profils comparables du modèle de classification | |
|---|---|---|
| | Protégé | Classifié |
| **Profil A** (Les objectifs de sécurité ne dépassent pas le niveau Faible) | NcFF | |
| | PaFF | DrFF |
| **Profil B** (Les objectifs de sécurité ne dépassent pas le niveau Modéré) | NcFM, NcMF, NcMM | |
| | PaFM, PaMF, PaMM | DrFM, DrMF, DrMM |
| | PbFF, PbFM, PbMF, PbMM | CFF, CFM, CMF, CMM |
| **Profil C** (Au moins un des objectifs de sécurité a atteint le niveau Élevé) | NcFE, NcME, NcEF, NcEM, NcEE | |
| | PaFE, PaME, PaEF, PaEM, PaEE | DrFE, DrME, DrEF, DrEM, DrEE |
| | PbFE, PbME, PbEF, PbEM, PbEE | CFE, CME, CEF, CEM, CEE |
| | PcFF, PcFM, PcFE, PcMF, PcMM, PcME, PcEF, PcEM, PcEE | SFF, SFM, SFE, SMF, SMM, SME, SEF, SEM, SEE |

Votre gouvernement

Québec

# Guide d’accompagnement du modèle

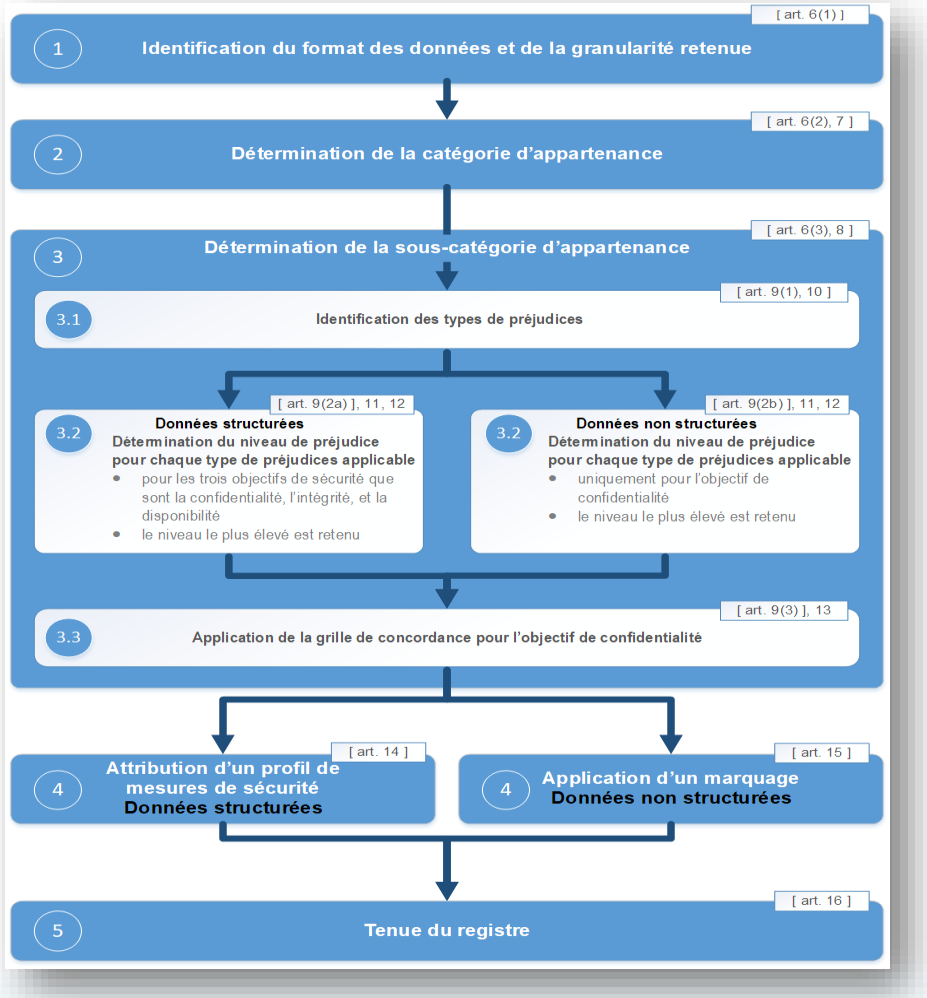
## Actualisation des analyses des préjudices du PCCTI

- **Pour les options 1 et 2 :**
  - Il s’agit d’étapes intermédiaires permettant de s’adapter rapidement au modèle de classification.
  - Elles devront être suivies ultérieurement, au terme d’une analyse complète, afin qu’elles soient parfaitement conformes au modèle de classification.

# Guide d’accompagnement du modèle

## Actualisation des analyses des préjudices du PCCTI

- **Pour l’option 3** : faire une analyse complète des systèmes n’ayant pas été analysés. Il s’agit de procéder à une analyse en respectant toutes les étapes du modèle de classification.



# Inventaire de données numériques gouvernementales

# Inventaire des données numériques gouvernementales

- Repose sur une **démarche intégrée** d'inventaire et de classification des données numériques gouvernementales.
- Permet la classification des données au fur et à mesure de la réalisation de la démarche intégrée.

À terme, toutes les données auront été classifiées selon le modèle de classification.

# Inventaire des données numériques gouvernementales

## Référentiel de l'information gouvernementale (RIG)*

- Outil gouvernemental pour documenter l'inventaire et la classification de sécurité des données des organismes publics (OP).
- Association avec les données des systèmes documentés à l'État de santé des actifs en ressources informationnelles (ÉSARI).
- Capacité d'importation et de conversion des analyses des préjudices du PCCTI.


À noter que vous ne pouvez pas importer les justifications que vous avez inscrites dans vos fiches d'analyse. Le système de revue diligente ne le permet pas. C'est pourquoi nous vous recommandons de conserver vos fiches d'analyse. Il vous appartient de les ajouter manuellement dans le RIG.

# Soutien et accompagnement

# Soutien et accompagnement

## Liste des documents

| Modèle de classification | Public cible | Description |
|---|---|---|
| Arrêté ministériel 2024-05 du modèle de classification des données numériques gouvernementales | Dirigeants d'organismes, chefs de la sécurité de l'information gouvernementale, intervenants de la classification de sécurité des données numériques gouvernementales* | Le document présente les dispositions du modèle de classification en regard de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Il présente également en détail la démarche de classification de sécurité. |
| Guide d'accompagnement (PFC : LIBRE) | Intervenants de la classification de sécurité des données numériques gouvernementales* | Le guide complète l'arrêté ministériel du modèle de classification des données numériques gouvernementales par des explications additionnelles, des exemples et des astuces. |
| Tableau des données visées par une restriction au droit d'accès (PFC : LIBRE) | Intervenants de la classification de sécurité des données numériques gouvernementales* | Le tableau est un outil dont l'objectif est d'aider à classifier des données qui sont soumises à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. |
| Capsule d'information sur le modèle de classification (à venir) (PFC : LIBRE) | Personnel des organismes publics | La capsule annonce l'entrée en vigueur du modèle de classification, sa raison d'être et les changements qui en découlent. Elle vise à susciter l'intérêt et amorcer une mobilisation du personnel. |
| À VENIR : Webinaire sur le Modèle de classification de sécurité des données numériques gouvernementales (PFC : LIBRE) | Intervenants de la classification de sécurité des données numériques gouvernementales* | La présentation aborde les nouvelles orientations concernant la classification de sécurité des données numériques gouvernementales, soit celles prévues au modèle, les outils offerts, l'organisation du soutien ainsi que les arrimages avec certaines grandes initiatives en cours dans les organismes publics. |

*Chargé de projet, conseiller en sécurité de l'information, détenteur ou propriétaire des données, responsable de l'accès aux documents et de la protection des renseignements personnels, gestion documentaire et autres.

# Soutien et accompagnement

## Liste des documents

| Données structurées | Public cible | Description |
|---|---|---|
| Aide à la tâche : Grille d'analyse (PFC : VERT) | Conseillers en sécurité de l'information qui soutiennent les intervenants de la classification de sécurité dans l'application du modèle de classification de sécurité* | La grille d'analyse permet de documenter sommairement les données à classifier, d'en faire l'analyse des préjudices et d'en déterminer le profil de mesures de sécurité. |
| Outils d'inventaire des données numériques gouvernementales (Référentiel de l'information gouvernementale [RIG] [1])<br><br>[1] Disponible seulement pour les organismes connectés au RITM | Conseillers en sécurité de l'information | L'outil (Référentiel de l'information gouvernementale [RIG]) est offert aux organismes publics qui réalisent l'inventaire des données numériques gouvernementales. Il intègre l'inventaire et la classification de sécurité des données. |
| Guide d'utilisation du référentiel de l'information gouvernementale (équipe Teams MCN-Inventaire-classification) | Conseillers en sécurité de l'information | Le guide décrit de façon détaillée les étapes pour importer les analyses de préjudices effectuées dans le cadre du PCCTI. |

*Chargé de projet, conseiller en sécurité de l'information, détenteur ou propriétaire des données, responsable de l'accès aux documents et de la protection des renseignements personnels, gestion documentaire et autres.

# Soutien et accompagnement

## Liste des documents

| Données non structurées | Public cible | Description |
|---|---|---|
| Aides à la tâche : Description des étiquettes – Format texte (PFC : LIBRE) | Personnel des organismes publics | Le document décrit les étiquettes en format texte. Il présente une brève description de l'étiquette ainsi que des exemples. |
| À VENIR : aide à la tâche : Outil d'aide au marquage (PFC : LIBRE) | Personnel des organismes publics | Le document présente les trois étapes du marquage des données non structurées ainsi que des exemples :<br>1. Catégorie<br>2. Préjudices<br>3. Étiquette |
| Élaboration d'une stratégie de déploiement de marquage (PFC : LIBRE) | Tous les intervenants impliqués dans le déploiement du marquage des données non structurées et plus particulièrement les gestionnaires et chargés de projet responsables | Le document propose une approche permettant de définir une stratégie de déploiement pour le marquage des données non structurées. |
| Configurations minimales pour le marquage dans l'environnement Microsoft 365 (PFC : VERT) | Équipes responsables de la gestion et de la sécurité des environnements M365 | Le document détaille les configurations techniques à appliquer dans l'environnement Microsoft M365 pour le marquage des données non structurées. |
| À VENIR : formation « Le marquage des données numériques gouvernementales » (PFC : LIBRE) | Personnel des organismes publics | La formation vise à transmettre au personnel les connaissances requises pour marquer les données non structurées comme prévu au Modèle de classification de sécurité. |
| À VENIR : webinaire intitulé Configurations de Microsoft Purview pour le marquage des données numériques gouvernementales (PFC : VERT) | Responsables de l'administration et de la sécurité des environnements Microsoft 365 (Purview) | Le webinaire vise à présenter les configurations Microsoft Purview pour le marquage des données non structurées, y compris les prérequis et préparatifs essentiels au déploiement de celles-ci. |

# Soutien et accompagnement

## Des questions portant sur l’application du modèle?

- Vous êtes invités à consulter le représentant désigné pour votre organisation. Si vous ne connaissez pas le vôtre, allez à la rubrique « Des questions? », disponible sur la page Web **Classification de sécurité des données numériques gouvernementales**, pour consulter la liste.

# Calendrier de déploiement du modèle

# Calendrier de déploiement du modèle

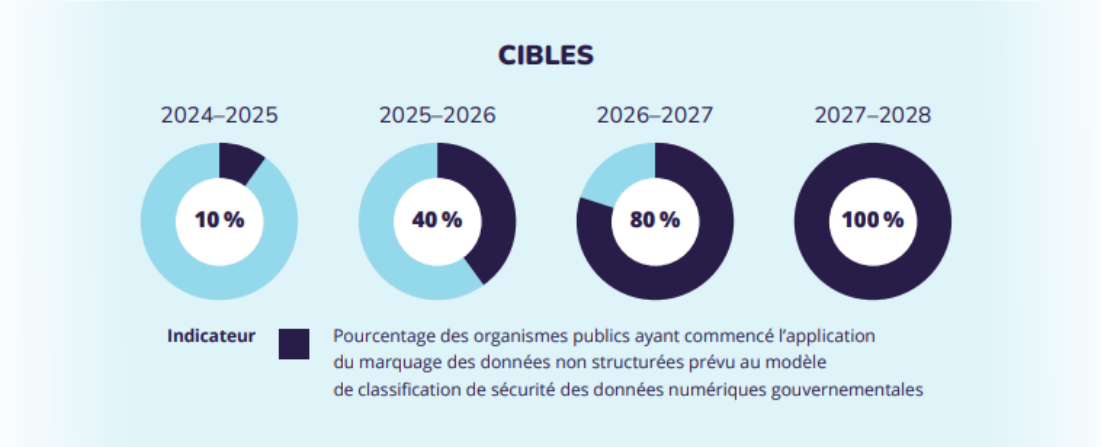
- Arrêté ministériel 2024-05 :
  - Article 18. Un organisme public peut, à compter de la date d'entrée en vigueur du présent modèle, échelonner la mise en œuvre des dispositions de celui-ci, dans le respect de l'échéancier suivant :
    - 1° le 31 décembre 2025, étant la date maximale à laquelle chaque 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.
    - Par « avoir commencé », on entend :
      - qu'un sous-ensemble ou l'ensemble du personnel ait commencé le marquage;
      - que le marquage soit appliqué sur un sous-ensemble ou sur l'ensemble des événements suivants :
        - transmission d'un courriel;
        - création d'un nouveau document;
        - mise à jour ou réouverture d'un document créé antérieurement.

# Calendrier de déploiement du modèle

## Classification des données non structurées

- Échéance : 31 mars 2028
- Cibles définies dans la Stratégie gouvernementale de cybersécurité et du numérique 2024-2028 (SGCN)

  - Pourcentage des organismes publics ayant commencé l'application du marquage des données non structurées prévu au modèle de classification de sécurité des données numériques gouvernementales.
  - Dans le respect de la séquence de déploiement à être élaborée par le ministère de la Cybersécurité et du Numérique.



# Calendrier de déploiement du modèle

## Webinaire – Configurations Microsoft Purview

Le webinaire vise à présenter les configurations Microsoft Purview pour le marquage des données non structurées, y compris les prérequis et préparatifs essentiels au déploiement de celles-ci.

**Sujets à l'ordre du jour** :

- Guide des **configurations minimales pour le marquage dans l'environnement Microsoft M365**;
- Organisation du soutien;
- Réponses aux questions soulevées par la présentation.

**Public cible** :

- Responsables de l'administration et de la sécurité des environnements Microsoft 365 (Purview);
- Chargés de projet;
- Conseillers en sécurité / Conseillers en cyberdéfense.

# Calendrier de déploiement du modèle

## Reddition de comptes

- Prochaine reddition de comptes :
  - Lancement à la mi-mars;
  - Portrait au 30 avril 2025.
- Les questions porteront sur :
  - l'application du modèle pour les données structurées;
  - le suivi des cibles de la SGCN pour les données non structurées.

Nous vous suggérons fortement l'utilisation du Référentiel de l'information gouvernementale (RIG) pour inscrire/convertir vos systèmes d'information. Cet outil nous permettra d'obtenir automatiquement des statistiques sur l'état d'avancement de l'application du modèle.

# Période de questions

# MERCI!