Ontario

Ministère des Services au public et aux entreprises et de l'Approvisionnement
Stratégie, Intelligence artificielle, Données
Division de l'intelligence artificielle

Document d'orientation pour la mise en œuvre du Règlement en matière de cybersécurité en vertu de la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*

Table des matières

Introduction 2

Objet 2

Nouvelles exigences prévues par la Loi de 2024 visant à renforcer la sécurité et la confiance en matière de nur

Exigence 1 : Désigner une personne-ressource principale et un suppléant en matière de cybersécurité 3

Étape 1 : Désigner une personne-ressource adéquate 3

Étape 2 : Informer la Division de la cybersécurité du MSPEA 3

Étape 3 : Modifier les renseignements 4

Exigence 2 : Réaliser des évaluations de la maturité en matière de cybersécurité 4

Scénario 1 : Organismes ayant réalisé une EMC entre le 1er juillet 2025 et le 30 juin 2026 4

Scénario 2 : Organismes n'ayant jamais réalisé d'EMC ou ayant réalisé une EMC avant le 1er juillet 2025 5

Scénario 3 : Organismes créés après le 1er juillet 2026 5

Méthodes pour réaliser une EMC 6

Que doit contenir un résumé de l'EMC 6

Exigence 3 : Signaler au directeur général de la sécurité de l'information (DGSI) du ministère des Services au public

Étape 1 : Repérer un cyberincident critique 7

Étape 2 : Signaler un cyberincident critique 9

Étape 3 : Informer les autres autorités, au besoin 10

Protection des documents recueillis en vertu de la Loi de 2024 visant à renforcer la sécurité et la confiance en matiè

Glossaire 11

Annexe 11

Exemple 1 : Rapport de cyberincident critique 11

Exemple 2 : Rapport de cyberincident critique (système de gestion des dossiers avec intégration de tiers) 12

Introduction

L'Ontario renforce de façon continue ses mesures de cybersécurité afin de protéger les données confiées aux organismes du secteur public. La *Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public* de l'Ontario a instauré la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*, entrée en vigueur le 29 janvier 2025.

La *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* jette les bases d'une collaboration et d'une coordination accrues en matière de cybersécurité entre le MSPEA et certains organismes du secteur public, notamment les conseils scolaires, les collèges, les universités, les hôpitaux publics de soins actifs, ainsi que les sociétés d'aide à l'enfance, y compris les organismes de bien-être des enfants et des familles autochtones.

Les exigences réglementaires entreront en vigueur le 1er juillet 2026.

Objet

Le présent document d'orientation a pour objet d'aider les organismes du secteur parapublic visés à comprendre et à respecter les trois nouvelles exigences réglementaires prévues par la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*, lesquelles s'inscrivent au cœur du programme de cybersécurité de tout organisme.

Exigence 1 : Désigner et communiquer au DGSI du MSPEA une personne-ressource principale ainsi qu'un suppléant en matière de cybersécurité.

Exigence 2 : Réaliser des évaluations de la maturité en matière de cybersécurité (EMC) et en transmettre les résultats au DGSI du MSPEA.

Exigence 3 : Signaler au DGSI du MSPEA tout incident critique de cybersécurité dès sa survenance.

Le présent document décrit, étape par étape, les processus à suivre ainsi que les échéanciers de signalement applicables aux trois exigences. Lorsque le règlement ne précise pas des délais, ce document propose des échéanciers recommandés et des pratiques exemplaires.

Les organismes du secteur parapublic de l'Ontario tenus de se conformer aux nouvelles exigences réglementaires comprennent :

- les conseils scolaires
- les collèges
- les universités
- les hôpitaux de soins actifs et l'Institut de cardiologie de l'Université d'Ottawa
- les sociétés d'aide à l'enfance, y compris les organismes de bien-être des enfants et des familles autochtones

D'autres organismes peuvent également s'appuyer sur ces exigences et ces lignes directrices sur une base volontaire.

Site Web de Cybersécurité Ontario

Le site Web de Cybersécurité Ontario met à la disposition des organismes du secteur parapublic des conseils, des repères, des ressources éducatives ainsi que d'autres outils gratuits.

Toute personne-ressource qui n'est pas encore inscrite peut créer un compte en suivant le processus d'inscription en ligne et en sélectionnant l'option d'authentification unique. Cette authentification permet aux utilisateurs d'accéder au site au moyen des identifiants fournis par leur organisme du secteur parapublic et de confirmer leur appartenance à l'organisme en question. Pour en bénéficier, les utilisateurs doivent s'inscrire au moyen des identifiants établis par leur organisme (le nom de domaine du courriel doit correspondre au domaine officiel de l'organisme).

Nouvelles exigences prévues par la Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique

Exigence 1 : Désigner une personne-ressource principale et un suppléant en matière de cybersécurité

Étape 1 : Désigner une personne-ressource adéquate

Les organismes visés doivent désigner une personne-ressource principale et un suppléant qui :

1. approuvera le résumé de l'évaluation de la maturité en matière de cybersécurité de l'organisme avant sa transmission au DGSI du MSPEA;
2. assurera la liaison avec le Centre des opérations en matière de cybersécurité (COC) du MSPEA pour toute question liée à la cybersécurité, notamment dans le cas d'un incident critique.

Le Règlement en matière de cybersécurité pris en application de la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* exige que les personnes désignées à titre de personne-ressource principale ou de suppléant occupent un poste de cadre supérieur et disposent d'un pouvoir décisionnel en matière de cybersécurité au sein de l'organisme. Ces personnes doivent également :

- bien comprendre les activités de l'organisme ainsi que ses technologies de l'information;
- appartenir à l'organisme;
- posséder une connaissance adéquate de la nature des incidents de cybersécurité, le cas échéant.

Les organismes ne sont pas tenus de recruter du nouveau personnel pour agir en tant que personne-ressource principale ou suppléant. Elles peuvent désigner une personne déjà responsable de la cybersécurité. Selon leurs fonctions et leurs responsabilités, les employés occupant l'un des postes énumérés ci-dessous peuvent être désignés par leur organisme comme personne-ressource ou suppléant :

- Postes de direction, notamment :
  - Directeur général
  - Directeur général de l'information
  - Directeur général de la technologie
  - Directeur général de la sécurité de l'information
- Directeurs et chefs
- Surintendants d'écoles
- Chefs et présidents de collèges
- Présidents d'universités

Il est recommandé de ne pas désigner comme personne-ressource ou suppléant :

- des membres du conseil scolaire ou conseilleurs scolaires
- des tiers, sous-traitants externes ou consultants
- des employés n'occupant pas un poste de cadre supérieur

Étape 2 : Informer la Division de la cybersécurité du MSPEA

Les organismes peuvent transmettre au DGSI du MSPEA les coordonnées de leur personne-ressource principale et de leur suppléant par l'entremise du site Web de Cybersécurité Ontario, en fournissant les renseignements suivants :

- nom de l'organisme
- prénom
- nom

- intitulé du poste
- numéro de téléphone professionnel
- adresse électronique professionnelle

Il est recommandé de transmettre les coordonnées de la personne-ressource principale et de son suppléant au plus tard dix (10) jours ouvrables après la date à laquelle le règlement s'applique pour la première fois à l'organisme.

Étape 3 : Modifier les renseignements

Dans le cas d'un changement concernant la personne-ressource principale ou le suppléant, ou de modification de leurs coordonnées, les organismes doivent mettre à jour ces renseignements dans un délai de dix (10) jours ouvrables suivant le changement, sur le site Web de Cybersécurité Ontario.

Exigence 2 : Réaliser des évaluations de la maturité en matière de cybersécurité

Les évaluations de la maturité en matière de cybersécurité (EMC) permettent de cerner, de mesurer et d'évaluer les forces, les faiblesses ainsi que le niveau de préparation d'un organisme en matière de cybersécurité afin d'atténuer et de gérer les risques.

Tous les organismes visés doivent :

1. réaliser une EMC initiale.
   - Les organismes ayant déjà réalisé une évaluation entre le 1er juillet 2025 et le 30 juin 2026 peuvent déposer un résumé de cette évaluation. Cette évaluation antérieure est réputée avoir été réalisée à la date d'entrée en vigueur initiale du règlement à l'égard de l'organisme.
   - Toutes les évaluations doivent se conformer au cadre de cybersécurité NIST CSF 2.0, approuvé par le DGSI du MSPEA. Si un organisme envisage de réaliser une EMC fondée sur un autre cadre, elle doit communiquer avec la Division de la cybersécurité du MSPEA par l'entremise du site Web de Cybersécurité Ontario.
2. préparer et déposer uniquement un résumé de l'EMC auprès du DGSI du MSPEA dans un délai de trente (30) jours ouvrables au moyen du site Web de Cybersécurité Ontario (voir les scénarios 1 à 3 ci-dessous).
   - Les organismes sont tenus de conserver l'intégralité des EMC à des fins internes, **sans** obligation de les soumettre.
   - Reportez-vous à la section « Que doit contenir un résumé de l'EMC ».
3. réaliser une EMC tous les deux ans après la première évaluation et déposer un résumé de chaque évaluation auprès du DGSI du MSPEA dans les trente (30) jours ouvrables suivant son achèvement.

Suivez les étapes ci-dessous selon le scénario correspondant à votre organisme.

Scénario 1 : Organismes ayant réalisé une EMC entre le 1er juillet 2025 et le 30 juin 2026

1. Les organismes relevant de ce scénario peuvent transmettre, sur le site Web de Cybersécurité Ontario, un résumé de l'EMC réalisée au DGSI du MSPEA, dans les trente (30) jours ouvrables suivant la date d'entrée en vigueur initiale du règlement à l'égard de l'organisme. Cette évaluation antérieure est réputée avoir été réalisée à la date d'entrée en vigueur initiale du règlement à l'égard de l'organisme.
2. Par la suite, elles doivent réaliser une EMC tous les deux (2) ans à compter de la date d'achèvement de la dernière évaluation.
3. Déposez un résumé dans les trente (30) jours ouvrables suivant chaque évaluation.

Exemple d’échéance : conseil scolaire ayant réalisé une EMC en 2025	
15 novembre 2025	School board completes a CMA.
1er juillet 2026	Entrée en vigueur du Règlement.
12 août 2026 (dans les 30 jours ouvrables suivant l’entrée en vigueur du Règlement)	Date limite pour déposer le résumé de l’EMC réalisée l’année précédente sur le site Web de Cybersécurité Ontario.
1er juillet 2028 (2 ans après l’achèvement de la première EMC)	Date limite pour réaliser la prochaine EMC.
Dans les 30 jours ouvrables suivant l’achèvement de l’EMC	Date limite pour déposer le résumé sur le site Web de Cybersécurité Ontario.
Tous les 2 ans à compter de la date d’achèvement de la dernière EMC	Réaliser une EMC et en déposer le résumé sur le site Web de Cybersécurité Ontario dans les 30 jours ouvrables suivant son achèvement.

Scénario 2 : Organismes n’ayant jamais réalisé d’EMC ou ayant réalisé une EMC avant le 1er juillet 2025

1. Les organismes doivent réaliser une EMC dans l’année suivant l’entrée en vigueur du Règlement (au plus tard le 1er juillet 2027), puis en déposer le résumé auprès du DGSI du MSPEA au moyen du site Web de Cybersécurité Ontario dans les trente (30) jours ouvrables suivant son achèvement.
2. Par la suite, elles doivent réaliser une EMC tous les deux (2) ans à compter de la date d’achèvement de la dernière évaluation.

Exemple d’échéance : hôpital n’ayant jamais réalisé d’EMC. L’hôpital doit réaliser son EMC initiale d’ici le 1er juillet 2027.	
1er avril 2027	L’hôpital réalise une EMC et dispose de 30 jours ouvrables pour en déposer le résumé.
13 mai 2027 (30 jours ouvrables plus tard)	Date limite pour déposer le résumé sur le site Web de Cybersécurité Ontario.
1er avril 2029 (2 ans plus tard)	Date limite pour que l’hôpital réalise la prochaine EMC.
Dans les 30 jours ouvrables suivant l’achèvement de l’EMC	Date limite pour déposer le résumé sur le site Web de Cybersécurité Ontario.
Tous les 2 ans à compter de la date d’achèvement de la dernière EMC	Réaliser une EMC et en déposer le résumé sur le site Web de Cybersécurité Ontario dans les 30 jours ouvrables suivant son achèvement.

Scénario 3 : Organismes créés après le 1er juillet 2026

1. Ces organismes doivent réaliser une EMC dans l’année suivant leur création et en déposer le résumé auprès du DGSI du MSPEA au moyen du site Web de Cybersécurité Ontario dans les trente (30) jours ouvrables suivant son achèvement.
2. Par la suite, elles doivent réaliser une EMC tous les deux (2) ans à compter de la date d’achèvement de la dernière EMC et en déposer le résumé dans les trente (30) jours ouvrables suivant sa réalisation.

Exemple d’échéance : nouvelle société d’aide à l’enfance (SAE), n’ayant jamais réaliser une EMC	
15 août 2026	Création de la SAE. Elle dispose jusqu’au 14 août 2027 pour réaliser sa première EMC.
4 mai 2027	La SAE réalise sa première EMC.
15 juin 2027 (30 jours ouvrables plus tard)	Date limite pour déposer le résumé de la première EMC sur le site Web de Cybersécurité Ontario.
4 mai 2029 (2 ans après l’achèvement de la dernière EMC)	Date limite pour réaliser la prochaine EMC.
Dans les 30 jours ouvrables suivant l’achèvement de l’EMC	Date limite pour déposer le résumé sur le site Web de Cybersécurité Ontario.
Tous les 2 ans à compter de la date d’achèvement de la dernière EMC	Réaliser une EMC et en déposer le résumé sur le site Web de Cybersécurité Ontario dans les 30 jours ouvrables suivant son achèvement.

Méthodes pour réaliser une EMC :

A. Réaliser une auto-évaluation

Certains organismes réalisent leurs propres EMC, ou des évaluations comparables, dans le cadre de leur gestion des risques organisationnels, des exigences de leur assureur ou d’évaluations nationales.

Ces auto-évaluations peuvent servir de base au résumé de l’EMC de l’organisme, à condition qu’elles fournissent les renseignements requis (voir la section « Que doit contenir un résumé de l’EMC ») et qu’elles soient conformes au cadre NIST CSF 2.0, sauf approbation contraire du DGSI du MSPEA pour l’utilisation d’un autre cadre.

Les organismes qui ne disposent d’aucun outil d’évaluation peuvent utiliser l’outil d’EMC gratuit, accessible sur le site Web de Cybersécurité Ontario.

Cet outil s’accompagne de documents d’orientation visant à en faciliter l’utilisation.

L’accès à la page de l’outil d’EMC offre également un accompagnement supplémentaire aux organismes pour la réalisation de leur EMC.

B. Évaluation par un fournisseur externe ou un tiers

Un organisme peut recourir à un fournisseur externe ou à un tiers pour réaliser une EMC, à condition que celle-ci soit conforme au cadre NIST CSF 2.0, approuvé par le DGSI du MSPEA. Les EMC qui ne reposent pas sur le cadre NIST CSF risquent de ne pas être acceptées. Si un organisme envisage de réaliser une EMC en fonction d’un autre cadre, elle doit communiquer avec la Division de la cybersécurité du MSPEA par l’entremise du site Web de Cybersécurité Ontario.

i. Organismes qui fournissent déjà des EMC à un ministère de tutelle

Certains organismes disposent déjà de mécanismes de signalement leur permettant de transmettre des EMC à leur ministère de tutelle. Sauf indication contraire de ce ministère, les organismes doivent continuer à suivre leurs procédures habituelles. En complément des obligations de signalement au ministère de tutelle, ils doivent également réaliser des EMC et en déposant les résumés auprès du MSPEA, conformément aux exigences du Règlement pris en application en vertu de la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*.

Que doit contenir un résumé de l’EMC

La personne-ressource principale de l’organisme doit approuver le résumé de l’EMC avant sa transmission au DGSI du MSPEA.

Le résumé doit comprendre :

- une brève description de la méthode utilisée pour réaliser l'évaluation
- le nom du modèle ou du cadre utilisé
- l'indice global de cybermaturité de l'organisme
- un résumé des autres scores issus de l'évaluation, notamment ceux liés à la capacité de l'organisme à gouverner, cerner et détecter les risques de cybersécurité, ainsi qu'à protéger, réagir et se rétablir face auxdits risques
- un résumé des domaines que l'organisme prévoit d'améliorer

Les organismes ne sont **pas** tenus de déposer l'EMC complète, mais il est recommandé d'en conserver les documents à des fins internes.

Les organismes qui utilisent l'outil d'EMC gratuit de la Division de la cybersécurité du MSPEA reçoivent un résumé prêt à être déposé.

Une fois le résumé parachevé, l'organisme peut transmettre le résumé de l'EMC au DGSI du MSPEA par l'entremise du site Web de Cybersécurité Ontario.

Pour de plus amples renseignements sur l'outil d'EMC, consultez la page Outil d'EMC sur le site Web de Cybersécurité Ontario.

Exigence 3 : Signaler au DGSI du MSPEA tout incident critique de cybersécurité

Le signalement des cyberincidents critiques au DGSI du MSPEA permet à la Division de la cybersécurité du MSPEA de fournir des conseils, des directives et des services à l'organisme concerné.

Ce signalement constitue un élément essentiel du processus de réponse aux incidents critiques de cybersécurité et permet ce qui suit :

- informer le gouvernement de la nature, du volume et de la gravité des menaces à l'échelle du secteur public;
- assurer le partage sécurisé et adéquat de renseignements sur les menaces susceptibles de présenter un risque élevé ou d'exiger des efforts de rétablissement importants;
- aider les différents secteurs à mieux cerner les lacunes et les priorités d'amélioration;
- permettre au MSPEA de fournir le soutien nécessaire pour répondre aux incidents critiques et en atténuer les effets de manière rapide et efficace.

Dès qu'un organisme confirme la survenance d'un cyberincident critique, il doit le signaler au DGSI du MSPEA dans les plus brefs délais raisonnables et, au plus tard, dans un délai de 72 heures.

Étape 1 : Repérer un cyberincident critique

Lorsqu'un organisme désigne un incident comme un cyberincident, il doit déterminer s'il revêt un caractère critique. Dans le cas d'une incertitude, il doit signaler l'incident au DGSI du MSPEA en respectant les délais indiqués ci-dessus.

Conformément au Règlement, un cyberincident critique est considéré comme critique lorsqu'un organisme constate qu'il a eu une incidence sur :

(i) sur la sécurité, la continuité, la confidentialité, l'intégrité ou la disponibilité de l'information numérique recueillie, utilisée, conservée ou divulguée par l'entité,

(ii) l'infrastructure qui héberge ou transmet les renseignements numériques recueillis, utilisés, conservés ou communiqués.

Un cyberincident critique doit également **satisfaire à au moins l'un** des critères suivants :

(i) **Perturbation des services** : l'incident entraîne des répercussions négatives importantes sur la prestation des services publics par l'organisme.

(ii) **Risque pour la sécurité** : l'incident présente un risque pour la sécurité publique.

(iii) **Efforts de rétablissement importants ou activation d'un plan d'intervention** : l'incident nécessite des efforts substantiels pour rétablir les renseignements numériques ou l'infrastructure ou entraîne l'activation d'un plan d'intervention en cas d'incident lié à la cybersécurité.

(iv) **Atteinte à la réputation** : l'incident présente un risque important de nuire à la réputation de l'organisme et à la confiance du public.

Au regard de ces critères, les répercussions d'un incident critique peuvent notamment inclure :

- des pertes financières pour des personnes ou des communautés;
- l'utilisation abusive ou la perte de données à caractère personnel
- des poursuites judiciaires visant des personnes ou des organismes
- l'interruption suivie de la restauration totale ou partielle d'un service
- un accès non autorisé à des données à caractère personnel
- une couverture médiatique négative

Exemples de cyberincidents critiques devant être signalés

Outre les facteurs ci-dessus, les exemples suivants illustrent des situations pouvant constituer des cyberincidents critiques à signaler au MSPEA.

Exemple	Justification du signalement
Une attaque par rançongiciel compromet le système d'un hôpital public, rend les dossiers des patients inaccessibles, entraîne l'annulation d'interventions chirurgicales et met en péril les soins. L'organisme déclenche alors des plans de continuité des activités (PCA) ou des plans équivalents.	• Incidence significative sur la prestation des services publics. • Risque pour la sécurité publique. • Efforts de rétablissement importants.
Une violation de données expose les adresses confidentielles de personnes placées sous protection familiale, créant un risque de préjudice physique.	• Risque pour la sécurité publique. • Efforts de rétablissement importants.
Une attaque par hameçonnage entraîne le vol d'identifiants d'administrateur, permettant l'exfiltration et la suppression d'informations financières critiques.	• Risque pour la sécurité publique. • Efforts de rétablissement importants.
Une attaque par logiciel malveillant contraint une grande université à fermer son réseau pendant deux semaines, perturbe l'enseignement en ligne et nécessite des efforts importants pour rétablir les services.	• Risque important d'atteinte à la réputation. • Incidence significative sur la prestation des services publics. • Efforts de rétablissement importants.
Une attaque par déni de service prolongé perturbe des services et des infrastructures essentiels à la mission et entraîne l'activation d'un plan de continuité des activités (PCA).	• Risque pour la sécurité publique. • Efforts de rétablissement importants. • Incidence significative sur la prestation des services publics.
Une cyberattaque visant un fournisseur de biens ou de services perturbe des services essentiels à la mission.	• Incidence significative sur la prestation des services publics. • Risque important d'atteinte à la réputation.

Étape 2 : Signaler un cyberincident critique

Un organisme doit signaler tout cyberincident critique au plus tard 72 heures après en avoir confirmé la survenance. Tout membre de l'organisme inscrit sur le site Web de Cybersécurité Ontario peut effectuer ce signalement.

Les membres des organismes du secteur parapublic peuvent créer un compte en suivant le processus d'inscription en ligne et en sélectionnant l'option d'authentification unique. Cette authentification permet aux utilisateurs d'accéder au site au moyen des identifiants fournis par leur organisme du secteur parapublic et de confirmer leur appartenance à l'organisme en question. Pour en bénéficier, les utilisateurs doivent s'inscrire au moyen des identifiants établis par leur organisme (le nom de domaine du courriel doit correspondre au domaine officiel de l'organisme).

À qui signaler un cyberincident critique :

- Organismes qui signalent déjà les cyberincidents critiques à un ministère de tutelle
    - Certains organismes disposent déjà de mécanismes de signalement les obligeant à signaler les cyberincidents critiques à leur ministère de tutelle. Sauf indication contraire de ce ministère, les organismes doivent continuer à suivre leurs procédures habituelles, tout en signalant également les cyberincidents critiques au DGSI du MSPEA conformément aux exigences réglementaires.
- Organismes qui ne signalent pas les cyberincidents critiques à un ministère de tutelle
    - Ces organismes doivent signaler les cyberincidents critiques directement au DGSI du MSPEA, conformément aux exigences réglementaires.

Que doit contenir le rapport de cyberincident critique

- le nom de la personne-ressource principale et du suppléant de l'organisme (le signalement peut être effectué par tout membre de l'organisme autre que la personne-ressource principale et le suppléant, inscrit sur le site Web de Cybersécurité Ontario);
- le nom de l'organisme
- le nom du ministère de tutelle
- la date et l'heure de survenance de l'incident
    - Il s'agit du moment où des indicateurs de compromission ou d'autres activités suspectes ont permis de le détecter;
- la date et l'heure de confirmation de l'incident
    - Il s'agit du moment où l'organisme a établi qu'un cyberincident critique s'était produit;
- une description générale de l'incident, y compris les raisons pour lesquelles il est considéré comme critique
- une description générale du type de renseignements concernés ou compromis, le cas échéant.

Consultez l'annexe pour des exemples de rapports de cyberincident critique

Après le signalement

Après avoir signalé un cyberincident critique, l'organisme doit continuer à surveiller la situation et appliquer ses procédures internes de réponse aux incidents.

Lorsque l'organisme ne dispose pas de plan ou de procédure formalisée, il doit prendre des mesures pour contenir l'incident et limiter les risques pour ses systèmes et ses réseaux. Ces mesures peuvent notamment inclure :

- la désactivation de comptes
- la déconnexion d'appareils des réseaux
- l'arrêt de serveurs, d'applications ou de systèmes présentant une vulnérabilité

Les organismes ayant signalé un cyberincident critique peuvent également être amenés à :

- fournir, au besoin, des renseignements supplémentaires concernant l'incident signalé au DGSI du MSPEA;
  - Les renseignements seraient nécessaires pour saisir l'ampleur et les répercussions de l'incident et de déterminer le niveau d'intervention requis par le MSPEA;
  - Des renseignements techniques clés peuvent être partagés sous forme anonymisée (par exemple, indicateurs de compromission, modes opératoires, séquence d'attaque) afin de renforcer les capacités de défense de l'écosystème de cybersécurité;
- poursuivre la surveillance de l'incident et informer le DGSI du MSPEA de toute évolution significative;
- participer, le cas échéant, à un examen postérieur à l'incident avec la Division de la cybersécurité du MSPEA afin d'améliorer les processus du gouvernement de l'Ontario et sa gestion des incidents futurs.

Étape 3 : Informer les autres autorités, au besoin

Le signalement d'un cyberincident critique au MSPEA ne dispense pas l'organisme de ses autres obligations de signalement. Il lui incombe de signaler l'incident aux autorités compétentes.

Selon la nature et les conséquences de l'incident, le plan d'intervention interne peut exiger d'informer les clients et les parties concernées, les fournisseurs, les forces de l'ordre, notamment lorsque l'incident constitue une infraction, d'autres autorités provinciales ou fédérales, par exemple le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) dans le cas d'une atteinte à la vie privée ou de communication de renseignements personnels.

Les organismes doivent effectuer ces signalements selon les besoins.

Protection des documents recueillis en vertu de la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*

La *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et l'accès à *Loi de 1990 sur l'information municipale et la protection de la vie privée* (LAIMPVP) imposent aux institutions visées de protéger les renseignements personnels et de donner accès aux informations qu'elles détiennent dans le cadre des demandes d'accès à l'information.

Le gouvernement a proposé des modifications à la LAIPVP et à la LAIMPVP afin de mieux prendre en compte les risques liés à la cybersécurité et à la protection de la vie privée. Si elles sont adoptées, ces modifications empêcheraient la divulgation, dans le cadre d'une demande d'accès à l'information, de certains documents préparés ou recueillis en vertu de ces règlements. Elles contribueraient ainsi à prévenir toute divulgation inadéquate, toute utilisation abusive ou tout accès non autorisé à des renseignements sensibles susceptibles de présenter un risque pour la cybersécurité. Ces modifications excluraient notamment du champ d'application de la LAIPVP et de la LAIMPVP :

A) les renseignements relatifs à la personne-ressource en matière de cybersécurité et à son suppléant

B) les évaluations de la maturité en matière de cybersécurité et leurs résumés

C) les logiciels numériques utilisés par les conseils scolaires qui traitent des renseignements personnels d'enfants (consulter le Règlement de l'Ontario 52/26);

D) tout autre document dont la divulgation pourrait compromettre la cybersécurité.

Glossaire

Secteur parapublic : organisme financé par le gouvernement de l'Ontario sans faire partie de l'administration gouvernementale. Il s'agit notamment des hôpitaux de soins actifs, des conseils scolaires, des collèges et universités, ainsi que des sociétés d'aide à l'enfance, y compris les organismes de bien-être des enfants et des familles autochtones.

Directeur général de la sécurité de l'information : fonctionnaire qui assure la direction générale, la supervision stratégique et l'excellence opérationnelle de la Division de la cybersécurité au sein de la fonction publique de l'Ontario (FPO). Le DGSI dirige la Division de la cybersécurité qui met en œuvre un programme exhaustif de gestion des risques cybernétiques visant à anticiper, cerner et contrer les menaces, ainsi qu'à permettre au gouvernement de l'Ontario de fonctionner de manière sécurisée tout en respectant ses engagements en matière de services numériques. Le DGSI fournit également des conseils en gestion des risques et des solutions innovantes en cybersécurité à la FPO et au secteur parapublic afin d'assurer une prestation sécurisée des services publics au sein d'un écosystème numérique.

Cyberincident critique :

(1) Incident qui :

(a) a eu des répercussions :

(i) soit sur la sécurité, la continuité, la confidentialité, l'intégrité ou la disponibilité de l'information numérique recueillie, utilisée, conservée ou divulguée par l'entité,

(ii) soit sur l'infrastructure servant à stocker ou à transmettre l'information numérique recueillie, utilisée, conservée ou divulguée par l'entité;

(b) remplit au moins l'un des critères énoncés au paragraphe (2).

(2) Pour l'application de l'alinéa b) de la définition de « cyberincident critique » au paragraphe (1), doit être rempli au moins l'un des critères suivants :

1. L'incident entraîne des conséquences défavorables importantes pour la prestation des services publics offerts par l'entité.
2. L'incident présente un risque pour la sécurité publique.
3. L'incident nécessite ou entraîne des efforts considérables de la part de l'entité pour le rétablissement de l'information numérique ou de l'infrastructure connexe ou pour l'activation de plans d'intervention en cas d'incident lié à la cybersécurité.
4. L'incident risque considérablement de nuire à la réputation de l'entité et à la confiance du public à son égard.

Évaluation de la maturité en matière de cybersécurité (EMC) : Évaluation du statut ou des progrès d'une entité du secteur public prescrite en ce qui concerne la cybersécurité, qui est effectuée conformément aux normes de l'industrie ou aux pratiques exemplaires qu'appuie le directeur général de la sécurité de l'information du ministère.

Site Web de Cybersécurité Ontario : Le **site Web de Cybersécurité Ontario** est administré par le **Centre d'excellence de l'Ontario pour la cybersécurité** afin de renforcer la sensibilisation et de répondre aux enjeux de cybersécurité auxquels fait face l'ensemble du secteur parapublic.

Cadre de cybersécurité (CSF) 2.0 du National Institute of Standards and Technology (NIST) : Cadre qui fournit des directives à l'intention du secteur, des organismes gouvernementaux et d'autres organismes pour la gestion des risques liés à la cybersécurité. Il propose une taxonomie de résultats de haut niveau que tout organisme peut utiliser pour mieux comprendre, évaluer, prioriser et communiquer ses activités en matière de cybersécurité.

Annexe

Exemple 1 : Rapport de cyberincident critique

Nom de la personne-ressource principale et du suppléant

Nom 1 (principal)
Nom 2 (suppléant)

Nom de l’organisme

Collège ABC

Nom du ministère de tutelle

Ministère des Collèges et Universités, de l’Excellence en recherche et de la Sécurité

Date et heure de survenance de l’incident

- Le 10 juillet 2025, une attaque par rançongiciel est détectée sur le réseau de l’organisme.
- 10 juillet, 4 h 45 – Détection d’une connexion au RPV non autorisée.

Date et heure de confirmation de l’incident

- 10 juillet, 6 h – Détection d’un chiffrement massif de fichiers.
- 10 juillet, 8 h 30 – Découverte d’une demande de rançon sur les serveurs de fichiers.

Description générale de l’incident, y compris les raisons pour lesquelles il est considéré comme critique

L’attaque a chiffré les serveurs de fichiers ainsi que les systèmes de sauvegarde, paralysant ainsi les opérations. L’incident est considéré comme critique en raison de la perturbation des activités, du risque élevé d’exposition des données et de son incidence financière.

Description générale du type de renseignements concernés ou compromis, le cas échéant

Documents financiers, y compris les budgets, ainsi que des communications par courriel et leurs pièces jointes. L’organisme a activé son plan d’intervention, mobilisé des équipes juridiques et restauré les systèmes à partir de sauvegardes hors ligne.

Exemple 2 : Rapport de cyberincident critique (système de gestion des dossiers avec intégration de tiers)

Nom de la personne-ressource principale et du suppléant

Nom 1 (principal)
Nom 2 (suppléant)

Nom de l’organisme

Société d’aide à l’enfance ABC

Nom du ministère de tutelle

Ministère des Services à l’enfance et des Services sociaux et communautaires

Date et heure de survenance de l’incident

Le 27 juin 2025, à 11 h – compromission du système du fournisseur.

Date et heure de confirmation de l’incident

Le 27 juin, à 15 h – déclenchement des alertes.

Description générale de l’incident, y compris les raisons pour lesquelles il est considéré comme critique

Le 27 juin 2025, la Société d’aide à l’enfance ABC détecte des tentatives d’accès anormaux aux données via un fournisseur tiers intégré à son système de gestion des dossiers. L’enquête révèle que le système du fournisseur a été compromis, permettant un accès non autorisé à des dossiers clients sensibles.

L’incident est classé comme critique en raison de la divulgation de renseignements confidentiels liés à des dossiers d’aide à l’enfance.

L’organisme désactive l’accès à l’API du fournisseur.

La SAE ABC informe les familles et les tuteurs concernés, le ministère de tutelle ainsi que le Commissaire à l’information et à la protection de la vie privée de l’Ontario et procède à une analyse des journaux de l’API.

Description générale du type de renseignements concernés ou compromis, le cas échéant.

- noms et dates de naissance des enfants pris en charge
- notes des travailleurs sociaux
- coordonnées des familles et des tuteurs.