ENGAGEMENT PERSONNEL

Je soussigné(e), ...déclare avoir pris connaissance du présent engagement de responsabilité et m'engage à en respecter le contenu et les règles de sécurité ci-dessous.

1. **Règles de sécurité et bonnes pratiques sur l'usage du système d'information**

   - L'utilisateur doit obligatoirement verrouiller son poste de travail lorsqu'il quitte son bureau (quelques secondes sont suffisantes à un utilisateur mal intentionné pour installer un programme malveillant sur un poste de travail);
   - L'utilisation de matériel personnel est interdite sur le système d'information de la DAP;
   - Le vol ou la perte d'un matériel informatique doit faire l'objet d'un rapport de vol qui doit être adressé au correspondant informatique et au responsable de la sécurité des systèmes d'information;
   - L'usage de matériel sans fil est interdit sur le système d'information (clef USB WiFi, clavier et souris sans fil...);
   - Les logiciels utilisés font obligatoirement l'objet d'une licence détenue par le bureau de des systèmes d'information de la DAP;
   - Les logiciels spécifiques doivent être installés par ce même bureau, l'installation de logiciel de jeux, de démonstration et de copie illicite sont interdites;
   - Afin d'éviter toutes propagations virales, il est de la responsabilité de l'utilisateur, en cas de détection d'un virus par l'antivirus, d'isoler son poste du travail du réseau (déconnexion du câble réseau sur la face arrière du poste) et de prévenir le support informatique et le responsable de la sécurité des systèmes d'information;
   - L'utilisateur est responsable des mots de passe qui lui permettent d'accéder au système d'information et aux applications présentes sur le système d'information. Ces mots de passe ne doivent jamais être divulgués, visibles ou facilement récupérables par autrui et doivent être changés tous les six mois. Ces mot de passe doivent contenir au moins 8 caractères minuscules ou majuscules et inclure des caractères spéciaux (#, !,@....) et des chiffres;
   - Les supports de stockage (disquette, cd-rom, clef USB) contenant des informations confidentielles doivent être enfermés au même titre que les documents papiers ;
   - Il est recommandé de sauvegarder les données professionnelles sur les lecteurs réseaux qui sont mis à disposition de l'utilisateur, afin d'en assurer leurs disponibilités (sauvegarde quotidienne automatique).
   - De façon plus générale, l'utilisateur doit signaler au service informatique référent toutes anomalies sur son poste de travail ;
   - Les ordinateurs portables doivent être équipés d'un câble antivol ou enfermés en lieu sûr lorsqu'ils ne sont pas utilisés ;

2. Règles de sécurité et bonnes pratiques sur l'usage de la messagerie et de la navigation sur internet

- L'utilisateur doit être vigilant sur les liens Internet présents dans les messages, même si l'expéditeur semble être un expéditeur de confiance. En cas de doute, il est conseillé de ne pas cliquer sur ces liens (si nécessaire, il est conseillé de saisir le lien manuellement dans le navigateur) ;
- L'utilisateur ne doit jamais ouvrir un fichier joint (quelle que soit son extension : .doc ou, .ppt ou .xls par exemple) présent dans un message au contenu suspect, même si l'expéditeur semble être de confiance et même si le fichier n'est pas détecté comme malveillant par l'antivirus. Il est important de s'attacher au contenu du message pour s'assurer de l'intégrité d'un message et de la confiance que l'on peut apporter aux pièces jointes ;
- L'utilisateur ne doit jamais répondre aux pourriels (ou « spam » en anglais) c'est-à-dire aux messages publicitaires.
- Toute communication de message à l'intention d'usagers de l'internet comporte, dans l'adresse de l'expéditeur, l'identification du ministère de la Justice (...@justice.gouv.fr ou ...@justice.fr) et peut engager en conséquence la responsabilité de l'administration. Il est donc recommandé à l'utilisateur de s'exprimer avec une extrême prudence (messagerie, listes de discussion, forum...) et de ne pas exprimer d'opinion personnelle en utilisant son adresse de messagerie.
- Afin de ne pas encombrer le réseau du ministère, il est interdit de relayer les chaînes de messagerie. Ex : message de soutien qu'on vous demande de transmettre à 10 personnes de votre connaissance... ;
- Il est de la responsabilité des utilisateurs de rendre confidentielles les informations sensibles envoyées par la messagerie, en les « chiffrant ». l'outil permettant de chiffrer est fourni par le service informatique. Exemples d'informations sensibles : résultat d'un audit, informations nominatives sur une personne détenue, informations topographiques d'un établissement... ;
- Les informations classifiées de défense ne doivent en aucun cas être transmises par messagerie.
- Il ne faut jamais rediriger son adresse professionnelle vers une boîte personnelle ;
- Il est recommandé de supprimer régulièrement les traces de connexion créées par la navigation sur Internet (fichiers temporaires, cookies...) ;
- Il est illusoire de penser que l'on conserve son anonymat lors d'une navigation sur Internet.
- L'utilisateur veille à respecter son devoir de réserve lorsqu'il s'exprime hors de l'institution judiciaire par le biais des nouveaux outils de communication mis à sa disposition.

Fait, en double exemplaire, à ..... le .....

Signature :