COLLÈGE Dawson

No. IST-04

Titre:	**POLITIQUE DES COMPTES**
CLASSIFICATION:	TECHNOLOGIES ET SYSTÈMES D'INFORMATION
ADOPTION INITIALE	Le 12 mai 2016
MODIFIÉE :	

Cette politique a été adoptée en anglais. En cas de divergence la version anglaise prévaut sur la version française.

1. Champ d'application

Cette Politique s'applique aux employés ayant un accès privilégié aux comptes, aux systèmes ou aux informations contenues dans les systèmes, ainsi qu'à ceux qui mettent en œuvre, déploient ou gèrent les systèmes.

2. Définitions

i. *Compte générique.* Un compte qui n'est pas lié à une personne spécifique par le biais d'un numéro d'employé ou d'une adresse électronique. Notez que le nom d'utilisateur lui-même ne suffit pas à identifier une personne. Par exemple, jsmith sans aucune autre information est générique, mais jsmith avec le numéro d'employé 12345, ou l'adresse électronique externe jsmith@yahoo.com n'est pas générique.

ii. *Compte partagé.* Un compte conçu pour être partagé entre divers utilisateurs. Par définition, il s'agit également d'un compte générique.

iii. *Compte invité.* Un compte qui n'est ni celui d'un employé ni celui d'un étudiant du Collège. Cela inclut les consultants, les membres externes des groupes de travail et des comités du Collège, les visiteurs lors des événements, etc.

iv. *Compte privilégié.* Compte donnant accès à des données sensibles, par exemple pour les gestionnaires aux financer, les superutilisateurs internes, les administrateurs de système, les éditeurs de sites web, les partenaires de sous-traitance informatique, etc.

v. *Administrateur de système.* Compte privilégié utilisé pour déployer, configurer ou gérer des systèmes, tel qu'un administrateur de système, un administrateur de base de données, etc.

vi. *Développeur d'applications.* Utilisateur qui développe une application à l'aide d'un langage de programmation tel que PHP, que d'autres personnes utiliseront, directement ou indirectement.

vii. *Super utilisateur.* Un utilisateur qui peut changer d'identité, par exemple un employé qui peut se connecter à un système comme s'il était un autre utilisateur, sans utiliser les informations d'identification de cet autre utilisateur.

3. Création des comptes

Les comptes invités ont une date d'expiration d'un an ou à la date d'achèvement de l'activité, selon ce qui se produit en premier.

Les comptes génériques doivent être autorisés par le Directeur des Technologies et des Systèmes d'Information ; ils ne sont accordés que lorsqu'il n'y a pas d'autres alternatives. En particulier, ils ne constituent pas une solution appropriée pour le simple partage de fichiers ou de courriers électroniques, ou dans la plupart des situations de services en vente libre.

Les comptes privilégiés doivent être autorisés par le Directeur des Technologies et des Systèmes d'Information. En outre, les comptes privilégiés donnant accès à des données sensibles doivent être autorisés par le Directeur ou le délégué responsable de l'information.

4. Exigences pour les administrateurs de système

Les systèmes doivent être configurés de manière à exiger une authentification pour la connexion, même pour les dispositifs mobiles (un code PIN ou une empreinte digitale peuvent être appropriés). Des exceptions sont accordées pour les dispositifs spécialisés tels que les kiosques d'accès public lorsque ces dispositifs sont configurés avec des comptes d'utilisateurs publics disposant d'autorisations extrêmement restreintes (par exemple, uniquement pour le web).

Les administrateurs de systèmes doivent renforcer leurs systèmes afin d'empêcher le piratage des mots de passe en utilisant des méthodes raisonnables pour atténuer les attaques par force brute des mots de passe, comme le verrouillage d'un compte pendant quelques minutes après plusieurs tentatives de connexion infructueuses.

Des mesures pratiques doivent être mises en place pour enregistrer les tentatives de connexion réussies et échouées. Les administrateurs du système ne doivent pas utiliser de mots de passe par défaut pour les comptes administratifs.

Les administrateurs de système réinitialisent les mots de passe des comptes d'utilisateurs ou demandent aux utilisateurs de réinitialiser leurs propres mots de passe lorsqu'ils ont pris connaissance d'un risque de sécurité lié au compte.

5. Exigences pour les développeurs d'applications

Les développeurs d'applications doivent, dans la mesure du possible, développer des applications qui requièrent des protocoles sécurisés pour l'authentification et la communication.

Les applications qui mettent en œuvre l'authentification doivent permettre des rôles ou la délégation de tâches, donnant ainsi la possibilité à un employé de prendre en charge les fonctions d'un autre employé sans avoir à connaître son mot de passe.

Dans la mesure du possible, les systèmes internes disponibles en dehors du réseau du Collège doivent utiliser l'authentification par jeton. Si des mots de passe sont nécessaires, ils ne seront pas stockés en texte clair ou sous une forme facilement réversible.

6. Exigences relatives aux comptes à privilèges

Les comptes privilégiés ne peuvent pas être génériques et leur utilisation doit suivre les principes du moindre privilège, c'est-à-dire qu'un compte privilégié ne peut pas être utilisé lorsqu'un compte moins privilégié suffit.

Les actions effectuées par ces comptes font l'objet d'un contrôle quotidien supplémentaire.