# ADMINISTRATION

## Gestion des droits d'accès | ADMI01

**Contexte :**

Accès aux ressources de l'entreprise à travers le réseau local.

**Objectifs :**

Protéger les données des indiscrétions (fuite d'information), des maladresses, de la fraude ou du sabotage, et contrôler les accès aux ressources du système d'information.

**Recommandations :**

Chaque utilisateur doit disposer d'un droit d'accès (ou « compte ») personnel et unique à son environnement de travail, lequel comprend :

- les logiciels et les données, dédiées ou partagées ;
- les outils de communication (messagerie, Internet, Intranet).

L'utilisateur est donc le plus fréquemment identifié par un nom de connexion ou « login » et authentifié par un mot de passe. La forme de ce mot de passe peut faire l'objet de différentes recommandations :

- être unique, à un instant donné ;
- contenir au moins huit caractères alphabétiques et numériques ;
- être inconnu des dictionnaires ;
- être changé périodiquement ;
- ne permettre sa réutilisation qu'après au moins 5 changements consécutifs ;

En cas de tentatives d'accès infructueuses, le compte utilisateur doit faire l'objet d'un blocage temporaire ou permanent, suivant la politique de l'entreprise.
L'utilisateur pourra aussi être authentifié de façon plus forte par les dispositifs cités dans la fiche LOGI01.

L'affectation des droits des utilisateurs sur les ressources implique tout d'abord de choisir entre les différents modèles de gestion des droits, dont les plus connus sont :

- DAC « Discretionary Access Control » qui se traduit par « rien n'est autorisé, sauf ce qui est discrétionnairement et explicitement permis par le propriétaire du fichier ou de l'objet » ;
- MAC « Mandatory Access Control » où l'utilisateur est autorisé à accéder à une ressource si son niveau d'habilitation est supérieur ou égal au niveau de classification (et donc de sensibilité) de celle-ci;
- Enfin, RBAC ("Role-Based Access Control"), le plus récent, basé sur la notion de rôles auxquels sont attachés des droits prédéfinis ; dans la pratique, ces rôles correspondent aux différentes fonctions.

Les règles de gestion doivent être bien définies, en veillant à ne pas affecter plus de droits que nécessaire aux utilisateurs. On s'assurera de la cohérence de ces droits, par exemple entre différentes applications utilisant la même base de données. Les procédures d'affectations doivent être mises à jour en permanence en fonction des entrées/sorties du personnel
Des dérogations à ces droits peuvent être accordés pour des besoins ponctuels, mais doivent être limités dans le temps.
Les droits des utilisateurs peuvent se résumer à :

- aucun accès ;
- accès en lecture ;
- accès en lecture et écriture ;
- accès réservé à l'administration.

L'affectation de ces droits sur les différents objets ou ressources du système d'information doit être formalisée en utilisant les outils adéquats (tableaux, outils des SGBD, etc.)

**Remarque :**
Pensez à conserver en lieu sûr, sous enveloppe scellée, le « login » et le mot de passe de l'administrateur.