Centre de services scolaire des Grandes-Seigneuries
Québec

PROCÉDURE

Relative à la gouvernance des données

 # 40-02

Adoption : 1er septembre 2026
Mise en vigueur le : 2 septembre 2026
Autorisation : BDG-20260901-919

Autorisation :

Christian Duval
Directeur général

1. Contexte et objectif

Au Centre de services scolaire des Grandes-Seigneuries (ci-après le « CSSDGS »), les données constituent un levier essentiel pour appuyer les décisions pédagogiques et de gestion, contribuer à l'atteinte de la mission éducative et soutenir les opérations administratives. Dans cette perspective, la gouvernance des données établit un cadre structuré composé de règles, de processus, de rôles, de politiques, de normes et de mécanismes de contrôle. Ce cadre vise à assurer une gestion, une protection, une utilisation et une valorisation responsables des données, dans le respect des exigences en matière de sécurité, de confidentialité et de sûreté, et ce, tout au long de leur cycle de vie.

La présente procédure constitue une première étape dans la mise en œuvre de ce cadre. Par celle-ci, le CSSDGS s'engage à instaurer une gouvernance des données rigoureuse, cohérente et conforme aux exigences légales.

2. Encadrement

La présente procédure découle de la *Politique relative à la sécurité de l'information, à l'utilisation des ressources informationnelles et à la protection des renseignements personnels* (#90-04) du CSSDGS.

Cette procédure permettra de soutenir le CSSDGS dans l'application des encadrements légaux auxquels il est assujetti, notamment :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics*, (RLRQ, chapitre G-1.03)*;*
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (RLRQ, c. A-2.1);
- *Loi sur les archives*, (RLRQ, c. A-21.1);
- *Loi sur le droit d'auteur* (L.R.C., 1985, c. C-42);
- *Loi concernant le cadre juridique des technologies de l'information*, (RLRQ, c. C-1.1)*.*

En cas de conflit entre les définitions ou modalités de la présente procédure et celles de tout encadrement légal ou réglementaire applicable, ces derniers prévalent.

3. Définitions

Architecture d'entreprise

L'architecture d'entreprise représente la conception de la structure et du fonctionnement des unités administratives d'une organisation donnée en vue de favoriser la qualité de l'information, la sécurité des échanges, ainsi que l'interopérabilité et la réutilisation.

Architecture technologique
L'architecture technologique est l'ensemble des principes, modèles, structures, standards et mécanismes définissant l'organisation des composantes technologiques, applicatives, infrastructurelles et informationnelles d'un système afin d'assurer la cohérence, la performance, la sécurité, l'évolutivité, l'interopérabilité et l'alignement avec les objectifs d'affaires.

Certification de la donnée
La certification de la donnée consiste à approuver officiellement une donnée comme étant fiable, conforme et prête à être utilisée au sein de l'organisation.

Confidentialité des données
La confidentialité des données correspond aux processus et aux éléments mis en place afin de protéger les données par rapport aux personnes internes et externes à l'organisation afin d'empêcher la consultation non autorisée.

Cycle de vie d'une donnée
Le cycle de vie d'une donnée correspond au chemin que parcourt une donnée, de sa création ou de sa collecte, jusqu'à sa destruction.

Domaine de données
Un domaine de données est un secteur fonctionnel ou un champ d'activité d'une organisation qui regroupe un ensemble cohérent de processus, de règles métier, d'acteurs, de responsabilités et d'informations liés à une même mission organisationnelle. Il sert à structurer les activités de l'organisation et il est immuable, même en cas de réorganisation ou de restructuration au sein de l'organisation.

Donnée
Une donnée est la plus petite unité d'information brute décrivant un fait, un objet, un événement ou un concept, sans contexte ni interprétation, quel que soit le support.

Intelligence numérique (IN)
Ensemble d'outils et de méthodologies combinant la création, la collecte et l'exploitation des données faisant appel à la conception et l'utilisation de modèles et d'algorithmes pour faciliter, enrichir et accompagner la prise de décisions. Au CSSDGS, l'intelligence numérique comprend la valorisation des données, les solutions numériques et l'intelligence artificielle.

Métadonnée
Une métadonnée est une donnée utilisée pour décrire une autre donnée et qui permet de savoir ce qu'elle est, comment elle est organisée et comment l'utiliser.

Métier
Un champ d'activité et de connaissances propre à une fonction ou une mission au sein d'une organisation.

Portabilité de l'architecture
La portabilité de l'architecture est la capacité d'une solution à être déployée, exploitée ou migrée vers un autre environnement technologique avec un minimum d'effort, de modification et de dépendances envers un fournisseur infonuagique, une technologie particulière ou un logiciel spécifique.

Sécurité des données
La sécurité des données correspond aux mesures, mécanismes, politiques et contrôles mis en place afin de protéger les données contre les actions provenant de l'intérieur et l'extérieur de l'organisation.

Sujet de données
Un sujet de données est une subdivision plus précise et ciblée d'un domaine de données, représentant un thème, une activité, un processus ou un ensemble d'informations spécifiques liés à ce domaine. Il permet de découper un domaine en composantes plus faciles à gouverner, analyser et exploiter.

Sûreté des données
La sûreté vient compléter la confidentialité et la sécurité, en s'assurant de la qualité, de la pertinence et de la cohésion des données lors de leur création, de leur collecte et de leur utilisation.

4. Champ d'application
La présente procédure s'applique à l'ensemble des données détenues par le CSSDGS, et ce, tout au long de leur cycle de vie.

La présente procédure s'applique à toutes les unités administratives, aux employés du CSSDGS, ainsi qu'à toutes autres parties prenantes ayant accès aux données du CSSDGS.

5. Principes directeurs
Les principes directeurs énumérés ci-dessous constituent les fondements de la gouvernance des données du CSSDGS et permettent d'assurer la cohérence, l'alignement stratégique et la prise de décision uniforme. Ces principes directeurs guident l'élaboration des différents niveaux d'architecture qui, eux-mêmes, permettront d'élaborer l'infrastructure adéquate.

5.1 Gouvernance des données

- Centralisation des traitements d'information (création, modification ou correction) dans les systèmes applicatifs opérationnels;
- Traçabilité et portabilité des processus de traitement des données;
- Alignement sans ambiguïté des processus sur le métier et la mission de l'organisation; Priorité aux processus d'entrée des données pour les données nécessitant un niveau élevé de qualité;
- Cohérence du choix des solutions avec l'architecture d'entreprise.

5.2 Architecture technologique

- Unicité et harmonisation de stockage;
- Captation du changement au niveau de la donnée;
- Protection contre la divulgation de renseignements personnels par un chiffrement obligatoire indépendant du fournisseur;
- Communication des systèmes uniquement vers le stockage unique;
- Application cohérente d'une sécurité et confidentialité par rôle;
- Gestion unique et simplifiée de chaque fonctionnalité;
- Architecture permettant la gouvernance et la protection des données
- Arbitrage de l'architecture entre l'élasticité et la portabilité;
- Prépondérance du principe de mutualisation dans le secteur;
- Application des bonnes pratiques et méthodes des métiers de la donnée.

6. Processus de gouvernance des données

Le processus de gouvernance des données est l'ensemble structuré des activités, règles, décisions, rôles et mécanismes permettant de gérer les données comme un actif stratégique de l'organisation afin d'assurer leur qualité, leur sécurité, leur conformité, leur disponibilité et leur utilisation cohérente.

La gouvernance des données repose sur trois processus principaux : la mise en place, le cycle de vie de la donnée et la gestion des métadonnées. Une représentation visuelle des trois processus est présentée en annexe 1.

Le processus de mise en place consiste à établir les éléments nécessaires pour poser les bases communes avant le lancement d'un projet IN.

Le processus de cycle de vie de la donnée correspond à l'application de la gouvernance des données en fonction de la vie de la donnée, à l'intérieur des projets IN, et comprend notamment le processus de certification des données.

Le processus de gestion des métadonnées est un processus qui relie le processus de mise en place et le processus de cycle de vie de la donnée.

7. Rôles et responsabilités

Cette section présente les rôles et les responsabilités en lien avec la gouvernance des données. Pour de plus amples détails sur la structure de gouvernance des données au CSSDGS, se référer au schéma présenté à l'annexe 2.

7.1 Rôles

7.1.1 Direction générale (DG)

La DG est responsable des mandats suivants :

- Encadre la stratégie de gestion des données pour valoriser les données de l'organisation et les utiliser de manière efficace pour atteindre les objectifs organisationnels;
- Définit la vision organisationnelle des données et pilote la gouvernance des données;
- Priorise les initiatives en intelligence numérique;
- Supervise la sécurité, la conformité et la sûreté.

Pour ce faire, la DG doit identifier un **Responsable de la gouvernance des données (RGD).**

7.1.2 Le Service de la performance organisationnelle et de l'approvisionnement (SPOA)

Le SPOA est responsable des mandats suivants :

- Met en œuvre, coordonne et alimente la prise de décision;
- Assure la cadence d'exécution de la gouvernance des données;
- Assume les responsabilités confiées par le RGD.

Pour ce faire, le SPOA doit identifier un **Responsable de la gouvernance des données adjoint (RGD adjoint)**.

De plus, les mandats suivants relèvent également du SPOA

- Développe et met en œuvre la stratégie de mise en place de la gouvernance et de la valorisation des données;
- Identifie les opportunités de création de valeur et supervise le développement d'outils décisionnels et d'analyses avancées;
- Assure la liaison entre les unités administratives et les équipes techniques favorisant une culture permettant d'appuyer les décisions pédagogiques et de gestion sur des données.
- Représente l'organisation auprès de certaines instances externes, en veillant à la cohérence et au respect d'un standard;
- Effectue une veille continue pour positionner l'organisation comme acteur mature et innovant en matière de gouvernance des données.

Pour ce faire, le SPOA doit identifier un **Responsable de la valorisation des données**.

7.1.3 Le Service des technologies d'information (STI)

Le STI est responsable des mandats suivants :

- Analyse le côté technique dans les bases de données;
- Participe à la mise en place d'une bonne stratégie de gouvernance des données dans son organisation afin d'en garantir la qualité et la sécurité.

Pour ce faire, le STI doit identifier des **Intendants de données (volet technique)**.

Les mandats suivants relèvent également du STI :

- Est responsable de la stratégie et de la gouvernance en matière de sécurité;
- Assure la protection des systèmes et des données;
- Assure la gestion des risques et des incidents de sécurité;
- Assure la conformité aux encadrements administratifs du ministère de la cybersécurité et du numérique (MCN);
- Est responsable de la sensibilisation et de la culture de sécurité.

Pour ce faire, le **Chef de la sécurité de l'information organisationnelle (CSIO)** assume ces mandats.

Les mandats suivants relèvent également du STI :

- Est responsable de traduire le métier en technique tout en optimisant les ressources et les besoins;
- Établit les règles et les principes de l'architecture technologique de l'organisation.

Pour ce faire, le STI doit identifier un **conseiller en architecture d'entreprise**.

Les mandats suivants relèvent également du STI :

- Est responsable de la qualité et de l'analyse de la donnée;
- Appuie les intendants de données;
- Est responsable de la modélisation conceptuelle et logique;
- Définit les modèles;
- Définit les stratégies d'intégration des données;
- Définit les standards de stockage;
- Définit le processus de certification et les métadonnées;
- Définit la situation future des données, l'alignement au cours du développement et le suivi nécessaire pour s'assurer que la conception est faite selon les spécifications architecturales d'origine.

Pour ce faire, le STI doit identifier un **Conseiller en architecture de données**.

7.1.4 Le Service du secrétariat général et des communication (SGC)

Le SGC est responsable des mandats suivants :

- Est responsable du respect des encadrements légaux relatifs à la protection des renseignements personnels et des données organisationnelles;
- Assure un rôle-conseil relativement à la protection des renseignements personnels et des données organisationnelles ;
- Est responsable de la réalisation des évaluations des facteurs relatifs à la vie privée (EFVP) en conformité avec la Procédure relative aux EFVP;
- Gère les incidents de confidentialité;
- Interagit avec les autorités gouvernementales et organismes d'application (MCN, Commission d'accès à l'information);
- Est responsable de l'application du calendrier de conservation et du plan de classification;
- Est responsable de l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Pour ce faire, le **responsable de la protection des renseignements personnels** (RPRP) assume ces mandats.

Les mandats suivants relèvent également du SGC :

- Supporte le Responsable de la protection des données afin d'assurer le respect des encadrements légaux relatifs à la protection des renseignements personnels et des données organisationnelles;
- Révise les conditions d'utilisation, les consentements et les documents relatifs à la confidentialité afin d'assurer leur conformité aux encadrements légaux relatifs à la protection des renseignements personnels et des données organisationnelles;
- Assure un rôle-conseil, en collaboration avec le STI, quant à la classification et au marquage des données, en conformité avec les orientations gouvernementales.

Pour ce faire, le SGC doit identifier un **Agent à la protection des renseignements personnels et des données organisationnelles**.

7.1.5 Les Directions de services sont responsables des mandats suivants :

- Assure la qualité, de la cohérence, de la définition et du bon usage des données dans l'organisation ;
- Établit les règles d'affaires, de conformité et de catégorisation des données pour les domaines qui lui sont attribués ;
- Gère les données du domaine attribué et définit leur cycle de vie ;

- Assure l'application de la présente procédure, ainsi que des directives et des normes applicables au domaine de données attribué ;
- Communique les nouveautés, les changements et les préoccupations liés à la qualité des données et contribue à la résolution des problèmes concernant un domaine de données entre les unités administratives ;
- Désigne les intendants de données ;
- Apporte une connaissance et une vision stratégique intersectorielle concernant l'utilisation et l'accessibilité des données ;
- Suit et gère la qualité des données du domaine attribué et fournit des mises à jour relatives à la gouvernance des données.

Pour ce faire, le Comité de direction en intelligence numérique (CODIR IN) en collaboration avec les directions de services devront identifier **des gardiens de données.**

De plus, les mandats suivants relèvent également des Directions de services

- Analyse le côté métier des données (sens et processus);
- Participe à la mise en place d'une bonne stratégie de gouvernance des données dans son organisation afin d'en garantir la qualité et la sécurité;
- S'assure du respect des règles et des définitions pour les données relatives à son domaine d'expertise.

Pour ce faire, les gardiens de données en collaboration avec les directions de services devront identifiées des **intendants de données** (volet métier) ayant une connaissance approfondie du métier.

7.1.6 L'ensemble des unités administratives sont responsables des mandats suivants :

- Utilise les outils appropriés pour saisir les données, dans le respect des règles du CSSDGS, afin de maintenir leur exactitude et leur fiabilité ;
- Assure la collecte, la saisie et la mise à jour des données avec précision et rigueur.

Pour ce faire, des **créateurs de données** collectent, saisissent et mettent à jour des données, de façon ponctuelle ou continue.

De plus, les mandats suivants relèvent également des unités administratives :

- Informe les intendants de données ou les gardiens de données des enjeux rencontrés relativement à l'accès, au contenu, à la qualité ou à la sécurité des données, dans une perspective d'amélioration continue;
- Déclare sans délai tout incident de sécurité ou de confidentialité impliquant des renseignements personnels, conformément aux directives en vigueur.

Pour ce faire, l'ensemble des unités administrative disposent **d'utilisateurs de données** qui consultent, manipulent ou exploitent les données pour accomplir leurs tâches et orienter leurs décisions.

7.2 Instances de gouvernance

a) Comité de direction en intelligence numérique (CODIR IN)

- Constitue le comité de gouvernance des données;
- Génère une prise de conscience et développe la culture et la stratégie de la donnée au sein de l'organisation;
- Promeut et encourage une culture de l'excellence et de la qualité des données;
- Statue sur les conflits de données non résolus;
- Définit et approuve les stratégies et les orientations en gouvernance des données;
- Accepte les risques identifiés;
- Accepte et propose aux instances appropriées les encadrements (politiques, procédures, modalités administratives, etc.) en vue de leur adoption;
- Communique les informations de niveau stratégique de la gouvernance des données interne et externe.

Ce comité est formé des personnes exerçant les rôles suivants :

- Responsable de la gouvernance des données;
- Responsable de la gouvernance des données adjoint;
- Responsable de la sécurité de l'information;
- Responsable de la protection des renseignements personnels
- Autres invités lorsque requis en fonction des sujets de décision.

b) Comité de pilotage en intelligence numérique (COPIL IN)

- Rédige et propose les encadrements requis relativement à la gouvernance des données;
- Détermine et surveille l'état d'avancement des travaux en gouvernance des données;
- Promeut et soutient les initiatives en matière de données auprès des domaines d'affaires;
- Forme ou délègue des groupes de travail pour des initiatives en matière de données;
- Collabore et est consulté sur les besoins de projets en intelligence numérique qui y sont présentés en amont du comité aviseur;
- Assure le partage des informations de niveau tactique de la gouvernance des données interne et externe;
- Formule des recommandations de priorisation des initiatives au comité aviseur.

Ce comité est formé des personnes exerçant les rôles suivants :

- Représentant de la sécurité et de la conformité;
- Représentant des solutions numériques;
- Agent de protection des renseignements personnels et des données organisationnelles;
- Responsable de la valorisation des données;
- Équipe d'accompagnement;
- Autres invités si requis.

c) Opérations

- Responsable de la qualité, de la cohérence, de la définition et du bon usage des données dans une organisation;
- Analyse le côté affaire et le côté technique des données;
- Collecte, saisit et met à jour les données;
- Signale rapidement tout problème lié à l'accès, au contenu, à la qualité, à la sécurité ou à la confidentialité des données.

Les activités des opérations sont réalisées par les rôles suivants :

- Gardiens de données;
- Intendants de données métier;
- Intendants de données techniques;
- Créateurs de données;
- Utilisateurs de données.

d) Comité sur la protection des renseignements personnels et des données organisationnelles

- Développe et tient à jour la liste des éléments à considérer afin de permettre aux promoteurs de projets d'intégrer une évaluation préliminaire de la conformité dans leurs fiches d'opportunités;
- Coordonne, encadre et supervise les travaux du sous-comité relatif aux EFVP;
- Émet des recommandations en matière d'application de la législation;
- Assure la veille des enjeux légaux et réglementaires en matière de gouvernance des données.

Ce comité est formé des personnes exerçant les rôles suivants :

- Responsable de la protection des renseignements personnels;
- Chef de la sécurité de l'information organisationnelle;
- Coordonnateur organisationnel des mesures de sécurité de l'information;
- Responsable de la gestion documentaire;
- Coordonnateur du Service du secrétariat général et des communications;
- Direction d'une école primaire ou secondaire.

7.3 Équipes

a) Équipe d'accompagnement

- Appuie la compréhension et la mise en œuvre de la gouvernance des données au sein de l'organisation ;
- Soutient le Responsable de la gouvernance des données dans la réalisation de ses mandats ;
- Accompagne et favorise l'arrimage, de façon continue, des parties prenantes impliquées dans la gouvernance des données ;
- Soutient la coordination des travaux du CODIR IN et du COPIL IN ;
- Coordonne les activités liées à l'inventaire, au processus de certification des données et aux premiers cas d'usage ;
- Suit et évalue l'avancement de la mise en œuvre de la gouvernance des données ;
- Soutient la réalisation du plan de formation, du plan de communication et du plan de gestion du changement.

Cette équipe est formée des personnes exerçant les rôles suivants :

- Responsable de la valorisation des données;
- Conseillers en intelligence d'affaires;
- Conseiller en architecture de données, selon le besoin.

b) Équipe en intelligence numérique volet valorisation des données

- Coordonne, gère les projets et assure la création de valeurs ;
- Fait le lien avec les utilisateurs de données ;
- Comprend les besoins des promoteurs et des utilisateurs finaux ;
- Interprète les données disponibles ;
- Coordonne la documentation requise;
- Identifie les sources, extrait, transforme et charge les données requises;
- Évalue la qualité des données ;
- Accompagne les utilisateurs dans la définition des règles d'affaires ;
- Crée et développe les solutions selon les maquettes.

Cette équipe est formée des personnes exerçant les rôles suivants :

- Conseillers en intelligence d'affaires;
- Analyste informatique;
- Conseiller en architecture de données.

c) Équipes de travail selon les expertises

- Analysent des orientations et des solutions en lien avec les sujets de la sécurité, la confidentialité, la sûreté et la gestion des métadonnées;
- Sont responsables de la revue d'architecture TI;

- Recommandent des orientations ou des solutions au COPIL-IN et CODIR-IN;
- Sont responsables de la conformité TI (données et sécurité);
- S'assurent que les décisions prises sont communiquées et en assurent l'intégration dans la livraison de projets et sur le plan opérationnel.

Ces équipes regroupent des sous-équipes de travail relevant du STI.

d) Sous-comité sur l'évaluation des facteurs relatifs à la vie privée (EFVP)
   - Analyse, approuve sous réserve ou refuse les EFVP de sa compétence en application de la Procédure relative aux EFVP;
   - Réfère au Comité sur la protection des renseignements personnels les EFVP pertinentes en application de la Procédure relative aux EFVP;
   - Émet toute recommandation ou suggère toute mesure jugée pertinente afin de protéger adéquatement les renseignements personnels et les données organisationnelles dans le cadre d'une EFVP.

   Ce comité est formé des personnes exerçant les rôles suivants :
   - Agent à la protection des renseignements personnels et des données organisationnelles;
   - Direction adjointe conformité au STI;
   - Autres invités lorsque requis en fonction des sujets de décision.

8. Mécanisme de révision

La modification de la procédure se fait par la direction du Service de la performance organisationnelle et de l'approvisionnement et doit être autorisée par la direction générale au plus tard tous les cinq (5) ans.

9. Dispositions finales

La direction du Service de la performance organisationnelle et de l'approvisionnement émet la présente procédure. Toute personne exerçant un des rôles y étant identifiés est responsable de son application.

La présente procédure entre en vigueur le 18 septembre 2026.

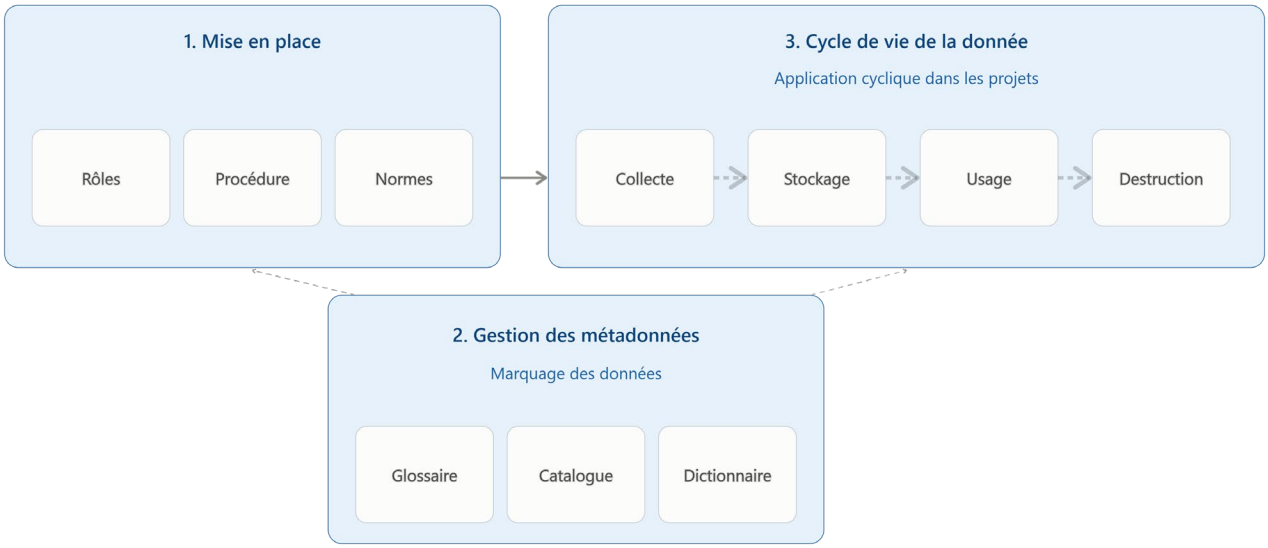
10. Référence

La présente procédure s'inspire des références suivantes :

- Divers ouvrages fournis par la firme externe Orym inc.
- Centre de services scolaire de Montréal, *Politique relative à la gouvernance des données*.
- DAMA International, *Data Management Body of Knowledge* (DAMA-DMBOK).

ANNEXE 1

Processus de gouvernance des données



ANNEXE 2

Structure de gouvernance des données au CSSDGS