3.5.2.2. Directive sur la gestion des identités et des accès logiques et physiques

OBJECTIF

- Sensibiliser les personnes impliquées aux mesures à prendre afin que les accès respectent les meilleures pratiques de sécurité.
- Assurer que les accès ne soient accordés qu'aux personnes autorisées qui ont un besoin d'affaire légitime.
- Protéger les renseignements personnels du personnel, des élus, des parents et des élèves.

ÉNONCÉ

Ce document présente les lignes directrices ainsi que les recommandations à suivre dans le cadre de la gestion des identités et des accès, autant logiques (par ex. aux applications informatiques) que physiques (par ex. aux bâtiments ou locaux). Les identités, les identifiants de connexion, les privilèges d'accès et tous les autres éléments utilisés pour fournir des accès aux installations, systèmes, applications et données du CÉF doivent être gérés en accord avec les règles généralement reconnues et acceptées afin de rencontrer les objectifs de la directive.

CHAMP D'APPLICATION

Cette ligne directrice s'applique aux gestionnaires responsables des données, aux responsables d'actifs informationnels et aux personnes à qui l'on délègue la responsabilité du contrôle d'accès aux actifs matériels, logiciels et informationnels du CÉF.

DÉFINITION

Authentification
Acte permettant d'établir la validité d'une personne ou d'un appareil.

Section 3 – Administration centrale

Chiffrement
Opération par laquelle on utilise un algorithme pour remplacer un texte en clair par un texte inintelligible et inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Classification de l'information
Identification de la valeur de l'information pour l'organisation dans le but d'assurer un niveau de protection approprié (public, interne ou confidentiel) selon les principes d'intégrité, de confidentialité et de disponibilité. Cet exercice est conduit en partenariat avec le service de la gestion des documents et le centre des archives du CÉF.

Identité
Ensemble d'éléments qui permettent de reconnaître une personne et de la distinguer d'une autre.

Identifiant
Information associée à une personne, connue de celle-ci ou contenue sur un support informatique dont elle est la détentrice, et qui permet son identification.

Identification
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.

Ouverture de session
Procédure d'entrée en communication d'un utilisateur qui doit inscrire un nom d'utilisateur et un mot de passe pour accéder à un réseau ou à un système informatique.

Direction propriétaire d'un actif informationnel
Direction qui a été désignée responsable d'un actif par le comité de sécurité.

Responsable d'un actif informationnel
Personne qui a été désignée par la direction propriétaire d'un actif pour prendre en charge la responsabilité de la sécurité de celui-ci, notamment en faisant la classification et en donnant les autorisations d'accès.

Période d'application
Cette directive est en vigueur dès son approbation par le CSF.

Section 3 – Administration centrale

Contenu

1. CONTRÔLE D'ACCÈS

Des règles générales et spécifiques gouvernent l'octroi et le contrôle des accès aux installations, systèmes, applications et informations du CÉF.

1.1 Règles générales

Les règles d'accès à un actif (matériel, logiciel ou informationnel) du CÉF sont déterminées par la coordination des technologies.

L'octroi d'accès ou de privilèges doit être aligné avec la classification de l'information (publique, interne ou confidentielle) associée à l'actif, c'est-à-dire que l'utilisateur doit posséder les habilitations nécessaires afin d'obtenir les accès aux actifs jugés internes ou confidentiels. L'octroi d'accès ou privilèges doit aussi être fait en relation avec les obligations légales, règlementaires et contractuelles du CÉF en matière d'accès à l'information et aux services.

Les privilèges et les accès doivent être accordés selon un modèle d'accès minimum, c'est-à-dire que seuls les accès et privilèges essentiels sont autorisés.

Les partages d'accès sont interdits en toutes circonstances. Il est essentiel qu'une identité ne corresponde qu'à une seule personne. Si un mot de passe ou une carte d'identité est partagé entre employés, il devient alors impossible d'établir hors de tout doute que les accès ont été faits par le détenteur autorisé.

1.2 Besoin de savoir et besoin d'affaires

Il doit exister une justification d'affaires pour l'octroi d'accès ou de privilèges, laquelle doit se baser sur le besoin de « savoir et d'utiliser », c'est-à-dire que l'accès et/ou les privilèges soient absolument nécessaires pour l'accomplissement des tâches reliées à l'emploi du récipiendaire de l'accès ou des privilèges.

Les besoins de savoir et d'utiliser sont définis comme suit :

1. **Besoin de savoir** :

   L'accès est accordé seulement à l'information requise pour l'accomplissement des tâches reliées à l'emploi. Les différentes tâches ou rôle dans l'organisation signifient des besoins de savoir différents et donc des profils d'accès différents.

2. **Besoin d'utiliser** :

   L'accès est accordé seulement aux locaux, installations, systèmes et applications qui sont requis pour l'accomplissement des tâches reliées à l'emploi.

1.3 Ségrégation des rôles et contrôle d'accès

Les rôles impliqués dans les processus de contrôle d'accès doivent être ségrégués pour prévenir l'octroi d'accès et/ou de privilèges frauduleux ou sans autorisation.

Les rôles suivants doivent être ségrégués :

- **Requérant** : Le requérant d'accès ou de privilèges ne peut pas être impliqué dans les processus de contrôle d'accès.
- **Autorisation** : L'autorisation doit être faite par un cadre du CÉF qui est le responsable de l'actif informationnel, l'autorisation ne peut pas être déléguée au requérant ou à un administrateur d'actif (installation, système ou application).
- **Administration** : La création d'un compte ou d'un privilège peut uniquement être effectuée par le personnel de la direction du propriétaire de l'actif ou son mandataire et ne peut pas l'être par le requérant ni la personne ayant autorisé les accès ou privilèges.
- **Délégation de l'attribution des accès** : Un responsable d'actif informationnel peut déléguer une personne responsable dans son service pour l'attribution des accès.

Le requérant est habituellement le supérieur immédiat de la personne devant recevoir les accès ou les privilèges. Si le requérant est le récipiendaire des accès, le supérieur du requérant doit approuver la requête. La personne autorisant les accès doit être le responsable de l'actif informationnel pour lequel les accès ou privilèges sont demandés.

1.4 Autorisation formelle

L'autorisation d'octroi des accès ou des privilèges doit être formellement documentée par le biais d'un registre de contrôle des accès.

Aucun accès ou privilège ne doit être accordé avant la finalisation des procédures d'autorisation.

1.5 Revue périodique des accès

Pour s'assurer que leur validité soit maintenue, tous les accès et privilèges doivent être revus périodiquement et minimalement de façon annuelle.

- La revue des accès est initiée par la coordination des TI et exécutée par le responsable de l'actif informationnel.

- La revue des accès se fait en collaboration avec les gestionnaires d'équipes, les requérants initiaux et les responsables d'actifs informationnels.

- Tout accès ou privilège qui n'est plus requis doit être révoqué immédiatement. Quand de tels accès non-requis sont découverts, les modalités d'exécution des procédures de contrôle d'accès doivent être examinées pour déterminer les raisons de la non-révocation au cours de l'exécution des procédures d'accueil, de transfert et de départ.

Particularité pour les accès physiques

La revue des accès aux salles technologiques est initiée par la coordination des TI et un des informaticiens afin de fournir l'information nécessaire.

1.6 Accès privilégiés

Les accès privilégiés (comptes) comprennent tous les niveaux d'accès permettant d'outrepasser les règles d'accès standard. Par exemple, les membres du groupe *Active Directory* appelés « Administrateurs » peuvent accéder à tous les actifs technologiques et informatiques (TI) peu importe les règles d'accès et modifier les attributs de ces actifs (les règles d'accès, la journalisation, etc.).

Parce que ces accès privilégiés peuvent avoir un impact majeur sur les actifs TI, ils sont soumis aux règles spécifiques suivantes :

1. Tous les accès ou comptes à privilège doivent être enregistrés sur une liste mentionnant le détenteur autorisé, les actifs qu'il est autorisé à accéder via ce compte et le niveau d'accès du compte.
2. Tous les accès à privilège doivent être autorisés par un cadre de la coordination des TI du CÉF ou son supérieur.

3. Toute utilisation d'un accès à privilège doit être faite via une requête de changement et formellement autorisée. Aucune utilisation non-autorisée d'un accès à privilège n'est permise.
4. Le partage des accès à privilège est formellement interdit et tous les accès à privilège doivent maintenir l'imputabilité des accès.

Les comptes à privilège doivent être différents de ceux utilisés pour les activités ne requérant pas de privilège, comme les tâches journalières telles que le courriel, la modification des documents, etc. Les comptes à privilège ne doivent être utilisés que pour les tâches requérant des privilèges plus élevés.

2. ACCUEIL D'UN NOUVEL EMPLOYÉ ou D'UN NOUVEL ÉLU

A) Dès l'embauche d'un nouvel employé, stagiaire, sous-traitant, consultant, etc, le processus « d'accueil » débute et est initié par la coordination des ressources humaines (RH) ou son délégué. La coordination qui accueille le nouvel employé est responsable de la création des accès et de leurs autorisations. La coordination des RH est responsable de la gestion des identités des employés.

B) Dans le cas d'un tiers (ex. consultant), un cadre doit être désigné pour se porter garant de l'identité du tiers. La coordination qui retient les services du tiers est responsable de la gestion des identités des tiers.

C) Dès l'élection d'un élu, le processus « d'accueil » débute et est initié par la direction générale aux affaires ou son délégué. La direction générale aux affaires qui accueille le nouvel élu est responsable de la création des accès et de leurs autorisations. La direction générale aux affaires ou son délégué est responsable de la gestion des identités des élus.

2.1 Enregistrement des utilisateurs

Lors de la création du dossier d'employé, les RH s'assurent d'y intégrer les identifiants numériques (comptes utilisateurs) de l'employé. Lors de l'entrée en fonction d'un tiers, la coordination responsable intègre les identifiants numériques (comptes utilisateurs) du tiers au dossier de l'employé qui se porte garant de celui-ci.

Lors de la création du dossier d'un élu, les RH s'assurent d'y intégrer les identifiants numériques (comptes utilisateurs) de l'élu.

Le dossier RH de l'employé ou de l'élu constitue son identité, laquelle sera reliée à tous les identifiants utilisés pour effectuer les accès aux installations, équipements, systèmes et application du CÉF.

Le détenteur d'un compte sera responsable de toute action faite via le compte. Par

exemple, le cas d'un employé ou d'un élu, une entrée dans un répertoire doit correspondre à un numéro d'employé ou d'élu lequel est associé à un dossier RH ou d'élu. Cette interrelation entre les comptes et les personnes constitue l'enregistrement des utilisateurs.

Tous les octrois d'accès nécessitent la confirmation de l'identité de l'utilisateur. Les accès doivent donc être une procédure formelle d'enregistrement des utilisateurs.

Le partage d'un compte est strictement interdit. Ces circonstances exceptionnelles peuvent demander la création d'un compte à être partagés. Les requêtes en ce sens doivent être acheminées à la coordination des TI qui effectuera une analyse de risque et mettra en place des mesures de sécurité compensatoire.

3. ACCUEIL D'UN NOUVEL ÉLÈVE

À l'arrivée d'un nouvel élève, le processus « d'accueil » débute et est initié par la coordination des TI ou délégué du secteur des technologies assigné dans les écoles fransaskoises. La coordination des TI ou son délégué qui accueille le nouvel élève est responsable de la création des accès et de leurs autorisations. La coordination des TI est responsable de la gestion des identités des élèves.

3.1 Enregistrement des utilisateurs

Lors de la création du dossier d'élève au secteur des ressources technologiques, ils s'assurent d'y intégrer les identifiants numériques (comptes utilisateurs) de l'élève.

Le détenteur d'un compte sera responsable de toute action faite via le compte.

Tous les octrois d'accès nécessitent la confirmation de l'identité de l'utilisateur. Les accès doivent donc être une procédure formelle d'enregistrement des utilisateurs.

Le partage d'un compte est strictement interdit. Ces circonstances exceptionnelles peuvent demander la création d'un compte à être partagé. Les requêtes en ce sens doivent être acheminées à la coordination des TI qui effectuera une analyse de risque et mettra en place des mesures de sécurité compensatoire.

4. Communication des mots de passe

Deux possibilités peuvent survenir lors de la création d'un nouveau compte utilisateur. Celles-ci ont un impact sur la façon dont doit être communiqué le mot de passe utilisateur.

Quand le système correspondant au compte permet à l'utilisateur de faire la gestion de

son mot de passe (le modifier, le réinitialiser, etc.), un mot de passe initial doit être configuré et communiqué à l'utilisateur, Celui-ci devra le changer lors de la première connexion avec le compte. Ce mot de passe initial doit expirer au bout de 48 heures le cas échéant.

Le mot de passe initial d'un compte doit être communiqué de façon sécuritaire à l'utilisateur. Le téléphone, les boîtes vocales, les textos ou verbalement en personne sont des moyens de communication acceptables. Le courriel est également un moyen de communication acceptable sous la condition que le « courriel de communication » du mot de passe ne contienne pas le nom du compte utilisateur. Si le mot de passe est communiqué à l'utilisateur par téléphone, une authentification sécuritaire de la personne doit avoir lieu avant de le lui communiquer.

Quand le système correspondant au compte ne permet pas à l'utilisateur de faire la gestion de son mot de passe, le mot de passe permanent ne doit jamais être communiqué par courriel.

Peu importe qu'ils soient temporaires ou permanents, les mots de passe, doivent être uniques et difficiles à deviner. Se référer à la directive ***3.5.2.1 Directive sur la sélection et la protection des mots de passe.***

5. Transfert

Dans une organisation, les employés peuvent changer de position, être promus et leur rôles et responsabilités peuvent ainsi changer au fil du temps.

Lorsque cette situation se produit, une révision et un ajustement des accès et des privilèges de l'employé et des élus doivent avoir lieu. La coordination des RH est responsable d'initier la procédure de révision des accès en amorçant le processus des interactions entre les groupes responsables des autorisations et ceux responsables d'effectuer les changements aux accès.

Par exemple : une personne travaillant à la direction des finances de l'organisation est promue comme chef d'équipe de l'équipe dont elle faisait partie. Les privilèges de cette personne doivent être revus puisque ses nouvelles tâches demanderont qu'elle agisse en tant que requérant d'accès pour les membres de son équipe. Son nouveau rôle ne nécessitera probablement plus le besoin d'accéder aux systèmes financiers. De plus, sans une révision de ses accès, un risque de conflit d'intérêts existe puisque cette personne pourrait effectuer des opérations dans les systèmes financiers en plus de les autoriser alors que ces deux rôles doivent être ségrégués.

Donc en règle générale, tous les accès et privilèges non-requis pour l'accomplissement des nouvelles tâches doivent être révoqués.

6. Départ

6.1 Désenregistrement des utilisateurs (employés et élus)

Les employés, stagiaires, consultants et autres membres du personnel du CÉF, quitteront un jour ou l'autre l'organisation pour diverses raisons (maladie prolongée, congé parental, invalidité, retraite, départ volontaire, mise-à-pied, congédiement, etc.).

Au départ de chaque utilisateur, tous les accès et privilèges doivent être immédiatement révoqués. Aucun accès ne doit être maintenu après la fin de l'emploi ou de la relation contractuelle. Dans le cas d'une absence temporaire, les accès et privilèges sont normalement désactivés et non pas révoqués.

La coordination des RH est responsable d'initier le processus visant la désactivation ou révocation des accès et des interactions avec les groupes autorisant et effectuant cette tâche. Le supérieur hiérarchique de l'employé qui quitte son emploi doit obligatoirement aviser les RH du départ de l'employé et leur demander d'initier le processus.

6.2 Désenregistrement des utilisateurs (élèves)

Les élèves quitteront un jour ou l'autre le CÉF. Au départ de chaque utilisateur, tous les accès et privilèges doivent être immédiatement révoqués. Aucun accès ne doit être maintenu après le départ de l'élève.

La coordination des TI ou son délégué est responsable d'initier le processus visant la désactivation ou la révocation des accès. La direction d'école doit obligatoirement aviser la coordination des TI du départ d'un élève et lui demander d'initier le processus.

7. Responsabilités des employés, élus et élèves

Les utilisateurs ne doivent, en aucune circonstance, partager leur mot de passe avec quiconque (supérieur, collègues, soutien technique, ressources humaines ou autres).

Il est interdit de demander le mot de passe d'un utilisateur afin qu'un collègue puisse accéder à ses dossiers durant son absence. Si un accès au compte d'un utilisateur est

requis durant son absence, un nouveau compte doit être créé avec les mêmes accès et privilèges et confié au remplaçant.

En cas d'urgence, le soutien technique peut être contacté pour avoir accès à des données d'un compte.

Les mots de passe ne doivent jamais être écrits sur un papier, dans un fichier ou enregistrés sur quelque média que ce soit sans chiffrement. L'utilisation de gestionnaires de mots de passe est permise s'il est autorisé par la coordination des TI.

8. Système d'authentification

8.1 Ouverture de session sécuritaire

Tous les actifs informationnels (systèmes, équipements et applications) devraient fournir une ouverture de session sécuritaire aux utilisateurs :

1. Masquer le mot de passe lorsqu'il est entré par l'utilisateur.
2. S'abstenir d'afficher l'identification du système, équipement ou application jusqu'à ce que le login soit complété avec succès.
3. Afficher une bannière avertissant que le système, équipement ou application doit seulement être accessible aux utilisateurs autorisés
4. Éviter de fournir de l'aide à l'utilisateur qui pourrait être utilisée par un intrus.
5. Afficher seulement des messages d'erreur génériques tels que « erreur de login » sans indication du champ en erreur (mot de passe ou nom d'utilisateur)
6. Fournir de la protection contre les attaques par force brute en verrouillant le compte pour 10 ou 15 minutes après 3 tentatives d'accès infructueuses.
7. Inscrire dans un journal toutes tentatives d'accès qu'elles soient couronnées de succès ou non.
8. Déclarer un évènement de sécurité dès qu'une tentative d'accès est détectée comme étant malicieuse (par exemple, 3 tentatives sur de multiples comptes).
9. Éviter de transmettre de mot de passe en clair sur un réseau.
10. Éviter de stocker des mots de passe sans chiffrement unidirectionnel.
11. Implanter un délai d'inactivité de 15 minutes.
12. Implanter un délai d'expiration de session de 8 heures.
13. Empêcher les ouvertures de sessions multiples simultanées d'un même compte.

8.2 Gestion centralisée

Tous les systèmes d'authentification doivent être gérés centralement. Il est donc interdit de configurer des comptes locaux sur les actifs informationnels.

Cette règle a pour but de faciliter la gestion des accès en permettant la création et la révocation d'accès via un seul processus (par exemple, en révoquant le compte dans un registre, tous les accès correspondants sont eux aussi révoqués). Avec des comptes locaux, il existe un risque que des comptes soient oubliés lors de la révocation des accès.

8.3 Gestion des mots de passe

Tous les systèmes d'authentification doivent gérer les mots de passe de façon sécuritaire et être conformes avec les règles minimales du CEF. Les systèmes d'authentification doivent :

1. Permettre aux utilisateurs de changer leur mot de passe et fournir un mécanisme de protection contre les erreurs de frappe pour le nouveau mot de passe.
2. Décourager le choix de mots de passe faibles et forcer la conformité des mots de passe aux règles de complexité des mots de passe du CEF.
3. Forcer les utilisateurs à changer leur mot de passe à la première ouverture de session.
4. Forcer l'expiration des mots de passe périodiquement (typiquement aux 90 jours).
5. Empêcher la réutilisation des 5 derniers mots de passe.

9. Support

Pour toute question reliée à l'interprétation de ces lignes directrices, veuillez vous adresser au secteur des ressources informatiques.

10. Historique des révisions

Date	Version	Description	Auteur