Charte Utilisateur @voclé

Version 1.0 du 20 juin 2013

1. INTRODUCTION

1.1. Objet du présent document

La présente charte a pour objectif de préciser les règles d'utilisation des ressources mise à la disposition à travers le SI @voclé.

Elle présente les règles liées à la politique de sécurité @voclé que les utilisateurs sont tenus de respecter dans l'exercice de leur fonction.

1.2. Champs d'application

La présente charte s'adresse à toute personne disposant d'un accès à des ressources du S.I @voclé.

2. DISPOSITIONS GENERALES

2.1. Accès au Système d'Information (SI) @voclé

a) L'accès est nominatif, soumis à l'autorisation et ne doit jamais être partagé. L'utilisateur ne doit en aucun cas faire usage des moyens d'authentification ou des habilitations d'une tierce personne.
b) Toute action effectuée par l'utilisateur, à l'aide de son identifiant est imputable et engage sa responsabilité.
c) L'utilisateur est entièrement responsable de la protection des moyens d'authentification mis à sa disposition (mots de passe, clé d'authentification, etc.), Ces moyens d'authentification ne doivent jamais être partagés, transmis ou communiqués à d'autres personnes.
d) L'utilisateur est tenu en général de ne pas laisser les médias d'authentification mis à sa disposition sans surveillance dans des lieux dont l'accès n'est pas contrôlé, et de faire preuve d'une vigilance particulière dans les lieux publics et les transports en commun.
e) Les mots de passes utilisés pour les activités professionnelles au sein du SI @voclé, ne doivent jamais être utilisés pour d'autres fonctions (sites Internet, réseau domestique). Ces mots de passe ne doivent jamais être affichés, imprimés, stockés sans protection.

2.2. Contrôle de l'usage

a) L'utilisateur ne doit jamais tenter de contourner les mécanismes de protection mis à sa disposition à travers le SI @voclé.
b) Il est interdit de tenter de tester ou d'exploiter, à des fins de démonstration ou de vérification, une faille suspectée. Seul le personnel dûment habilité des équipes chargées du contrôle de la sécurité est autorisé à réaliser de telles actions.

c) L'ODA se réserve le droit de bloquer toute connexion et de désactiver tous crédentiels pouvant constituer une menace à la disponibilité, à l'intégrité ou à la confidentialité du SI @voclé.
d) En particulier l'utilisateur doit être vigilant quant à la confidentialité des informations auxquelles il accède dans des lieux publics via les ressources mises à sa disposition.

3. TRAITEMENT D'INCIDENT

a. L'utilisateur est tenu d'avertir immédiatement son responsable hiérarchique et le HelpDesk en cas :
   - D'anomalie ou de dysfonctionnement des applications @voclé.
   - De la compromission ou de la divulgation du mot de passe utilisateur.
   - De la perte ou du vol de ses moyens d'authentification.

b. En particulier et en cas de perte ou de vol il est nécessaire d'effectuer les actions suivantes :
   - Informer immédiatement le HelpDesk.
   - Faire une déclaration auprès du commissariat ou de la gendarmerie.

4. DISPOSITIFS DE CONTROLE APPLIQUES

Dans l'objectif de garantir le bon fonctionnement et la sécurité de son Système d'Information et de préserver ses intérêts, l'ODA se réserve le droit d'analyser, de limiter et de contrôler les accès et échanges effectués via ses Systèmes d'Information, quels que soient leur nature ou leur objet.

Ces contrôles sont réalisés, dans le respect de la législation en vigueur et des directives de la CNIL, exclusivement sous la responsabilité des équipes informatiques spécifiques afin de préserver la confidentialité des informations qui pourraient être connues à cette occasion.

Il est utile de rappeler que les équipes informatiques spécifiques sont soumises à une charte de déontologie prévoyant notamment le respect de la confidentialité des données personnelles qui seraient portées à leurs connaissances.

Il est à noter que les entités informatiques spécifiques sont également amenées à réaliser, dans l'anonymat, des tests destinés à vérifier l'application des procédures de sécurité et la robustesse des infrastructures,

Conformément aux directives de la CNIL, le détail des informations enregistrées concernant les accès et les échanges utilisateur sont décrites ci-dessous.

a. Les informations pouvant être enregistrées, pour chaque connexion aux Systèmes d'Information @voclé depuis l'extérieur (accès VPN, etc.) sont :

   - Date et heure de début et de fin de connexion.
   - Applications consultées.
   - L'identifiant utilisé par la connexion ainsi que l'identifiant du délégué si l'accès est effectué dans le cadre d'une délégation.

b. Les informations pouvant être enregistrées au niveau des applications soumises à des contrôles d'accès sont :
   - Identification de l'utilisateur et de son délégué en cas d'accès dans le cadre d'une délégation.
   - La liste des actions réalisées.
   - Date et heure de la connexion.

La durée de conservation de données est de :

- 12 mois pour les informations concernant les connexions depuis l'extérieur.
- 12 mois pour les informations concernant l'application soumise à des contrôles d'accès.

5. RESPECT DE LA LEGISLATION ET DE LA PRESENTE CHARTE

En cas de non-respect de la législation en vigueur et des dispositions de la présente charte, l'utilisateur sera tenu pour responsable de ses actes et pourra encourir les sanctions prévues dans le Règlement Intérieur de l'ODA ainsi que toute autre sanction civile ou pénale prévue par la loi.

Par ailleurs, l'utilisateur engage pleinement sa responsabilité en cas d'infraction ou de complicité d'infraction à la législation ou à la réglementation en vigueur.

Les principales dispositions légales en vigueur prévues par la législation française dans le domaine de la sécurité des Systèmes d'Information sont notamment les suivantes :

- la loi n° 78-17 du 06/01/78 dite « informatique et liberté », modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
- la législation relative à la fraude informatique (articles 323-1 à 323-7 du Code pénal).
- la législation relative à la propriété intellectuelle.
- la loi du 04/08/94 relative à l'emploi de la langue française.
- la législation applicable en matière de cryptologie.
- L'article 226-15 du Code Pénal relatif à la violation du secret des correspondances.
- la législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du Code pénal et loi du 29 juillet 1881).
- Réglementations et directives de la Commission nationale de l'informatique et des libertés (C.N.I.L).