# SECURITE ET BONNES PRATIQUES INFORMATIQUES
# FORMATION DES UTILISATEURS

**1 jour – 07h00**

### *Public visé*

*Toute personne qui souhaite être sensibilisée à la sécurité informatique*

### *Pré - requis*

*Utilisateurs réguliers des outils informatiques et communicants (téléphone, ordinateur, messagerie, internet...).*

### *Objectifs*

*Lister des situations à risque,*
*Décrire les principales règles d'usage en matière de sécurité informatique*

### *Méthode et moyens pédagogique*

*Formateur informatique spécialiste de la gestion des risques et de la conformité Informatique et libertés*
*Alternance d'apports théoriques et d'exercices pratiques*
*Ces exercices peuvent être modifiés en fonction de la population concernée afin de se rapprocher de l'activité professionnelle des participants*

***Modalités de déroulement** : formation en présentiel ou distanciel – phases d'apprentissage mentionnées au programme*

***Moyens de suivi :** feuille d'émargement signée par demi-journée par le formateur et le(s) stagiaire(s)*

***Modalités de sanction de l'action :** délivrance d'une attestation de formation*

***Moyens d'évaluation :** avant la formation : questionnaire oral et/ou évaluation de positionnement.*
*Après : le formateur évalue les acquis du stagiaire (savoirs et savoir-faire) au moyen de questionnement oral et reformulations des apprenants + exercices de mise en application*

### *Programme*

**DEFINITION DE LA SECURITE INFORMATIQUE**
Panorama de la cyber menace, son contexte, ses enjeux
L'importance de la prise en compte de la sécurité informatique pour les entreprises et organisations
Les réseaux d'entreprise (locaux, distantes, Internet).
Les réseaux sans fil et mobilité
Les applications à risques : Web, messagerie...
La base de données et système de fichiers : menaces et risques

**PRESENTATION DES SITUATIONS A RISQUE**
**Les gestes du quotidien**
Accès internet
Mises à jour
Les réseaux sociaux
**Gestion des mots de passe**
Identifier et savoir créer un mot de passe fort
Apprendre à gérer ses mots de passe
**Détection d'attaques**
Connaître le principe du phishing
Connaître le ransomware
Reconnaître les techniques utilisées par les pirates informatiques
Donner les bonnes pratiques en cas d'attaque
**Déplacements professionnels et nomadisme**
Apprendre à cloisonner le professionnel et le personnel
Créer des sessions différentes pour chaque usage et utilisateur
Se méfier des objets connectés
**Le processus d'authentification**
Les contrôles d'accès : l'authentification et l'autorisation
L'authentification par certificats et par token.
La connexion à distance via Internet.
Qu'est-ce qu'un VPN ?
Pourquoi utiliser une authentification renforcée

**SENSIBILISATION RGPD**

### *Moyens techniques mis à disposition*

*Supports d'animation pédagogique utilisés en vidéo-projection.*
*1 PC/stagiaire, connexion Wifi, imprimante multifonctions.*
*Installation dans notre centre de formation : salles de formation équipées de tables, chaises, mur clair pour la projection, paperboard et/ou tableau blanc ou numérique interactif.*
*En cas de formation intra-entreprise, des installations équivalentes doivent être mises à disposition par l'employeur des stagiaires.*