RECTORAT DE BORDEAUX
Secrétariat Général
Sécurité des Systèmes d'Information

Bordeaux, le lundi 16 octobre 2006.

Affaire suivie par : RSSI
rssi@ac-bordeaux.fr

RECOMMANDATION DE SECURITE

Objet : Politique d'habilitation des droits d'accès et de la gestion des mots de passe.

Gestion du document :

Référence	SG-SSI-2006-REC-05
Date 1ere version	16/10/2006
Destinataires cibles	Tous les utilisateurs d'applications informatiques de l'académie
Destinataires pour information	
Sources	Schéma Directeur SSI du MENESR
Pièces jointes	
Niveau de confidentialité	NC : non classifié.

Sommaire

Introduction et principes

➢ La plus part des accès à nos informations se fait par l'intermédiaire d'application informatique. La sécurité est en général assurée par l'emploi d'un couple "**compte d'accès - mot de passe**".

- Le "compte d'accès" permet d'identifier la personne (on parle aussi "d'identifiant" ou de "login"). Ce compte d'accès attribué individuellement à chaque utilisateur est associé à un profil d'autorisation.
- Le "mot de passe" permet d'authentifier qu'il s'agit bien d'une connexion effectuée par une personne dûment autorisée (on parle aussi de code d'accès ou de code secret).

➢ Le couple « identifiant – mot de passe » peut être remplacé par un dispositif technique généralement appelé « **passeport électronique** ». Contrairement à l'authentification classique basée sur la connaissance d'un code confidentiel, le passeport électronique est basé sur une signature et un certificat électroniques. L'emploi de cette technologie permet d'obtenir un accès plus sûr, on parle alors **d'authentification forte**.

➢ Notion d'identifiant **fonctionnel ou personnel** :

- Le dispositif de sécurité d'accès peut être spécifique à l'application informatique, on parle alors d'identifiant fonctionnel. Il associé un profil caractérisé par des droits à un compte d'accès confié à une personne. Du point de vue de l'utilisateur, ce procédé présente l'inconvénient majeur de lui confier autant de compte d'accès que d'application informatique qu'il doit utiliser. Par contre, en cas de besoin (par exemple pour assurer une suppléance), rien n'empêche un utilisateur (s'il en a l'autorité) de confier son compte d'accès à une tierce personne.
- Pour répondre à la contrainte de plus en plus lourde de la multiplication des comptes fonctionnels, l'idée est d'associer à une personne physique le profil lui correspondant pour toutes les applications informatiques. Le compte d'accès devient donc nominatif. L'utilisateur devra présenter son identifiant personnel et unique. Par contre, il ne lui sera plus possible de le confier à une tierce personne dans le cas d'une suppléance.

Recommandations sur les habilitations

Le principe général de la gestion des droits d'accès à une application informatique comprend 2 phases :

- La définition par la maîtrise d'ouvrage des différents niveaux d'accès et de droits associés aux informations (droits en lecture, en modifications, ...). Cela se traduit par la notion de profils types.
- L'attribution par le responsable du traitement d'un profil à une ou plusieurs personnes.

➢ Voici les consignes principales de sécurité sur la gestion des profils et des attributions :
- les comptes génériques ou partagés sont strictement prohibés ;
- la gestion des droits doit être rigoureuse, une gestion laxiste entraîne des failles de sécurité ne pouvant être compensé par le l'authentification;
- le rattachement d'une personne à des profils doit être mis à jour à chaque changement de ces fonctions;
- un contrôle périodique doit être réalisé à l'initiative du responsable des informations (et non pas du responsable informatique).

➢ S'agissant des comptes "administrateurs" de systèmes informatiques, les règles supplémentaires doivent être respectées :
- l'accès aux outils d'exploitation (notamment la gestion des droits, les sauvegardes, les traces) doit être limités et contrôlés ;
- la création systématique de journaux des actions d'administration doit être effectuée;
- la gestion des droits doit s'accompagner d'une gestion de délégation afin que chaque responsable d'une mission puisse déléguer vers ses collaborateurs les autorisations nécessaires.

Recommandations sur les mots de passe

La sécurité de l'accès s'appuie sur la robustesse du mot de passe et sur notre capacité à le garder secret.

➢ Tous les utilisateurs doivent pour cela respecter les consignes suivantes :
- le mot de passe doit être renouvelé au minimum tous les 6 mois;
- il doit comporter au moins 7 caractères formant une combinaison de caractères spéciaux et de lettres alphanumériques;
- s'il est conservé sur un support numérique, le fichier doit être chiffré;
- il ne doit pas être facilement accessible à proximité du poste de travail;
- il est interdit de pré enregistrer des procédures de connexion comportant le mot de passe (pourtant parfois proposé par les écrans de connexions).

Importance du vocabulaire : il est préférable de parler de "code secret" ou "code personnel" ou encore "code confidentiel" plutôt que de "mot de passe". Nous communiquons en effet moins facilement un "secret" ou une information "personnelle".

Suivi du document

Date	Modifications ou commentaires
9/10/2006	MB - Version initiale

Tous les bulletins sur http://ssi.ac-bordeaux.fr