RÈGLE DE RÉGIE CONCERNANT LA GESTION DES ACCÈS LOGIQUES ET DES AUTHENTIFICATIONS

C. Parents
2017-11-08
5.2

1.0 PRÉAMBULE

En assurant un contrôle efficace des accès à l'information, la Commission scolaire de la Beauce-Etchemin réduit les risques encourus à l'égard des objectifs d'intégrité, de disponibilité et de confidentialité de son information et répond à l'obligation gouvernementale énoncée au paragraphe (c) du premier alinéa de l'article 7 de la Règle sur la sécurité de l'information gouvernementale.

Celle-ci fait obligation aux organismes publics de s'assurer de la mise en œuvre de processus formels de sécurité de l'information, dont la gestion des accès à l'information.

2.0 OBJET

La présente règle définit les lignes directrices en matière de gestion des accès et les responsabilités à assumer par les principaux intervenants, notamment le dirigeant de l'organisme, le responsable organisationnel de la sécurité de l'information, les détenteurs de l'information, les gestionnaires des unités administratives, le responsable des technologies de l'information, l'administrateur des accès et les utilisateurs.

Elle précise également les sanctions prévues pour tout utilisateur qui contrevient aux dispositions énoncées.

3.0 CADRE LÉGAL ET ADMINISTRATIF

- Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1).
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).
- Loi sur les archives (chapitre A-21.1).
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).
- Loi constitutive de l'organisme qui adopte la présente règle.
- Lois et règlements sectoriels régissant la mission de chaque organisme relativement à la gestion des accès.

- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.
- Règle sur la sécurité de l'information gouvernementale, en vigueur depuis le 15 janvier 2014.
- Cadre gouvernemental de gestion de la sécurité de l'information, en vigueur depuis le 15 janvier 2014.
- Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information.

4.0 CHAMP D'APPLICATION

Cette règle s'applique à :

- L'information que détient la Commission scolaire de la Beauce-Etchemin dans l'exercice de ses fonctions, que sa conservation soit assurée par elle-même ou par un tiers.
- L'information confiée à la Commission scolaire de la Beauce-Etchemin en vertu d'une entente et qui est reconnue comme devant faire l'objet d'un contrôle d'accès.
- L'infrastructure technologique de la Commission scolaire de la Beauce-Etchemin.
- Toute personne physique ou morale qui, à titre d'employé, de consultant, de stagiaire, de partenaire ou de fournisseur, a un accès, sur place ou à distance, à l'information dont la sécurité est assurée par la Commission scolaire de la Beauce-Etchemin.

5.0 ACRONYMES ET DÉFINITIONS

5.1 Acronymes :

- **COGI :** coordonnateur organisationnel de gestion des incidents.
- **COSI :** conseiller organisationnel en sécurité de l'information.
- **ROSI :** responsable organisationnel de la sécurité de l'information.
- **SRIO :** le service des ressources informationnelles et organisationnelles

5.2 Définitions :

Authentifiant

Information confidentielle détenue par une personne et permettant son authentification. Elle peut être sous la forme d'un mot de passe, d'un numéro d'identification personnel (NIP) ou autre, selon la technologie utilisée.

Authentification

Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel. L'authentification permet de valider l'authenticité de l'entité qui demande l'accès. S'authentifier, c'est apporter la preuve de son identité.

Comptes à privilèges spéciaux

Comptes qui comprennent les comptes d'administrateur, les comptes intégrés et les comptes utilisés pour exécuter des programmes de service. Ils sont des comptes hautement sensibles qu'il faut entourer de mesures de sécurité supplémentaires et contrôler périodiquement.

Comptes intégrés

Comptes utilisés par un système pour se connecter à un autre système.

Compte générique

Compte anonyme n'appartenant pas à une personne en particulier. Il peut être utilisé par plusieurs utilisateurs.

Contrôle d'accès

- Procédure qui consiste à vérifier si un sujet (personne ou dispositif) demandant d'accéder à un objet (fichier, base de données ou dispositif) dispose des permissions nécessaires pour le faire.

- Contrôles qui permettent d'autoriser ou d'interdire l'accès utilisateur aux ressources à l'intérieur du système d'information.

- Processus par lequel les données d'authentification fournies par une personne, ou toute autre entité, pour avoir accès à un centre ou à un système informatique, sont comparées avec des valeurs de référence définies touchant cette entité, permettant ainsi l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique.

Critères d'habilitation

Exigences à respecter par une entité pour avoir l'autorisation d'accès à une information sensible.

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 de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

Documents structurants

La Règle sur la sécurité de l'information gouvernementale, le Cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents d'une portée gouvernementale et l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information.

Droit d'accès logique

Désigne l'effet recherché lorsqu'un sujet accède à un objet, c'est-à-dire lire écrire, modifier, supprimer, imprimer, créer, copier, transmettre et approuver.

Habilitation

Ensemble des droits d'accès autorisés à une entité par une autorité de l'organisme, généralement la hiérarchie immédiate. L'habilitation est associée à une fonction organisationnelle et elle est constituée de l'ensemble des profils d'accès nécessaires à l'accomplissement des tâches associées à la fonction considérée. Ainsi, toutes les personnes qui occupent la même fonction organisationnelle bénéficient, théoriquement, d'une même habilitation.

L'habilitation est appelée également « profil » dans certains organismes. Il est important de ne pas la confondre avec l'habilitation sécuritaire qui est un filtrage de sécurité.

Identification

- Permets à une entité (personne ou ordinateur) de se faire reconnaître du système par un élément dont on l'a doté préalablement. Cet élément est appelé généralement « identifiant ». S'identifier, c'est communiquer une identité préalablement enregistrée.
- L'identification permet de connaître l'identité d'une entité alors que l'authentification permet de vérifier cette identité.

- Opération qui consiste, pour une personne ou pour toute autre entité demandant l'accès au système informatique, à communiquer à ce dernier l'identité dont elle se réclame.

Matrice de profils d'accès applicatifs

Grille associée à un système de mission (application) et contenant les profils d'accès applicatifs supportés par ce système ainsi que les exigences de sécurité correspondantes.

Matrice de profils d'accès général

Grille associée à une entité administrative et contenant les profils d'accès général défini pour ses utilisateurs ou groupes d'utilisateurs.

Politique d'accès fermée

Politique d'accès qui considère qu'un accès est refusé à moins qu'il ne soit explicitement permis.

Principe de privilège minimal

Principe qui exige que l'utilisateur ne dispose pas plus de droits que nécessaire pour accomplir ses tâches. Cela implique que les permissions affectées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches associées à ce rôle.

Principe de séparation des tâches

Principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible ou essentielle sont réparties entre plusieurs entités (personnes, processus, etc.), afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité. Il vise à limiter les possibilités d'abus et d'infraction par une seule personne.

Profil d'accès applicatif

Profil qui regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction sur un système de mission ou une application (par exemple : pilote d'application, enquêteur, analyste). Un utilisateur peut avoir un ou plusieurs profils.

Profil d'accès général

Profil qui décrit les accès standard, nécessaires à un utilisateur ou un groupe d'utilisateurs, aux ressources autres que les systèmes de mission. Il concerne les accès aux messageries, boîtes aux lettres de partage, listes de distribution, répertoires de données, serveurs, intranet, extranet, etc.

Programmes de services

Programmes faisant généralement partie de la bibliothèque de programmes et destinés à augmenter les possibilités de base du système d'exploitation en permettant l'exécution d'opérations courantes telles que la conversion de supports de fichiers, le tri, la fusion et le diagnostic.

Registre des accès accordés

Répertoire dans lequel sont consignées toutes les permissions d'accès accordées à un compte.

Registre d'autorité

Répertoire, recueil ou fichier dans lesquels sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information. Dans ce registre sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leurs sont assignés ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information. [Guide d'élaboration d'un registre d'autorité de sécurité de l'information, 2015]

Registre de catégorisation

Répertoire dans lequel sont consignés les niveaux d'impacts, en matière de disponibilité, d'intégrité et de confidentialité des actifs informationnels. [Guide de catégorisation de l'information, 2014]

Règle de contrôle d'accès

Règle qui définit les paramètres permettant d'évaluer l'autorisation d'accès à un objet. L'application des règles de contrôle d'accès permet d'assurer que les sujets possèdent uniquement les droits d'accès qui leur sont octroyés sur les objets.

Référentiel des profils d'accès à l'information

Répertoire dans lequel sont consignées les matrices de profils d'accès applicatifs de chaque système de mission de l'organisme et les matrices de profils d'accès généraux.

Référentiel des habilitations

Répertoire dans lequel sont consignés, pour chaque fonction organisationnelle, les profils d'accès applicatifs et les profils d'accès général nécessaires pour accomplir les tâches associées à la fonction ainsi que les critères d'habilitation requis.

Rôle

Un rôle définit les autorisations nécessaires à l'utilisation des objets (applications ou ressources). Un rôle applicatif est un ensemble de droits d'accès propres à une seule tâche dans une application.

Traçabilité

La traçabilité garantit que les accès et tentatives d'accès aux éléments considérés sont enregistrés et que ces renseignements sont normalement conservés et exploitables.

Télétravail

Activité professionnelle qui s'exerce en dehors des bureaux de l'employeur et pour laquelle on fait appel aux technologies de l'information et de la communication pour communiquer à distance.

6.0 LIGNES DIRECTRICES DE LA GESTION DES ACCÈS

- La documentation nécessaire à la mise en place du processus formel de gestion des accès doit être développée et révisée, si requise.
- Les accès à l'information doivent être définis sur la base du principe du privilège minimal et du principe de séparation des tâches.
- Un compte unique et nominatif est requis pour chaque accès octroyé. Les comptes génériques doivent être évités, à moins d'en justifier techniquement l'utilisation. Cette précaution permet de responsabiliser les propriétaires des comptes à l'égard des actions accomplies.
- L'octroi et l'utilisation de privilèges (comptes à privilèges spéciaux) doivent être encadrés et contrôlés rigoureusement.
- Les justificatifs d'attribution des privilèges d'accès de haut niveau doivent rester valides durant toute la période d'attribution de ces privilèges.
- Les contrôles d'accès doivent être mis en place pour s'assurer que les utilisateurs n'auront accès, en tout temps, qu'à l'information nécessaire à l'exercice de leurs fonctions.
- Le départ, le transfert ou la mutation d'un utilisateur ainsi que tout autre changement relatif à ses tâches et ses fonctions doit conduire systématiquement à la révision de ses droits d'accès.

- Toute dérogation aux critères d'habilitation prévus pour disposer des accès requis pour une fonction organisationnelle doit être signée par le gestionnaire et le détenteur concernés.
- Les mécanismes de contrôle d'accès doivent être mis en place en se basant sur le principe du privilège minimal et du degré de sensibilité de l'information utilisée.
- Des règles d'autorisation et de restriction des accès à distance doivent être clairement définies et approuvées par les détenteurs de l'information.
- Les accès attribués doivent être revus de manière périodique, soit tous les trois (3) mois « 21 septembre, 21 décembre, 21 mars, 21 juin ». Les droits, leurs modifications et leurs violations doivent être répertoriés.
- Les habilitations consignées au référentiel des habilitations doivent être, en tout temps, conformes aux descriptions de tâches associées aux fonctions organisationnelles et aux profils d'accès à l'information.
- Un audit des mécanismes de contrôle de gestion des accès doit être effectué périodiquement.
- Les utilisateurs de dispositifs mobiles doivent être sensibilisés aux risques de sécurité encourus par l'information à laquelle ils ont accès. Ils doivent être également formés à l'utilisation des bonnes pratiques en la matière.
- Les utilisateurs doivent être informés de la mise en place des journaux d'activités qui permettent de détecter et de retracer toute activité et tout accès non autorisé.
- Les équipements informatiques de l'organisme doivent être protégés adéquatement contre tout accès non autorisé et contre toute perte ou tout dommage qui pourrait être causé de façon accidentelle ou délibérée.
- L'attribution d'un accès à des données stratégiques est précédée d'un engagement formel de l'utilisateur quant au respect des règles de protection des moyens d'accès fournis et au devoir de signalement en cas de divulgation non autorisée ou même de suspicion de divulgation d'information stratégique.
- Le réseau de l'organisme doit être divisé en zones de sécurité, si requis. Les niveaux de sécurité de ces zones sont fonction du degré de sensibilité de l'information et de la criticité des applications.

7.0 PARTAGE DE RESPONSABILITÉS DE LA GESTION DES ACCÈS

Dans le cadre de la mise en place d'un processus formel de gestion des accès, les principales responsabilités assignées par la présente règle sont les suivantes.

7.1 Le conseil des commissaires

- Adopte la présente règle.

7.2 La direction générale

- S'assure de la diffusion de la présente règle.
- S'assure de la mise en place du processus formel de gestion des accès à l'information au sein de son organisme.

7.3 Le responsable organisationnel de la sécurité de l'information (ROSI)

- Élabore et met à jour la règle de gestion des accès et la soumet pour validation au comité chargé de la sécurité de l'information.
- Soumets à l'approbation du dirigeant de l'organisme la règle de gestion des accès et assure le suivi de sa mise en œuvre. Il lui soumet également toute dérogation à l'application de la règle.
- Définit le processus de gestion des accès.
- S'assure de la documentation et de la mise à jour des procédures nécessaires à la mise en place du processus formel de gestion des accès.
- S'assure de la mise en œuvre du processus de gestion des accès.
- Approuve toute dérogation aux dispositions de la règle.

7.4 Le conseiller organisationnel de la sécurité de l'information (COSI)

- Soutiens-le ROSI dans l'élaboration et la mise à jour de la règle de gestion des accès.
- Soutiens-le ROSI dans la définition du processus de gestion des accès.
- Mets en œuvre le processus de gestion des accès.
- Définis clairement la procédure d'élaboration et de maintien du référentiel des habilitations.
- Définis clairement la procédure d'élaboration et de maintien du référentiel des profils d'accès à l'information.
- Définis clairement la procédure de gestion des identifiants et des autorisations d'accès.
  - ✓ Cette procédure couvre tout le cycle de vie d'un utilisateur dans l'organisme — arrivée, mutation, promotion, départ en congé de longue durée, départ définitif.
- Définis clairement la procédure de gestion et de révision des accès privilèges et des contrôles associés.

- Organise des séances de sensibilisation des utilisateurs des dispositifs mobiles aux risques de sécurité encourus par l'information à laquelle ils ont accès au moyen de ces dispositifs.
- S'assure que l'audit des mécanismes de contrôle de gestion des accès est effectué périodiquement.

7.5 Le coordonnateur organisationnel de la gestion des incidents (COGI)

- Contribue à l'élaboration, la mise en œuvre et la révision de la règle de gestion des accès.
- Détermine les menaces et les situations de vulnérabilité liées à la gestion des accès et, si requis, propose des mesures de renforcement des contrôles d'accès.
- Formule des avis de pertinence sur les mécanismes de gestion des accès mis en place.

7.6 Les détenteurs de l'information

- Définissent les profils d'accès applicatifs supportés par les systèmes de mission (applications) relevant de leur autorité et s'assurent de la conformité des mécanismes d'accès aux exigences relatives à la sécurité de cette information.
- Définissent clairement les règles d'autorisation et de restriction des accès à distance à l'information relevant de leur autorité.
- Définissent les accès à l'information sur la base du principe du privilège minimal et du principe de la séparation des tâches.
- Autorisent les accès à l'information relevant de leur autorité.
- Ajustent dans les délais recommandés tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées.

7.7 Les gestionnaires

- Définissent les habilitations et les critères d'habilitation associés aux fonctions organisationnelles relevant de leur autorité.
- S'assurent de la conformité, en tout temps, des accès autorisés au principe du privilège minimal et des qualifications de leur personnel aux critères d'habilitation associés aux fonctions occupées.
- Documentent les processus d'affaires et définissent clairement les règles de séparation des tâches associées.

- Autorisent et justifient tout besoin d'accès à l'information qui ne fait pas partie des habilitations prévues pour la fonction occupée par l'employé.
- Assurent le suivi des autorisations d'accès octroyées aux utilisateurs relevant de leur autorité depuis leur arrivée jusqu'à leur départ de leur unité administrative.
- Ajustent dans les délais recommandés tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées.
- S'assurent de l'intégration dans les ententes et contrats de clauses garantissant le respect des exigences en matière de sécurité de l'information, dont celles sur la gestion des accès.

7.8 Le responsable de la gestion des technologies de l'information

- Met en place les solutions technologiques répondant aux exigences de la règle de gestion des accès.
- S'assure que les profils d'accès général sont clairement définis pour l'ensemble des postes de travail de l'organisme.
- S'assure que les utilisateurs n'ont pas accès à leur poste de travail en tant qu'administrateurs et que toute exception est documentée et approuvée.
- Met en place :
  - ✓ Des outils de journalisation des accès, ainsi, lors des vérifications périodiques ou sur demande, il sera possible de savoir qui a accédé à quoi.
  - ✓ Des mesures de protection sur les postes de travail contre les accès non autorisés et les vulnérabilités logicielles.
  - ✓ Des mécanismes de surveillance et de contrôle des méthodes d'accès à distance.

7.9 L'administrateur des droits d'accès

- Applique la règle de gestion des accès et les procédures afférentes.
- Crée les identifiants et les droits d'accès pour les utilisateurs dûment autorisés par les gestionnaires et les détenteurs de l'information.
- Édite à l'intention des détenteurs et des gestionnaires les rapports périodiques des autorisations d'accès réellement attribuées et s'assure de leur validation.

7.10 L'utilisateur

- Emploie l'information à laquelle il a accès seulement pour des tâches qui lui sont assignées.
- Est responsable des accès qui lui sont octroyés et redevable auprès de ses gestionnaires de toute action exécutée en utilisant son identifiant et son authentifiant.
- S'engage formellement au respect des règles de protection des moyens d'accès aux données stratégiques.
- Signale, sans délai, toute atteinte à la sécurité de l'information à laquelle il accède.

8.0 LIGNES DIRECTRICES CONCERNANT L'AUTHENTIFICATION

- L'authentification est une procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.
- La méthode d'authentification de loin la plus courante consiste en un code d'accès qui peut être public et un mot de passe qui est toujours privé et qui est associé à l'utilisateur. D'autres méthodes existent aussi.
- Les codes d'accès et les mots de passe sont un aspect important de la sécurité d'un poste de travail ou d'un serveur. Ils sont la ligne de front pour la protection des données de l'utilisateur.
- Un mot de passe mal choisi peut compromettre l'intégrité du réseau de la Commission scolaire de la Beauce-Etchemin.
- Tout utilisateur du réseau de la Commission scolaire de la Beauce-Etchemin, de même que les entreprises et leurs représentants ayant accès au réseau sont responsables de prendre les mesures appropriées, comme décrites ci-dessous, pour choisir et sécuriser son mot de passe.
- L'utilisateur est en tout temps responsable de toute forme de communication effectuée grâce à l'utilisation d'un code d'accès et du mot de passe qui lui est associé et elle ou il voit à les protéger.
- Le but de ces règles de sécurité est d'établir des normes en ce qui concerne l'authentification, de même que la création de mots de passe suffisamment sécuritaires, la protection de ces mots de passe, et leur fréquence de changement.

- Ces règles de sécurité s'appliquent à toute personne qui s'authentifie pour accéder à un poste de travail, un serveur, un réseau ou un logiciel sur le réseau de la commission scolaire.

9.0 TYPE DE CODES D'ACCÈS

On peut distinguer quatre types de codes d'accès :

9.1 Code d'accès personnel

- Un code d'accès personnel en est un qui est alloué individuellement à un utilisateur par l'administratrice ou l'administrateur à titre strictement personnel et confidentiel. Il ne comporte que les privilèges minimaux nécessaires pour accomplir les tâches régulières requises par la personne à qui il est alloué.
- Un code d'accès personnel peut donner accès à différents types de services, par exemple :
  - ✓ L'accès à un poste de travail soit pour l'authentification initiale au début de la session de travail ou pour désactiver l'économiseur d'écran.
  - ✓ L'accès à un compte de courriel.
  - ✓ L'accès à des fichiers ou à des imprimantes disponibles sur un serveur.
  - ✓ L'accès à une application administrative.
  - ✓ L'accès à des données stockées dans une base de données.
  - ✓ L'accès au contenu d'un site Web pour les gestionnaires de sites Web.
  - ✓ L'accès à site Web transactionnel.
  - ✓ L'accès à un serveur de copies de sécurité.

9.2 Code d'accès de groupe

- Un code d'accès et un mot de passe de groupe peuvent être alloués à un membre désigné responsable de ce groupe. Dans ce cas, la personne responsable du groupe se porte garante de l'utilisation qui est faite du code d'accès de groupe.
- Seul le responsable d'un groupe peut dévoiler le mot de passe associé au code d'accès, ou le modifier.

9.3 Code d'accès système

- Un code d'accès système comporte les particularités suivantes :
- Beaucoup plus de privilèges sont associés aux codes d'accès système qu'aux autres types de codes d'accès.
- Un code d'accès système est utilisé pour modifier la configuration d'un serveur ou d'un poste de travail, ou encore pour accéder à la configuration d'une composante importante d'un progiciel comme c'est le cas pour les codes d'administrateurs de bases de données.
- Ces caractéristiques font qu'il est crucial de bien encadrer l'utilisation des codes d'accès système et des mots de passe qui leur sont associés.

9.4 Code d'accès générique

- Dans certaines circonstances particulières, lorsqu'il n'y a pas moyen de faire autrement, un code d'accès et un mot de passe générique peuvent être utilisés. Toutes les précautions doivent alors être prises pour limiter au minimum les privilèges du code d'accès générique.

10.0 RÈGLES GÉNÉRALES CONCERNANT LES MOTS DE PASSE

10.1 Changement et choix du mot de passe

- Chaque utilisateur a la responsabilité de choisir un mot de passe difficile à deviner. Le mot de passe doit contenir au moins neuf (9) caractères et inclut au minimum deux (2) lettres et deux (2) chiffres. La directive concernant le contenu du mot de passe pourra être redéfinie par le responsable des technologies de l'information, selon les critères de sécurité qui évoluent dans le temps.
- Le mot de passe devra être changé au plus tard 90 jours après avoir été modifié. Il ne sera pas possible d'utiliser l'historique des 5 derniers mots de passe. La directive concernant le changement du mot de passe pourra être redéfinie par le responsable des technologies de l'information, selon les critères de sécurité qui évoluent dans le temps.

10.2 Divulgation, conservation et transfert d'un mot de passe

- Un utilisateur, de même qu'une ou un responsable de groupe ou un membre du groupe à qui les informations sont communiquées ne peut, en aucun cas, communiquer, transmettre ou dévoiler d'aucune façon son mot de passe à un autre utilisateur, ou à un tiers.
- Les mots de passe ne doivent jamais être conservés par écrit ou en ligne, à moins d'utiliser un mécanisme sécuritaire. De même, les mots de passe ne peuvent en aucun cas être stockés sur disque ou circuler sur le réseau en texte clair. Ils doivent être chiffrés.
- Lorsque techniquement réalisable, un algorithme de chiffrement à sens unique doit être utilisé pour le stockage des mots de passe.

10.3 Mot de passe compromis

- Un utilisateur qui croit que son mot de passe a pu être deviné ou compromis doit rapporter l'incident à l'équipe du centre d'assistance du SRIO et modifier immédiatement ce mot de passe.

10.4 Divers

- Le mot de passe choisi doit être exclusivement utilisé pour la Commission scolaire de la Beauce-Etchemin. Il ne doit pas être utilisé à dans un contexte personnel, par exemple, un compte de fournisseur d'accès Internet pour la maison, un site de commerce en ligne, un serveur public de courrier électronique comme Hotmail ou Gmail, etc.).
- Une recherche de mots de passe peut être réalisée périodiquement ou aléatoirement par l'équipe de sécurité informatique du SRIO dans le but de découvrir des mots de passe trop faciles à découvrir. Si un mot de passe est trouvé pendant une de ces recherches, l'utilisateur devra le modifier ou, à défaut, son code d'accès sera désactivé.
- Lorsque techniquement réalisables, des mécanismes empêchant les utilisateurs de choisir des mots de passe simples seront mis en place.

11.0 RÈGLES PARTICULIÈRES CONCERNANT LES CODES D'ACCÈS SYSTÈME

- En temps normal, seul le personnel spécialisé en informatique travaillant sous la supervision de la direction du SRIO peut détenir un code d'accès système et le mot de passe qui lui est associé. Si ce n'est pas le cas, une autorisation préalable de la direction du SRIO est nécessaire.

- Lorsqu'un code d'accès système est partagé par plus d'une personne, le nombre de personnes doit être maintenu au minimum.
- Les mots de passe des codes d'accès système doivent être différents de tous les autres codes d'accès personnels ou de groupe détenus par une même personne.
- Les mots de passe des codes d'accès du système doivent être changés au moins tous les 90 jours, qu'il soit exigé ou non par les systèmes.
- Lorsque ceci est techniquement possible, des mécanismes de journalisation doivent être mis en place pour qu'il soit possible d'identifier qui a utilisé un code système partagé par plusieurs personnes.
- Un registre sécurisé des codes d'accès système, des mots de passe qui leur sont associés et des personnes qui les détiennent doit être mis en place.

12.0 AUTRES MÉTHODES D'AUTHENTIFICATION

D'autres méthodes d'authentification existent, dans tous les cas, toutes les précautions nécessaires doivent être prises pour que le processus d'authentification visé soit respecté et que seules les personnes autorisées puissent accéder à la ressource protégée.

Voici des méthodes d'authentification et les précautions à prendre lorsque chacune de ces méthodes est utilisée :

12.1 Biométrie

- La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne (empreintes digitales, pupille des yeux, visage, voix), destinée à déterminer son identité de manière irréfutable.
- Lorsque la biométrie est utilisée, il faut s'assurer que l'algorithme utilisé pour reconnaître une personne par rapport à une autre est suffisamment raffiné pour assurer l'authentification de la bonne personne.
- Si des mots de passe sont impliqués dans le processus d'authentification (par exemple, lorsque l'empreinte digitale du bon utilisateur est reconnue, un logiciel fournit le mot de passe, préalablement enregistré au système), toutes les dispositions relatives aux mots de passe doivent aussi être respectées.

12.2 Radio-identification (cartes RFID)

- La radio-identification, le plus souvent désignée par le sigle RFID (de l'anglais *Radio Frequency Identification*), est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes »
- Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collés ou incorporés dans des objets. Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur.

  Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.

  Dans tous les cas où une serrure est impliquée, incluant les contrôles d'accès des établissements, les utilisateurs doivent être sensibilisés à la sécurité des accès. Ils doivent ainsi refermer derrière eux une porte barrée et ne pas laisser entrer avec eux des personnes n'ayant pas droit d'accès.

12.3 Serrure physique

- Dans certains cas, la seule méthode de contrôle disponible en est une physique, à savoir une serrure pouvant être ouverte avec un code numérique ou une clé physique.
- S'il s'agit d'une serrure avec un code numérique, il faut donner un code numérique différent à chaque personne ayant accès au local. Les codes doivent être désactivés lorsqu'une personne part ou perd le droit d'accès au local. Il est aussi fortement recommandé d'enregistrer toutes les entrées et sorties.
- Lorsqu'il s'agit d'une serrure à clé physique, les règles normales de sécurité physique s'appliquent : comptabiliser les clés qui sont distribuées, les récupérer lorsque les gens partent, etc.
- Dans tous les cas où une serrure est impliquée, les utilisateurs doivent être sensibilisés à la sécurité des accès. Ils doivent ainsi refermer derrière eux une porte barrée et ne pas laisser entrer avec eux des personnes n'ayant pas droit d'accès.

13.0 SANCTIONS

- Lorsqu'un utilisateur contrevient à la présente règle concernant la gestion des accès et l'authentification ou aux réglementations en découlant, il s'expose à faire face à des mesures disciplinaires, administratives ou légales en fonction de son geste, conformément aux dispositions des conventions collectives, des ententes, des contrats ou des règlements.
- L'organisme peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.