Elections Ontario

Politique sur la cybersécurité

Bureau du directeur général des élections
Élections Ontario
Juillet 2026

Historique des versions

Numéro de révision	Date de révision	Date d'entrée en vigueur	Description des modifications	Responsable de l'approbation
1.0		27 juillet 2026	Document original	Greg Essensa – DGE

TABLE DES MATIÈRES

Section 1 : Introduction

Élections Ontario (EO) s'engage à protéger ses systèmes d'information numériques et son infrastructure contre les accès non autorisés, les atteintes à la sécurité et les cyberattaques. EO priorise la sécurité numérique afin de protéger la confidentialité et la sécurité des renseignements personnels, d'assurer la continuité de la prestation des services électoraux et de maintenir la confiance des Ontariens et Ontariennes.

EO maintient l'intégrité de son environnement de technologie de l'information (TI) en établissant des exigences de sécurité qui réduisent la vulnérabilité et renforcent la résilience face aux cybermenaces actuelles et futures, y compris, mais sans s'y limiter, les logiciels malveillants, l'hameçonnage, les logiciels de rançon, les attaques d'États-nations et l'exploitation de la chaîne d'approvisionnement.

La présente politique sur la cybersécurité a pour objet de prévenir les perturbations et les préjudices aux systèmes, aux réseaux et à l'infrastructure d'EO, notamment les produits numériques et les renseignements. Elle définit les exigences obligatoires, les approbations ainsi que les rôles et responsabilités d'EO en matière de gestion des cybermenaces.

Section 2 : Principes

Élections Ontario protège ses actifs informationnels afin de remplir son mandat législatif visant à garantir des élections provinciales justes, sûres et transparentes, et à préserver l'intégrité électorale pour les Ontariens et Ontariennes.

EO se conforme aux politiques connexes du gouvernement de l'Ontario, dans la mesure du possible et du réalisable, y compris les normes de technologies de l'information du gouvernement de l'Ontario (NTI-GO).

Résilience et atténuation des risques

EO s'engage à veiller à ce que ses systèmes d'information et son infrastructure numériques puissent anticiper les cyberperturbations, y résister, s'en rétablir services et s'y adapter. EO privilégie une prise de décision fondée sur l'analyse des risques afin de maintenir un environnement de TI sécurisé et stable, en s'attaquant de manière proactive aux menaces connues et potentielles.

Vie privée et protection des données

EO prend tous les moyens raisonnables pour protéger les renseignements personnels de manière proportionnelle à leur sensibilité afin de maintenir la confiance du public. EO protège toutes les composantes de son environnement de TI contre toute compromission afin de maintenir la confidentialité, l'intégrité et la disponibilité de l'information.

Réactivité et préparation opérationnelle

EO adapte continuellement son approche afin de tenir compte des risques en matière de cybersécurité et d'un contexte technologique en constante mutation. Étant donné la nature particulière des activités de terrain, la direction d'EO peut adopter des pratiques et des procédures propres à EO afin de protéger la sécurité de l'information et d'agir dans l'intérêt du public.

Section 3 : Portée

La présente politique s'applique aux utilisateurs et utilisatrices des systèmes, des postes de travail, des réseaux, des appareils et des données appartenant à EO, y compris :

- Tous les réseaux et l'infrastructure au siège social et dans les bureaux de terrain d'EO
- L'ensemble du personnel (permanent et temporaire), des consultants et consultantes, des utilisateurs et utilisatrices autorisé·e·s ayant accès au réseau et à l'infrastructure d'EO, ainsi que du personnel électoral, notamment les personnes retenues par EO pour gérer le processus électoral lors des élections générales et partielles (par exemple, directeur ou directrice du scrutin, secrétaire du scrutin, personnel de terrain, personnel des bureaux de vote), ci-après désigné comme le personnel d'EO
- Toutes les composantes d'un environnement de TI qui stockent, traitent ou transmettent des renseignements, qu'elles soient gérées directement par EO ou par des fournisseurs et des entrepreneur·e·s pour le compte d'EO.

La présente politique n'énonce pas de lignes directrices pour la mise en œuvre des mesures de protection en cybersécurité, y compris la surveillance des cybermenaces. L'équipe de cybersécurité d'EO fournit des conseils, des processus et des procédures en matière de cybersécurité.

La présente politique n'aborde ni la gestion des atteintes à la vie privée et à la sécurité ni les interventions requises en cas d'incident de cybersécurité. Consultez les documents suivants pour de plus amples détails :

- Le Protocole de gestion des atteintes à la vie privée et à la sécurité présente de plus amples renseignements sur les responsabilités du personnel d'EO et des fournisseurs de services en matière de gestion des atteintes.
- Le *Plan d'intervention en cas d'incident de cybersécurité* présente des directives classifiées sur l'intervention en cas d'incident à l'intention des premier·ère·s intervenant·e·s autorisé·e·s.

La présente politique ne traite pas de la protection ou de la conservation des renseignements personnels sous des formats non numériques sous la garde et le contrôle d'EO. Consultez les documents suivants pour de plus amples détails :

- La Politique de protection de la vie privée d'Élections Ontario présente de plus amples renseignements sur la collecte, l'utilisation, la

divulgation, la conservation et la protection des renseignements personnels, sous toutes leurs formes.

- Le Calendrier de conservation des dossiers contient de plus amples renseignements sur le stockage, la conservation et l'élimination des documents d'EO.

Section 4 : Dispositions obligatoires

Élections Ontario s'engage à respecter les normes de sécurité suivantes :

4.1 Évaluation des cyberrisques et approbation

- EO veille à ce que les risques soient maintenus à un niveau acceptable en mettant en œuvre un processus de gestion des cyberrisques qui évalue en continu la sécurité des systèmes d'information et de l'infrastructure.

- Le degré de tolérance au risque d'EO est défini et approuvé par le directeur général ou la directrice générale des élections. Tout risque dépassant le degré de tolérance requiert une approbation officielle pour l'éviter, l'accepter/atténuer ou le transférer. Un rapport régulier sur les cyberrisques est remis à la direction d'EO.

- EO désigne des personnes-ressources principales et suppléantes en cybersécurité, qui sont responsables des communications avec le ministère des Services au public et aux entreprises et de l'Approvisionnement EO fournit un avis de tout changement apporté aux personnes-ressources désignées dans un délai de dix (10) jours ouvrables.

- EO effectue une évaluation de la maturité en cybersécurité, au besoin, selon son degré de tolérance au risque. Conformément aux considérations sur le risque organisationnel et aux exigences en matière de gouvernance, la personne-ressource désignée par EO remet un résumé de l'évaluation au responsable de la sécurité des systèmes d'information du ministère des Services au public et aux entreprises et de l'Approvisionnement une fois l'évaluation terminée.

4.2 Sensibilisation à la sécurité et formation

- EO veille à ce que des mesures soient en place pour approfondir les connaissances et la sensibilisation à la cybersécurité du personnel d'EO afin qu'il puisse repérer les enjeux et intervenir en conséquence.

- Le personnel d'EO doit comprendre les responsabilités en matière de sécurité de l'information en vertu de la présente politique et des autres politiques, normes et procédures pertinentes, y compris celles énoncées dans les documents suivants :

    - Politique d'utilisation acceptable des ordinateurs et des technologies

    - Politique de protection de la vie privée d'EO

- Protocole de gestion des atteintes à la vie privée et à la sécurité

- EO offre une formation en sécurité fondée sur les rôles, des tests simulés et des outils uniquement au personnel d'EO dont les fonctions exigent l'exercice de responsabilités en matière de sécurité et le respect des exigences de la présente politique.

4.3 Contrôles d'accès et de sécurité

- EO met en œuvre un processus d'approbation documenté conformément à la Politique sur le contrôle de l'accès aux TI et la gestion de l'accès des utilisateurs pour autoriser le personnel et les appareils d'EO qui nécessitent un accès aux systèmes d'information d'EO.

- EO met en œuvre des mesures de protection appropriées pour sécuriser les systèmes d'information numériques et l'infrastructure, dans une mesure conforme aux exigences énoncées dans le présent document ou dans d'autres politiques d'EO (tel qu'il est énuméré à la section 7) et dans la législation applicable.

- EO met en œuvre des mesures de protection supplémentaires dès qu'une évaluation de la menace et des risques, un plan de traitement des cybermenaces, un rapport de gestion des vulnérabilités, une évaluation des facteurs relatifs à la vie privée ou une autre évaluation permet de cerner des risques pour la sécurité du système.

4.4 Sécurité en matière de fournisseurs de services et de tiers

- EO inclut des clauses de sécurité conformes aux exigences de la présente politique et aux normes applicables dans les contrats conclus avec les fournisseurs de services ayant accès aux systèmes d'information numériques et à l'infrastructure d'EO ou qui en partagent la garde. Ces exigences contractuelles doivent également préciser qu'elles s'appliquent à tout sous-traitant sur lequel les fournisseurs de services s'appuient pour offrir des services à EO ou aux électeurs et électrices.

- EO effectue une diligence raisonnable et un examen continu de tous les fournisseurs de services ayant accès aux systèmes d'information numériques ou aux données d'EO. Les fournisseurs à risque élevé, tel qu'il est défini par l'évaluation des risques, sont surveillés en continu.

- EO exige que les fournisseurs de services donnent un préavis de tout changement apporté à la prestation des services, y compris les changements à l'infrastructure technique, à l'emplacement ou au territoire de compétence où les renseignements sont traités, à la

reconfiguration des services ou au recours à d'autres parties externes (par exemple, de nouveaux sous-traitants pour appuyer la prestation des services).

4.5 Disponibilité et fiabilité des systèmes et des ressources d'information

- EO emploie son Plan de continuité des activités pour assurer une reprise rapide et ordonnée à la suite d'une perturbation, d'une urgence ou d'une panne causée par un incident de cybersécurité, et rétablir les fonctions opérationnelles essentielles ainsi que la prestation des services conformément aux normes de qualité et de disponibilité prévues.

- EO veille à ce que les systèmes et applications appuyant les fonctions et services essentiels disposent de plans de reprise après sinistre opérationnels, vérifiés et mis à l'essai afin de rétablir le fonctionnement normal en cas d'incident de cybersécurité. Les plans sont examinés et mis à l'essai périodiquement.

- EO crée et conserve des copies de sauvegarde des renseignements nécessaires pour vérifier ou remplacer des documents qui ont été falsifiés, perdus ou détruits avant leur date d'élimination prévue, conformément à la Procédure de stockage, de transfert et de destruction sécurisés des renseignements personnels et à la législation applicable.

4.6 Surveillance et signalement des incidents de cybersécurité

- EO contrôle les systèmes d'information numériques et l'infrastructure afin de détecter et de prévenir les atteintes potentielles à la sécurité.

- EO met en œuvre un plan d'intervention en cas d'incident de cybersécurité, advenant une atteinte à la sécurité liée à un cyberévénement. Ce plan précise clairement les rôles et responsabilités des intervenants autorisés et les procédures d'escalade à appliquer auprès des parties pertinentes.

- EO signale les incidents de cybersécurité critiques au Responsable de la sécurité des systèmes d'information du ministère des Services au public et aux entreprises et de l'Approvisionnement dans les soixante-douze (72) heures suivant leur confirmation, y compris tous les renseignements exigés par la réglementation.

- Conformément aux exigences et aux normes en matière de cybersécurité de la présente politique, celles de la Politique d'utilisation acceptable des ordinateurs et des technologies et celles de la Politique de protection de la vie privée d'EO, toute personne qui cause ou

contribue à des incidents de sécurité peut être tenue responsable si ses actions contreviennent à la formation reçue, aux exigences du poste, aux ententes, aux directives organisationnelles, aux politiques ou à la loi.

Section 5 : Rôles et responsabilités

5.1 Directeur général ou directrice générale des élections (DGE)

Le directeur général ou la directrice générale des élections assume les responsabilités suivantes :

- Adopter les politiques qui régissent l'engagement d'Élections Ontario à maintenir des systèmes d'information numériques et une infrastructure sécurisés et stables.
- Établir une orientation stratégique pour l'élaboration et la mise en œuvre de pratiques opérationnelles qui garantissent une application uniforme de la présente politique.
- Veiller à ce que les principes et les exigences de la présente politique soient respectés, appliqués et fassent l'objet de rapports.
- Approuver les évaluations des risques et les stratégies de gestion des risques, s'il y a lieu, sur avis du directeur général ou de la directrice générale de l'information, du ou de la chef de la cybersécurité et de l'équipe de direction d'EO.

5.2 Directeur général adjoint ou directrice générale adjointe des élections

Le directeur général adjoint ou la directrice générale adjointe des élections peut remplacer le directeur général ou la directrice générale des élections au besoin. Si cette personne agit à titre de directeur général ou de directrice générale des élections, le directeur général adjoint ou la directrice générale adjointe des élections assume les mêmes responsabilités que ce dernier ou cette dernière.

5.3 Directeur général ou directrice générale de l'information

Le directeur général ou la directrice générale de l'information assume les responsabilités suivantes :

- Élaborer la stratégie de cybersécurité d'EO, y compris des mesures d'efficacité.
- Fournir des directives sur les politiques et procédures de cybersécurité d'EO.
- Évaluer la conformité à la présente politique et aux normes.
- Approuver les évaluations des risques et les stratégies de gestion des risques, le cas échéant.

5.4 Directeur général ou directrice générale de la protection de la vie privée

Le directeur général ou la directrice générale de la protection de la vie privée assume les responsabilités suivantes :

- Orienter et appuyer les responsables des activités opérationnelles et des projets afin qu'ils comprennent leurs obligations en matière de protection de la vie privée, conformément à la Politique de protection de la vie privée d'EO, et les politiques et lignes directrices qui en découlent.
- Fournir un soutien ou une orientation sur les pratiques exemplaires en matière de protection de la vie privée en ce qui concerne la gestion des atteintes réelles ou potentielles à la vie privée et à la sécurité, y compris le processus, les lignes directrices et les outils nécessaires pour évaluer si une évaluation des facteurs relatifs à la vie privée est requise, et ce qu'elle devrait couvrir.

5.5 Directeurs

Les directeurs assument les responsabilités suivantes :

- Fournir des ressources pour maintenir un degré de contrôle en cybersécurité conforme à la présente politique.
- Cerner et mettre en œuvre tous les processus, procédures et contrôles relatifs aux normes de cybersécurité définies par la société et la présente politique.
- Soutenir la participation du personnel de cybersécurité et du personnel technique à la protection des actifs numériques, ainsi qu'au repérage, à la sélection et à la mise en œuvre de contrôles et de procédures de sécurité appropriés et rentables.
- Gérer les manquements à la présente politique et mettre en œuvre des mesures d'atténuation pour contenir les risques associés à la non-conformité à la présente politique.
- Mettre en œuvre les plans de continuité des activités et de reprise après sinistre liés à la cybersécurité.

5.6 Chef de la cybersécurité

La ou le chef de la cybersécurité assume les responsabilités suivantes :

- Élaborer et mettre en œuvre le programme de cybersécurité d'EO, qui comprend les tâches suivantes :
  - Fournir la coordination et l'expertise en matière d'intervention en cas d'incident.
  - Surveiller les réseaux afin de détecter les anomalies.
  - Surveiller les sources externes pour détecter des indications d'atteintes à la protection des données, de défigurations de sites Web, etc.
  - Assurer une communication continue avec les parties concernées.

  - Communiquer rapidement des avis sur les menaces et les vulnérabilités actuelles.
  - Dispenser du matériel de sensibilisation et des ressources de formation.
- Évaluer la conformité aux politiques de cybersécurité applicables et aux exigences législatives en matière de cybersécurité.
- Superviser la mise en œuvre des évaluations des risques et des activités de gestion des risques en matière de cybersécurité.
- Superviser la surveillance et l'évaluation des contrôles de sécurité mis en œuvre.
- Formuler des recommandations sur les volets liés à la cybersécurité des propositions et des autres documents contractuels relatifs à l'acquisition de produits et de services.
- Transmettre aux instances supérieures les préoccupations en matière de sécurité qui ne sont pas traitées adéquatement, conformément aux procédures applicables de signalement et d'escalade.
- Communiquer les renseignements sur les menaces aux parties concernées.
- Prendre part à l'examen et à l'élaboration des politiques et procédures d'EO qui ont des incidences sur la cybersécurité.

5.7 Personnel d'EO

Tout le personnel d'EO, notamment les personnes retenues par EO pour gérer le processus électoral pendant les élections générales et partielles (par exemple, directeur·rice du scrutin, secrétaire du scrutin, personnel de terrain, personnel des bureaux de vote), assument les responsabilités suivantes :

- Comprendre les contrôles de sécurité de base nécessaires pour protéger les systèmes d'information numériques et l'infrastructure d'EO.
- Protéger les systèmes d'information numériques et l'infrastructure afin de prévenir les accès non autorisés, les interruptions ou les modifications, le vol ou les dommages.
- Respecter les exigences et les normes de cybersécurité de la présente politique et des autres politiques et procédures pertinentes d'EO, y compris : Politique d'utilisation acceptable des ordinateurs et des technologies, Politique de protection de la vie privée d'EO et Politique sur le contrôle de l'accès aux TI et la gestion de l'accès des utilisateurs

- Signaler les incidents ou les vulnérabilités de cybersécurité soupçonnés, conformément au Protocole de gestion des atteintes à la vie privée et à la sécurité

Section 6 : Glossaire

On trouvera ci-après les vingt et une (21) définitions de termes employés dans la présente politique.

Atteinte à la sécurité :

Un événement lié à l'information, à la sécurité ou à la protection de la vie privée qui compromet ou porte atteinte à la confidentialité, à l'intégrité ou à la disponibilité de l'information ou des systèmes d'information.

Contrôle de sécurité :

Une mesure de protection administrative, opérationnelle ou technique mise en œuvre pour protéger les actifs et les systèmes d'information et en maintenir la confidentialité, l'intégrité et la disponibilité. Les contrôles de sécurité peuvent être mis en œuvre au moyen de diverses solutions de sécurité, notamment des produits, politiques, pratiques et procédures de sécurité.

Cybermenace :

Une circonstance, un événement, un acteur ou une activité susceptibles d'exploiter une vulnérabilité et de nuire à la confidentialité, à l'intégrité ou à la disponibilité des actifs ou des systèmes d'information.

Cyberrisque :

L'exposition potentielle à une perte ou à un préjudice découlant des renseignements numériques ou des systèmes d'information d'EO. La possibilité d'un dommage ou d'un préjudice, et la probabilité que ce dommage ou ce préjudice se réalise.

Cybersécurité :

La protection des renseignements numériques, ainsi que de l'intégrité de l'infrastructure qui les héberge et les transmet. Plus précisément, la cybersécurité comprend l'ensemble des technologies, des processus, des pratiques ainsi que des mesures d'intervention et d'atténuation conçues pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés, afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

Fournisseur/fournisseur de services :

Entreprises ou personnes (tiers) qui fournissent des produits ou des services à EO et qui peuvent avoir accès aux renseignements, systèmes, réseaux, infrastructures ou renseignements personnels d'EO dans le cadre de la prestation de ces services.

Hameçonnage :

Une tentative par un tiers de solliciter des renseignements confidentiels auprès d'une personne, d'un groupe ou d'une société en imitant une marque précise, habituellement bien connue, ou en usurpant l'image, généralement à

des fins financières. Les hameçonneurs tentent d'inciter les utilisateurs et utilisatrices à divulguer des renseignements personnels, tels que des numéros de carte de crédit, des identifiants bancaires en ligne et d'autres renseignements de nature délicate, qu'ils peuvent ensuite utiliser pour commettre des actes frauduleux.

Incident de cybersécurité :

Toute tentative non autorisée, fructueuse ou non, d'accéder aux actifs informationnels, aux systèmes, aux postes de travail, aux réseaux, aux appareils ou à toute donnée appartenant à EO, de les modifier, de les détruire, de les supprimer ou de les rendre inaccessibles. Un incident de cybersécurité risque de compromettre la confidentialité, l'intégrité et la disponibilité des renseignements d'EO. Ces incidents peuvent comprendre les cyberattaques, les cybermenaces, les accès non autorisés, le déni de service, le code malveillant, ainsi que les atteintes soupçonnées ou réelles à la vie privée ou à la sécurité.

Incident de cybersécurité critique :

Un incident qui touche (a) la sécurité, la continuité, la confidentialité, l'intégrité ou la disponibilité des renseignements numériques d'EO (ou de l'infrastructure qui les héberge ou les transmet), et qui (b) répond à au moins l'un des critères suivants :

1. Entraîne des conséquences négatives importantes sur la prestation des services publics d'EO;
2. Pose un risque pour la sécurité publique;
3. Nécessite ou entraîne d'importantes mesures de récupération pour les renseignements numériques ou l'infrastructure connexe, ou l'activation des plans d'intervention en cas d'incident de cybersécurité;
4. Entraîne un risque important de préjudice à la réputation d'EO ou à la confiance du public.

Logiciel de rançon :

Un type de logiciel malveillant qui bloque l'accès d'un utilisateur ou d'une utilisatrice à un système ou à des données jusqu'à ce qu'une somme d'argent soit versée.

Logiciel malveillant :

Logiciel malveillant conçu pour infiltrer ou endommager un système informatique, à l'insu de son propriétaire. Les formes courantes de logiciels malveillants comprennent les virus informatiques, les vers, les chevaux de Troie, les logiciels de rançon, les logiciels espions et les logiciels publicitaires.

Mesure de sécurité :

Une mesure ou un contrôle de protection et de précaution visant à empêcher un agent de menace de causer des dommages ou des pertes.

Non autorisé :

Sans l'approbation, l'autorisation ou la permission du personnel désigné d'EO ou de son représentant ou de sa représentante.

Personnel d'EO :

Le personnel d'EO comprend tout le personnel (permanent et temporaire), les fonctionnaires des élections, les consultant·e·s et les utilisateurs et utilisatrices autorisé·e·s ayant accès au réseau et à l'infrastructure d'EO. De ce nombre, comptons les personnes retenues par EO pour gérer le processus électoral pendant les élections générales et partielles (par exemple, directeur·rice du scrutin, secrétaire du scrutin, personnel de terrain, personnel des bureaux de vote).

Renseignements de nature délicate :

Renseignements qui, s'ils étaient divulgués sans autorisation, causeraient un préjudice (préjudice personnel ou organisationnel, atteinte à la réputation, avantage économique injuste, etc.).

Renseignements personnels :

Renseignements identificatoires concernant des particuliers, comme le nom, l'adresse personnelle, le numéro de téléphone à domicile ou cellulaire, l'adresse courriel, la date de naissance, le numéro d'assurance sociale, les informations relatives au vote permettant d'identifier un individu, ainsi que les données financières. Ils comprennent également les renseignements sur le personnel ou les fournisseurs de services d'EO (p. ex., le niveau d'étude, la santé ou les antécédents professionnels), ainsi que tout numéro d'identification, symbole ou autre particularité associé à une personne. Les coordonnées d'affaires sont exclues. EO renvoie à la définition des renseignements personnels figurant au paragraphe 2(1) de la Loi sur l'accès à l'information et la protection de la vie privée de l'Ontario.

Ressources :

Tout ce qui a de la valeur pour la société et qui nécessite une protection. Cela comprend les actifs informationnels (par exemple, les données, les dossiers et les documents), les actifs numériques (par exemple, le contenu numérique, les bases de données, les ressources infonuagiques et les identifiants), ainsi que les actifs de TI (par exemple, le matériel, les logiciels, les applications, les réseaux et les systèmes d'information), de même que les services et l'infrastructure de soutien.

Systèmes d'information numériques :

L'environnement technologique utilisé pour recueillir, traiter, stocker, transmettre ou gérer les renseignements numériques, y compris, mais sans s'y limiter, les applications, les bases de données, le matériel, les réseaux, les systèmes d'exploitation, les serveurs, le stockage et l'infrastructure de soutien.

Tolérance au risque :

Le degré et le type de risque qu'EO accepte de tolérer dans la poursuite de ses objectifs. La tolérance au risque oriente la prise de décision et doit respecter les exigences législatives et réglementaires applicables.

Utilisateur et utilisatrice :

Tout le personnel d'EO, y compris les employé·e·s, les entrepreneur·e·s, les sous-traitant·e·s, le personnel des agences de placement, la direction du scrutin et les autres membres du personnel électoral (y compris le personnel de terrain et les membres du personnel électoral), les consultant·e·s et les fournisseurs de services, ainsi que les autres utilisateurs et utilisatrices autorisé·e·s à accéder aux systèmes d'information et aux applications d'EO.

Vulnérabilité :

Une faille ou une faiblesse dans un système d'information, dans les procédures de sécurité du système, dans les contrôles internes ou dans la mise en œuvre, qui pourrait être exploitée ou déclenchée par une menace.

Section 7 : Documents de référence supplémentaires

Le tableau suivant présente les politiques et procédures d'Élections Ontario, ainsi que les pratiques exemplaires du secteur, qui complètent la Politique sur la cybersécurité d'Élections Ontario.

Titre du document	Autrices et auteurs
1. Boîte à outils des objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels	Gouvernement du Canada
2. Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique	Gouvernement de l'Ontario
3. La politique générale sur la cybersécurité et la gestion des cyberrisques	Gouvernement de l'Ontario
4. Politique de protection de la vie privée d'Élections Ontario	Élections Ontario
5. Politique sur le contrôle de l'accès aux TI et la gestion de l'accès des utilisateurs	Élections Ontario
6. Politique d'utilisation acceptable des ordinateurs et des technologies	Élections Ontario

Titre du document	Autrices et auteurs
7. Procédure de stockage, de transfert et de destruction sécurisés des renseignements personnels	Élections Ontario
8. Plan d'intervention en cas d'incident de cybersécurité	Élections Ontario
9. Protocole de gestion des atteintes à la vie privée et à la sécurité	Élections Ontario
10. Plan de continuité des activités	Élections Ontario
11. Plan de gestion des situations d'urgence	Élections Ontario
12. Calendrier de conservation des dossiers	Élections Ontario

Section 8 : Approbation

Le tableau ci-après indique les dates d'autorisation, de modification et d'examen de la présente politique.

Politique sur la cybersécurité	
Autorisation	Greg Essensa Directeur général des élections Date : 27 juillet 2026
Date d'entrée en vigueur	27 juillet 2026
Date de la dernière modification	Juillet 2026
Date de la prochaine révision (une fois par cycle électoral)	Juillet 2028
Personne-ressource	ceo@elections.on.ca