|  |  |  |
| --- | --- | --- |
| logo | Engagement des règles sécurité | 1028 |

Responsable :

Mis à jour :

Voir aussi les politiques Sécurité de l’information, Contrôle d’accès, Droits d’accès et Bureau propre et écran vide.

**Règles de sécurité à respecter :**

* respecter la réglementation
* se conformer aux dispositifs mis en place pour lutter contre les virus et les attaques informatiques
* ne pas divulguer son mot de passe et toute autre information confidentielle
* avertir le département informatique de tout dysfonctionnement ou anomalie suspecte y compris la divulgation non autorisée d’une information confidentielle
* ne pas accéder ou de tenter d'accéder à des ressources spéciales du système d'information, sans autorisation explicite
* ne pas se connecter aux réseaux externes, sans autorisation explicite
* ne pas installer, télécharger ou utiliser des logiciels ou progiciels dont les droits de licence n’ont pas été payés
* respecter les droits de la propriété intellectuelle
* respecter les conditions d’utilisation autorisée de l’information confidentielle
* utiliser les ressources d'une manière raisonnable (Internet et messagerie)
* assumer son identité (ne pas se faire passer pour quelqu’un d’autre)
* ne pas démanteler les équipements sans autorisation appropriée
* ne pas violer la vie privée des personnes sans autorité appropriée

Ne jamais oublier que ne pas respecter son engagement de suivre scrupuleusement les règles de sécurité de l’information peut amener à des sanctions disciplinaires.

Une information confidentielle est celle qui est dévoilée aux seules personnes autorisées.

La durée de cet engagement prend fin à la rupture du contrat.

Prénom, nom :

Signature :

Date :