Direction générale adjointe

DE LA CYBERSÉCURITÉ
ET DE L'INFONUAGIQUE (DGACI)

2023-07-14

CYBERSÉCURITÉ

Directive sur l'utilisation sécuritaire des plateformes de développement d'applications à faible code

MSSS-DIR007

Votre gouvernement

Ministère de la Santé et des Services sociaux
Québec

Table des matières

Préambule

L'utilisation de plateformes de développement d'applications à faible code est de plus en plus répandue au ministère de la Santé et des Services sociaux (MSSS) ainsi que dans le Réseau de la Santé et des Services sociaux (RSSS).

Ces plateformes permettent d'agréger des ensembles disparates de données reliées à une même réalité, généralement avec moins d'efforts de programmation. Elles favorisent la prise de décisions éclairées et contribuent ainsi à l'évolution de la qualité de prestation de services aux citoyens. Elles offrent de plus :

- la possibilité de recevoir, traiter, créer et échanger des données (incluant avec les systèmes existants);
- la création rapide de valeur;
- des solutions davantage personnalisées et accessibles.

Les plateformes sont des outils très puissants qui, en l'absence d'encadrement adéquat, risquent de causer des brèches de sécurité et ainsi porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information.

Dans ce contexte, la présente directive précise les obligations liées à cet encadrement, ainsi que les rôles et responsabilités qui y sont liés.

Objectifs

La présente directive a pour but :

- de préciser un encadrement en matière de sécurité de l'information qui est spécifique aux plateformes de développement d'applications à faible code (information collectée, manipulée, etc.);
- d'encadrer la gestion des résultats qui y sont générés en fonction de la sensibilité des données, et ce, tout au long de leur cycle de vie;
- de réduire le risque de divulgation massive de l'information sensible qui y est collectée, manipulée, etc.;
- de définir les rôles et responsabilités des principaux intervenants afin de favoriser l'exploitation et l'utilisation sécuritaire de ces plateformes.

Champs d'application et portée

Cette directive s'applique aux entités suivantes qui effectueront du développement de solution à l'aide de plateformes de développement d'applications à faible code :

- au ministère de la Santé et des Services sociaux (MSSS);
- aux organismes publics visés au paragraphe 5 de l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G 1.03).

Elle englobe toute information détenue par ces entités, indépendamment de son format ou du support sur lequel elle se trouve (papier, enregistrement sonore ou vidéo, données électroniques ou numériques, etc.), utilisée à des fins applicatives, analytiques, décisionnelles ou d'intelligence d'affaires.

Cadre légal et administratif

Cette directive fait partie du cadre de gouvernance du MSSS et du RSSS et s'y inscrit, sans s'y limiter, en conformité avec :

- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- la Loi sur le partage de données entre établissements de santé;
- la politique gouvernementale de cybersécurité;
- la Politique provinciale de la sécurité de l'information;
- le Cadre provincial de gestion de la sécurité de l'information;
- la Règle particulière sur la sécurité organisationnelle;
- la directive sur la cybersécurité;
- les règles d'utilisation des systèmes d'information.

Définitions

Pour l'application de la présente directive, les termes suivants signifient :

Terme	Description
Actif informationnel	Une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.
Document	Un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'image (Loi sur le cadre juridique des technologies de l'information, LRQ, chapitre C-1.1).
Entrepôt de données	Un ensemble de données déjà nettoyées, transformées et intégrées de façon cohérente dans les entrepôts de données afin que les utilisateurs finaux des plateformes de développement d'applications à faible de code puissent l'exploiter.
Environnement	Un environnement est une zone qui est créée pour cloisonner une ou plusieurs solutions. Des zones peuvent être créées pour isoler les différentes étapes de développement, telles que les tests et la production, ceci afin de s'assurer que les modifications apportées dans un environnement n'affectent pas les autres environnements.
Incidents de sécurité de l'information	Tout évènement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de service.
Détenteur de l'information	Employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité d'un actif informationnel et des ressources qui le sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

Terme	Description
Plateforme de développement d'applications à faible code	Plateforme qui permet le développement et le déploiement rapide de solutions nécessitant moins d'efforts de programmation. Un exemple de ce type de plateforme est la suite de produits « Microsoft Power Platform » qui permet notamment le développement de solutions à l'aide d'outils simples tels que des composants « glisser-déposer » ainsi que des connecteurs préconstruits et offre des applications telles que Power BI, Power Virtual Agents, Power Automate et Power Apps.
Solution	Une solution peut être composée d'une ou de plusieurs entités qui ont été développées ou acquises à l'aide d'une application à faible code. Ainsi, une solution peut être un flux d'automatisation jumelé à un tableau de bord analytique, ou tout simplement une application logicielle Power Apps.
Utilisateur	Toute personne de l'organisme de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme ou y a accès – utilisateur développeur ou utilisateur consommateur compris.
Utilisateur consommateur	Toute personne autorisée appartenant à l'organisation de quelque catégorie d'emploi ou de quelque statut ainsi que toute personne morale ou physique qui utilise un actif informationnel de l'organisation pour mener à bien toutes ou une partie de ses activités.
Utilisateur développeur	Toute personne autorisée ayant accès aux données sources de l'établissement, dans un contexte d'intelligence d'affaires, appelée à les manipuler, à développer les interfaces et à gérer les accès utilisateurs.

Principes directeurs

Les exigences de sécurité de l'information sont basées sur les principes suivants pour l'acquisition et l'utilisation des plateformes de développement d'applications à faible code, ainsi qu'à leurs environnements et leurs configurations :

- la protection des données assurée durant tout leur cycle de vie;
- le contrôle de l'accès aux données à tous les niveaux :
  - données sources;
  - données traitées dans les solutions;
  - données stockées dans les environnements;
- l'application du moindre privilège d'accès.

Exigences de sécurité de l'information

Les exigences suivantes s'appliquent sur les solutions et les environnements qui sont créés à l'intérieur des plateformes de développement d'applications à faible code :

I. **Réaliser les activités de sécurité préalables au déploiement de toute solution**

- mener un exercice de classification (catégorisation et préjudices) de l'information;
- réaliser une analyse de risques liés à la sécurité de l'information lorsque la catégorisation de cette information est à 3 ou à 4 pour au moins l'un des volets suivants : disponibilité, intégrité ou confidentialité;

- élaborer les schémas d'architectures et la documentation des flux de données, incluant la classification de celles-ci (données en intrant et en extrant.

II. Effectuer une saine gestion des accès

- appliquer le principe du moindre privilège et la séparation des tâches pour s'assurer que les utilisateurs n'auront accès qu'à l'information nécessaire à l'exercice de leurs tâches[1];
- réviser annuellement les droits d'accès attribués et particulièrement ceux à privilèges élevés;
- obtenir, lorsque requis[2] et avant l'attribution d'un accès à des données, un engagement formel de confidentialité de l'utilisateur à respecter les règles de protection de l'information, les moyens d'accès fournis et le devoir de signalement en cas de divulgation non autorisée, ou même de suspicion de divulgation d'information sensible ou stratégique;
- mettre en place et maintenir à jour une matrice répertoriant minimalement les noms, les tâches, les rôles/fonctions et les accès associés;
- instaurer les règles de gestion des identités et des accès des utilisateurs consommateurs des outils (création/suppression/modification des comptes utilisateurs).

III. Mettre en place une journalisation basée sur les conclusions de l'analyse de risques

- tenir à jour un registre de journalisation des accès, accessible sur demande;
- élaborer un processus de demandes de rapports impliquant des données classifiées comme sensibles et veiller au respect des exigences en matière de protection des renseignements personnels;
- intégrer les journaux de sécurité dans les outils de surveillance des équipes de sécurité de l'organisation;
- définir les règles de gestion du cycle de vie des journaux de sécurité;
- journaliser minimalement les accès, les évènements[3] et les transactions.

IV. Protéger les données sensibles

- s'assurer que des mécanismes de chiffrement soient mis en place lors de la manipulation des données sensibles en mouvement[4] ainsi que celles aux repos (TDE = chiffrement complet de la base de données);
- veiller à ce que tout échange transitant par des interfaces applicatives de programmation (IAP) soit chiffré et authentifié.

V. Protéger les bases de données

- séparer les entrepôts de données de la plateforme cible et cloisonner les données;
- procéder, lorsque requise, à l'anonymisation des informations stockées dans les entrepôts de données et utilisées par les plateformes;
- s'assurer, par des mécanismes de vérification, que les données utilisées hors production ne soient pas exploitables, par leur anonymisation par exemple.

[1] Applicable également à l'accessibilité ou non de certains connecteurs DLP (Data Loss Prevention).
[2] Ces engagements sont dans certains cas obligatoires, en lien avec la législation en vigueur. Les détenteurs des informations concernées sont au fait de ce besoin.
[3] Évènements : toute action impliquant un changement, une modification ou une suppression.
[4] Il s'agit des fichiers plats qui doivent être échangés sur un canal sécurisé.

Obligations des principaux intervenants

La présente section énonce les rôles et responsabilités des principaux intervenants devant participer à la mise en place, au développement et au déploiement de solutions bâties à l'aide d'applications à faible code, en complément aux responsabilités déjà incluses dans les documents de la section « *Cadre légal et administratif* ».

Chef délégué de la sécurité de l'information (CDSI)

Le CDSI s'assure de la cohérence des dispositions de la présente directive au regard des exigences gouvernementales et ministérielles.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est responsable de la sécurité de l'approche préconisée dans la gestion des données. À ce titre, il doit :

- s'assurer que les détenteurs d'actifs informationnels des données sources sont impliqués dans l'approche;
- s'assurer de la prise en charge des exigences de sécurité lors du développement ou d'acquisition de solutions réalisées à l'aide d'applications à faible code;
- s'assurer de la désignation d'un détenteur (propriétaire) pour chaque solution.

Détenteur de la solution (propriétaire)

Le détenteur de la solution est responsable de la sécurité de la solution qui lui est confiée ainsi que des données collectées et traitées par celles-ci. À ce titre, il doit :

- s'assurer que les niveaux de sécurité établis pour cette solution correspondent à ceux exigés par la sensibilité des données sources;
- veiller à la sécurité des informations stockées dans les entrepôts de données qui sont utilisés par la solution (anonymisation, chiffrement, gestion des accès, etc.);
- obtenir l'approbation préalable et explicite du détenteur des données sources;
- s'assurer que les utilisateurs développeurs d'une solution aient les droits d'accès légitimes sur ces données sources;
- s'assurer qu'un processus rigoureux de gestion des accès ainsi que des privilèges octroyés dans le cadre de cette démarche est implanté et suivi pour cette solution;
- s'assurer de l'élaboration de la documentation afférente à chaque solution afin d'en assurer la pérennité;
- former et sensibiliser les utilisateurs développeurs et les utilisateurs consommateurs à la sensibilité des données mises à leur disposition.

Responsable de la protection des renseignements personnels (RPRP)

Le RPRP veille au respect des exigences de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels lors de l'utilisation des données de son organisation. À ce titre, il doit :

- s'assurer que la nécessité des besoins d'accès aux renseignements a été confirmée par le gestionnaire;
- déterminer si les données auxquelles il est demandé d'avoir accès sont nécessaires aux fins de l'exploitation et de l'utilisation soumises;
- déterminer la sensibilité des données sources devant être utilisées par les plateformes;

- tenir un registre des renseignements personnels exploités par chaque solution sous sa juridiction;
- autoriser toute demande d'utilisation des données de son organisation en la matière;
- interdire toute utilisation de données sources :

  — pour laquelle il existe un risque élevé de non-respect de la vie privée, lequel s'avérerait dommageable et porterait préjudice;

  ou

  — qui ne répond plus aux besoins exprimés initialement ou ne serait plus conforme à ceux-ci.

Gestionnaire

Le gestionnaire est responsable du respect de l'exploitation et l'utilisation sécuritaire des plateformes de développement à faible code par le personnel qui lui est hiérarchiquement rattaché. À ce titre, il doit :

- analyser et documenter la nécessité, pour son personnel, d'utiliser des données sources;
- informer l'utilisateur développeur de tout changement affectant les privilèges d'accès de son personnel, notamment lorsqu'ils ne sont plus requis;
- prendre connaissance des exigences de la présente directive, les communiquer à son personnel et veiller à ce qu'il les respecte.

Utilisateur développeur

Tout utilisateur développeur ayant accès à des données sources d'une organisation dans un contexte de développement d'applications à faible code a l'obligation de veiller à leur protection et à les utiliser conformément aux modalités prévues. À ce titre, il doit :

- obtenir l'approbation préalable du détenteur des données exploitées avant la sauvegarde, le transfert ou l'utilisation des données sources qui lui sont confiées;
- s'assurer que toute action posée (ajout, retrait, modification) n'affecte pas la sécurité des données sources, et que la sécurité est révisée systématiquement;
- respecter et mettre en œuvre les exigences de sécurité de la présente directive;
- adopter une démarche sécuritaire lors de la manipulation des données sources (accès, transmission, transformation, etc.), notamment dans la création ou l'exécution des requêtes;
- produire, à l'intention du détenteur et des gestionnaires, les rapports périodiques des autorisations d'accès attribuées;
- effectuer une révision périodique des accès aux solutions et aux environnements;
- établir les modalités de fonctionnement sécuritaire relatives à la manipulation, l'extraction, la consultation, l'entreposage et l'entretien (environnement de test) des entrepôts de données.

Utilisateur consommateur

Tout utilisateur consommateur d'information provenant d'une plateforme de développement d'applications à faible code doit se conformer aux exigences de sécurité de l'information de son organisation. Il doit notamment :

- informer rapidement l'utilisateur développeur et son gestionnaire de tout changement quant à ses besoins en matière de privilèges d'accès, notamment dès qu'ils ne sont plus requis;
- aviser immédiatement le détenteur ou son gestionnaire de tout acte dont il a connaissance et qui est susceptible de constituer une violation réelle ou présumée des règles gouvernementales ou ministérielles en matière de sécurité de l'information.

Sanctions

Tout utilisateur qui contrevient à la présente directive s'expose à des mesures disciplinaires, administratives ou légales. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre.

Entrée en vigueur et révision

Cette directive entre en vigueur à la date de son approbation. Elle doit être révisée :

- tous les trois ans;

  ou

- lors de changements organisationnels ou de l'adoption de nouvelles orientations ministérielles en la matière.

Approuvée par le chef délégué de la sécurité de l'information (CDSI) :	*Boris Gueissaz-Teufel pour* Reno Bernier
Date d'approbation :	2023-07-14