3.5.2.1. Directive sur la sélection et la protection des mots de passe

1. Objectif

- Assurer la sécurité des informations détenues par l'administration centrale des bureaux administratifs et les écoles fransaskoises.
- Définir les rôles et les responsabilités dans la sélection et la protection des mots de passe.
- Normaliser la sélection des mots de passe.
- Établir la durée d'un mot de passe.
- Diminuer les risques de piratages informatiques.

2. Énoncé

L'utilisation de mots de passe est à la base de la sécurisation des systèmes d'information, mais en contrepartie, cette technique est souvent contournée pour tenter de simplifier la vie des utilisateurs.

Sans la présence de règles précises et forcées, il n'est pas rare de voir des gens faire le choix de mot de passe triviaux, utiliser les mots de passe par défaut des systèmes et même au pire, ne pas utiliser de mot de passe.

Dans ce contexte, la présente directive a pour but :

- De sensibiliser les usagers des systèmes informatiques à l'importance d'utiliser un mot de passe fort;
- De sensibiliser l'administration dans les bureaux administratifs et les écoles du CÉF sur l'importance de mettre en place des contrôles systématiques pour valider la qualité des mots de passe;
- De sensibiliser les concepteurs et les administrateurs de systèmes informatiques de l'utilisation et la gestion des mots de passe;
- De préciser les limites de la sécurité apportée par les mots de passe.

3. Champ d'application

Les lignes directrices sont applicables à tous les employés, élus, contractuels, parents, bénévoles et élèves du CÉF, titulaires d'un compte utilisateur, ou toutes autres formes d'accès similaire, qui supportent ou requièrent un mot de passe et qui donnent accès aux systèmes informatiques du CÉF.

4. Définition

Authentification
Acte permettant d'établir la validité de l'identité d'un membre du personnel ou d'un appareil.

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 la ramener à sa forme initiale.

Compte utilisateur (nom d'usager, *username*, *login*)
Il s'agit d'une séquence unique de caractères utilisés pour identifier un usager et permettre l'accès à un ordinateur ou un système informatique. Le compte utilisateur est habituellement accompagné d'un mécanisme d'authentification comme par exemple un mot de passe.

Infrastructure technologique
Ensemble des installations et des équipements nécessaires à l'emploi des technologies de l'information et de l'informatique.

Mot de passe
Moyen d'authentification pour utiliser une ressource ou un service dont l'accès est limité et protégé.

5. Contenu

1. INTRODUCTION

Malgré le développement de mécanismes d'authentification intrinsèquement plus robustes, l'usage des mots de passe est encore répandu pour établir la base des mécanismes d'authentification.

Pour être efficace, un mot de passe doit respecter certaines règles de base qui lui permettront de se qualifier dans la catégorie mot de passe fort. En établissant une base solide, les mots de passe deviennent plus difficiles à deviner même à l'aide d'outils automatisés qui peuvent générer des millions de possibilités en quelques secondes. Il faut savoir que la force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. Si un mot de passe est construit à l'aide de plusieurs types de caractères (minuscules, majuscules, caractères spéciaux et chiffres) il devient techniquement beaucoup plus difficile à deviner qu'un mot de passe composé uniquement d'une sorte de caractères.

Par exemple :

- Un mot de passe composé de 10 caractères, avec l'alphabet en minuscule. 10 caractères et 26 possibilités par caractères (les lettres de l'alphabet)

10^{26} = 100 000 000 000 000 000 000 000 000 000

- Un mot de passe composé de 10 caractères, avec l'alphabet en minuscule et majuscule. 10 caractères et 52 possibilités par caractères (les lettres de l'alphabet x2)

10^{52} = 10 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000

Malgré ceci, un mot de passe ne peut pas être considéré fort s'il est trop difficile à retenir. Dans de tel cas, l'expérience démontre que les utilisateurs utilisent toutes sortes de techniques qui compromettent la force de leurs mots de passe afin de les retenir plus facilement. Par exemple, les techniques les plus connues sont l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier.

En annexe (A) à cette directive, nous vous fournissons de la documentation qui présente des techniques afin de faciliter le choix de vos mots de passe forts.

2 SÉLECTION DES MOTS DE PASSE

2.1 Pour chacun des systèmes informatiques où il se voit confier un accès avec des privilèges, un utilisateur a l'obligation de choisir un mot de passe fort qui respecte les normes présentées ci-après.

2.2 Lorsque la technologie le permet, la coordination des technologies et de l'informatique (TI) s'assure d'implanter des règles automatisées pour forcer cette façon de faire. Pour les autres cas, les utilisateurs ont la responsabilité d'appliquer ces règles eux-mêmes.

2.3 Sur une base régulière, la coordination des TI transmet des rappels aux usagers des différents systèmes où les mécanismes de changement de mots de passe ne sont pas automatisés. Ces avis doivent alors être interprétés comme une obligation d'exécution, et ce, dès qu'ils sont reçus.

2.4 La coordination des TI se base sur les meilleures pratiques de l'industrie afin d'établir les critères à respecter lors de la création d'un mot de passe fort. Ces critères sont les suivants :

2.4.1 Le nombre de caractères minimum est établi à dix (10) ;

2.4.2 Un mot de passe fort est un mot de passe qui contient des caractères provenant de trois des quatre groupes suivants :
- Lettres minuscules (a,b,c …)
- Lettres majuscules (A,B,C…)
- Chiffres (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
- Symboles (` ~ ! @ # $ % ^ & ( )* - + = | \ { } [ ] : ; " ' < > , . ? /)

2.4.3 Un mot de passe fort ne doit pas contenir plus de quatre lettres consécutives du compte utilisateur auquel il est associé ;

2.4.4 Un mot de passe fort ne doit pas être créé à partir d'informations personnelles concernant l'utilisateur, son conjoint, un membre de sa famille, un numéro de licence automobile, une date d'anniversaire, un numéro d'assurance sociale, etc. ;

2.4.5 Un mot de passe fort ne doit pas être un mot du dictionnaire, le nom du personnage d'un livre ou d'un film, le nom de votre animal de compagnie, etc. ;

2.4.6 Un mot de passe fort ne doit pas être un mot de n'importe quelle langue correctement orthographié et écrit à l'endroit ou même à l'envers ;

2.4.7 Un mot de passe fort doit être renouvelé à une fréquence raisonnable. Idéalement entre 2 et 4 fois par an selon la criticité des données du système informatique qu'il protège ;

2.4.8 Un mot de passe fort ne doit pas être identique aux 5 derniers mots de passe utilisés (validation de l'historique).

3 PROTECTION DES MOTS DE PASSE

3.1 Pour qu'un mot de passe demeure un moyen d'authentification efficace, il doit demeurer secret sans quoi vos privilèges sont accessibles à tous et vos responsabilités ne sont plus sous votre gouverne.

3.2 Pour assurer la protection de vos mots de passe, vous avez l'obligation de respecter les directives suivantes :

3.2.1 Ne révélez pas ou ne partagez pas vos mots de passe avec un employé de l'administration incluant le personnel du service des TI ou votre supérieur ;

3.2.2 Ne partagez pas un mot de passe avec des membres de votre famille ;

3.2.3 Ne révélez jamais un mot de passe pendant une conversation téléphonique ;

3.2.4 Ne demandez jamais à un tiers de vous créer un mot de passe ;

3.2.5 Modifiez systématiquement et le plus rapidement possible les mots de passe par défaut lorsque les systèmes en contiennent ;

3.2.6 Ne vous envoyez pas vos propres mots de passe par votre messagerie personnelle ;

3.2.7 N’utilisez pas le même mot de passe pour vos accès professionnels et pour vos accès personnels ;

3.2.8 Ne révélez jamais un mot de passe sur des questionnaires ou des formulaires peu importe leur nature ;

3.2.9 Ne stockez pas les mots de passe dans un dossier de n’importe quel système informatique. Ceci inclut les ordinateurs de poche et autres dispositifs semblables qui ne sont chiffrés selon une méthode reconnue ;

3.2.10 N'écrivez pas les mots de passe et ne les stockez pas n'importe où dans votre bureau ;

3.2.11 N'employez pas la caractéristique « *se souvenir du mot de passe* » des applications et des logiciels (par exemple, Internet Explorer, Outlook, applications web) ;

3.2.12 Si vous soupçonnez que quelqu’un est en possession de vos mots de passe ou si vous constatez que quelqu’un tente de vous les subtiliser, assurez-vous de réaliser les deux tâches suivantes dans les plus brefs délais :

3.2.12.1 Informer un membre de l’équipe de la coordination des TI de cette situation ;

3.2.12.2 Changez **tous** vos mots de passe professionnels et personnels.

4 VALIDATION DU RESPECT DE CETTE DIRECTIVE

4.1 Sur une base ponctuelle, le service des TI se réserve le droit de vérifier si les règles établies dans cette directive sont respectées par les usagers. Par exemple, la coordination des TI pourrait demander à une firme externe de procéder à un test de pénétration qui ciblerait particulièrement le choix des mots de passe. Dans une telle approche un spécialiste pourrait tenter des techniques d’ingénieries sociales ou il pourrait utiliser des outils spécialisés.

4.2 Si cet exercice permet de déceler des problèmes quant à l’application des règles établies par certains employés, la coordination des TI fera un rapport immédiat aux directions concernées, ainsi qu’à la direction générale. Le rapport de cet évènement sera concilié dans la base de données du service des TI.

5 RÉVISION DE LA DIRECTIVE

Sur une base régulière, des modifications seront apportées à ce document afin de suivre l’évolution des bonnes pratiques en matière de sécurité de l’information. Ces modifications seront faites au minimum sur une base annuelle et ne nécessiteront pas que ce document soit resoumis pour approbation si les principes fondamentaux ne sont pas modifiés. Les usagers seront tout de même informés des modifications.

6 SUPPORT

Pour toute question reliée à l'interprétation de ces lignes directrices et les conseils contenus à l'Annexe, veuillez vous adresser au service des TI du CÉF.

ANNEXE A

CONSEILS SUR LA CRÉATION DES MOTS DE PASSE

1 UTILISEZ DES SYMBOLES PLUTÔT QUE DES CARACTÈRES

Généralement, les gens ont tendance à mettre les symboles et les nombres requis à la fin d'un mot qu'ils connaissent, par exemple « Allison1234 ». Malheureusement, ces mots sont relativement faciles à décrypter. Le mot « Allison » figure dans de nombreux dictionnaires qui contiennent des noms courants. Une fois le nom découvert, il ne reste plus qu'au pirate à deviner les quatre autres caractères. Remplacez plutôt une ou plusieurs des lettres du mot par des symboles que vous pourrez facilement retenir. La plupart des personnes interprètent de manière personnelle la ressemblance de certains symboles et chiffres avec les lettres. Par exemple, essayez de remplacer le « A » par le « @ », le « l » par le « ! », le « O » par le zéro (0), le « S » par le « $ » et le « E » par le « 3 ». Pour vous, ces remplacements (« @llis0nbe@ute », « A!!isonB3aute » et « A//i$onBeaute ») sont faciles à reconnaître, mais ils sont extrêmement difficiles à deviner ou à décrypter par quelqu'un d'autre. Observez les symboles de votre clavier et pensez au premier caractère qui vous vient à l'esprit. Ce n'est pas forcément celui auquel une autre personne pense, mais vous, vous vous en souviendrez. Utilisez désormais certains des symboles comme valeurs de remplacement.

2 CHOISISSEZ DES ÉVÉNEMENTS OU DES PERSONNES AUXQUELS VOUS PENSEZ

Pour retenir un mot de passe fort qui doit changer sur plusieurs mois, essayez de sélectionner un événement personnel ou public à venir. Utilisez-le comme une occasion de vous rappeler quelque chose d'agréable dans votre vie, ou une personne que vous admirez ou aimez. Vous n'oublierez certainement pas le mot de passe s'il est drôle ou attachant. Faites-en sorte qu'il soit unique pour vous. Assurez-vous de faire une expression contenant au moins deux mots, et continuez à y insérer vos symboles, exemple : « J0hn$Gr@du@tion ».

3 UTILISEZ LA PHONÉTIQUE DANS LES MOTS

En général, les dictionnaires de mots de passe utilisés par les pirates recherchent des mots incorporés à votre mot de passe. Comme décrit plus haut, n'hésitez pas à utiliser les mots, mais assurez-vous d'y insérer librement des symboles. Une autre façon de déjouer le pirate est d'éviter d'écrire le mot correctement, ou encore d'utiliser une phonétique drôle dont vous pouvez vous souvenir. Par exemple, « Renégocier un contrat » pourrait devenir « RenégOcier1c0ntrat! » ou « Renégocier 1 cOntrat ! ».

4 N'AYEZ PAS PEUR DE CRÉER UN MOT DE PASSE LONG

S'il vous est plus facile de retenir une expression complète, n'hésitez pas à la taper. Les mots de passe plus longs sont beaucoup plus difficiles à décrypter. Et même s'il est long, tant que vous pouvez facilement le retenir, vous aurez probablement beaucoup moins de problèmes pour vous connecter, même si vous n'êtes pas le meilleur dactylo au monde.

5 UTILISEZ LES PREMIÈRES LETTRES D'UNE EXPRESSION

Pour créer un mot de passe fort et facile à retenir, commencez par écrire une phrase correcte en termes de ponctuation et de capitalisation. Exemple : « Ma fille Kay étudie à l'International School. » Ensuite, prenez la première lettre de chaque mot de votre phrase, en conservant les majuscules utilisées dans la phrase. Dans l'exemple ci-dessus, le résultat donne « MfKeaIS ». Enfin, remplacez certaines lettres du mot de passe par des caractères non alphanumériques. Vous pouvez utiliser le signe « @ » pour remplacer le « a » ou le signe « ! » pour remplacer le « L ». Après ce remplacement, l'exemple de mot de passe ci- dessus pourrait être « MfKea!S ». C'est un mot de passe très difficile à décoder, mais facile à retenir, tant que vous pouvez vous souvenir de la phrase sur laquelle il se fonde.

6 RECOMMANDATIONS :

6.1 Combinez des lettres, des symboles et des nombres faciles à retenir pour vous, mais difficiles à deviner pour les autres.

6.2 Créez des mots de passe prononçables (même si ce ne sont pas des mots) et faciles à retenir, afin de réduire la tentation de les noter.

6.3 Essayez d'utiliser les premières lettres d'une expression qui vous plaît, surtout si elle contient un chiffre ou un caractère spécial.

6.4 Prenez deux noms de choses qui vous sont familières, puis entourez-les d'un chiffre ou d'un caractère spécial. Vous pouvez également modifier l'orthographe pour intégrer un caractère spécial. Ainsi, le résultat est inhabituel, ce qui en fait un bon mot de passe parce que vous seul pouvez vous en souvenir rapidement, alors que les autres peineront pour le décrypter.

EX

« Téléphone + 4 + vous » = « Telephone4vous » ou « Tel4v0u »
« chat + * + Souris » = « chat*Souris » ou « chat*$ouris »
« attaque + 3 + livres » = « attaque3livres » ou « @taque3livrEs »