|  |  |  |
| --- | --- | --- |
| logo | Plan d’augmentation de la sensibilité | 1013 |

Responsable :

Mis à jour :

Le programme de sensibilisation en matière de protection des données à caractère personnel fait partie de la politique Protection de la vie privée.

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée nécessaires pour respecter le [RGPD](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679) (Règlement général sur la protection des données) avec des actions suivantes :

* sensibiliser les utilisateurs travaillant avec des données à caractère personnel aux risques liés aux libertés et à la vie privée
* les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement, cf. le processus Appliquer la discipline
* toute action sur un traitement de données à caractère personnel (opérations d’administration ou de la simple utilisation d’une application) est expliquée dans un langage clair
* rédiger une charte informatique et lui donner une force contraignante (par exemple annexion au règlement intérieur)

Exemple de points d’une charte informatique (à adapter à votre organisation) :

* rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci (règlement RGPD)
* domaine d’application :
  + les modalités d’intervention des équipes chargées de la gestion des ressources informatiques de l’organisation
  + les moyens d’authentification utilisés
  + les règles de sécurité auxquelles les utilisateurs doivent se conformer :
    - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique
    - ne jamais confier son identifiant/mot de passe à un tiers
    - ne pas installer, copier, modifier, détruire des logiciels sans autorisation
    - verrouiller son ordinateur dès que l’on quitte son poste de travail
    - ne pas accéder, tenter d’accéder, ou supprimer des informations si cela ne relève pas des tâches directes de l’utilisateur
    - respecter consignes des opérations de copie de données sur des supports amovibles (en obtenant l’accord préalable du supérieur hiérarchique et en respectant les règles de sécurité)
* les modalités d’utilisation des moyens informatiques et de télécommunications mis à disposition comme :
  + le poste de travail
  + les équipements nomades (notamment dans le cadre du télétravail)
  + les espaces de stockage individuel
  + les réseaux locaux
  + les conditions d’utilisation des dispositifs personnels
  + l’Internet
  + la messagerie électronique
  + la téléphonie
* les conditions d’administration du système d’information :
  + systèmes automatiques de filtrage
  + systèmes automatiques de traçabilité
  + gestion du poste de travail
* les responsabilités et sanctions encourues en cas de non-respect de la charte

Nommer la personne responsable du plan d’augmentation de la sensibilité (par défaut c’est le RSI, responsable sécurité de l’information). Cibler le public à sensibiliser et éventuellement créer des groupes.

Exemple d’un plan d’augmentation de la sensibilité :

|  |  |
| --- | --- |
| Formation | Sensibilisation |
| * problèmes de sécurité potentiels * ensemble de règles faciles à comprendre (et à suivre) pour réduire le risque de problèmes éventuels | permettre au personnel de mieux comprendre :   * les risques de sécurité * l'importance de la sécurité pour les activités quotidiennes |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Expliquer :

* ce que le plan doit accomplir
* combien la protection des actifs d'information est réellement vitale pour l’organisation
* pourquoi « la sécurité est la responsabilité de chacun » et non seulement du département informatique
* comment une personne sans formation pourrait facilement sans le vouloir mettre en danger des informations sensibles