

# CHARTRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

<b>Accessibilité</b>		Accès non restreint	
<b>Destinataires</b>		Usagers du CRIANN	
	<b>Responsable</b>	<b>Entité</b>	<b>Date</b>
<b>Rédaction</b>	PW/AB/HP	INSAR / CRIANN	01/02/2016
<b>Vérification</b>	Direction	CRIANN	11/05/2016
<b>Validation</b>	AG	CRIANN	27/05/2016
<b>Historique des mises à jour</b>			
<b>Date</b>	<b>Auteur</b>	<b>Changement</b>	<b>Version</b>

## 1 DOMAINE D'APPLICATION

La présente charte s'applique à l'ensemble des utilisateurs qui ont accès aux Systèmes d'Information du CRIANN (voir paragraphe 3.1).

## 2 OBJET

La présente charte a pour objet d'informer les utilisateurs de leurs droits et de leurs responsabilités, dans le cadre de l'usage des ressources informatiques et des services numériques du Centre Régional et d'Applications de Normandie (CRIANN), en application de sa politique de sécurité des Systèmes d'Information et de la législation.

Elle définit les règles d'usage et de sécurité que le CRIANN et ses utilisateurs doivent respecter et précise les droits et les devoirs de chacun.

Elle répond à la préoccupation du CRIANN de protéger ses systèmes d'informations contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. En effet, tout manquement aux règles qui régissent la sécurité des systèmes d'information est susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique de l'établissement).

## 3 DÉFINITIONS

### 3.1 Système d'Information

Le terme « Système d'Information » (SI) désigne un ensemble organisé de ressources (personnel, matériels, logiciels, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information dans un environnement donné.

### 3.2 Utilisateur

Le terme « Utilisateur » recouvre toute personne, ayant accès aux ressources des systèmes d'information du CRIANN. Il s'agit notamment :

- du personnel du CRIANN ;
- de toute personne agissant dans le cadre d'une convention, d'un contrat ou d'une relation de partenariat, contractualisé ou non avec le CRIANN.

### 3.3 CRIANN

Pour gérer ses systèmes d'information, le CRIANN s'appuie sur une équipe technique qui gère les moyens informatiques (réseau et serveurs, bases de données, etc.) sur lesquelles reposent ses différents services numériques. Cette équipe est également en charge de la sécurité physique et logique de l'infrastructure (sécurité des accès, des données et des échanges).

## 4 CONDITIONS D'UTILISATION DES SYSTÈMES D'INFORMATION DU CRIANN

### 4.1 Autorisation d'accès

Toute utilisation d'un SI est soumise à une autorisation d'usage personnelle, temporaire et incessible, accordée par le Directeur du CRIANN.

Cette autorisation est matérialisée par des identifiants (typiquement un couple formé d'un "login" et d'un mot de passe). L'Utilisateur est responsable de toute utilisation faite à partir de ses identifiants. Il lui appartient de veiller au choix, à la qualité et à la confidentialité de son mot de passe.

### 4.2 Finalité d'utilisation

L'utilisation des ressources informatiques est limitée aux missions du CRIANN et aux besoins de l'activité qui en découle.

### 4.3 Utilisation résiduelle à titre privé

Toutefois, une utilisation résiduelle à titre privé est tolérée. Elle doit rester non lucrative et raisonnable, tant dans sa fréquence que dans sa durée, afin de ne pas nuire à la qualité du travail ou au bon fonctionnement du CRIANN.

Les données privées et leurs traitements associés ne doivent pas occasionner de surcoût notable pour le CRIANN. A ce titre, leur volume doit rester raisonnable et les sauvegardes restent à la charge de l'Utilisateur.

### 4.4 Caractère des données

Toute information stockée ou tout message échangé est réputé professionnel.

L'Utilisateur peut conserver des données privées dans un dossier intitulé « Privé » situé dans son espace personnel de stockage.

L'Utilisateur peut recevoir et envoyer des messages à titre privé. Pour être considérés comme tels, ils doivent comporter la mention « [Privé] » dans leur sujet.

### 4.5 Utilisations prohibées

L'Utilisateur respecte les règles d'éthique professionnelle et de déontologie.

Conformément à la loi, la diffusion d'idéologies politiques ou religieuses, ou qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée de personnes physiques sont interdites.

En outre, l'Utilisateur s'engage à ne pas porter atteinte à la réputation ou à l'image du CRIANN.

## 5 OBLIGATIONS DE L'UTILISATEUR

L'Utilisateur contribue à son niveau à la sécurité des systèmes d'Information. Il s'engage notamment à :

- respecter les lois et règlements en vigueur ;
- respecter la présente charte ainsi que les celles dont le CRIANN est signataire pour l'accès à certains services (par exemple la charte RENATER) ;
- être courtois et poli lors de l'utilisation des ressources informatiques du CRIANN ;
- respecter les matériels, logiciels et locaux mis à leur disposition ;
- faire une utilisation non-abusive des moyens informatiques auxquels ils ont accès ;
- respecter les mesures de sécurité mises en place par les responsables informatiques ;
- se conformer aux décisions des responsables informatiques ;
- ne pas utiliser ou tenter d'utiliser le compte d'un tiers ;
- veiller à la confidentialité des codes, mots de passe ou tout autre dispositif de contrôle d'accès qui leur sont confiés ;
- signaler sans délai tout dysfonctionnement ou incident de sécurité potentiel ;
- veiller à ce que les données confidentielles ne soient pas accessibles à des tiers non autorisés ;
- respecter l'obligation de réserve et de confidentialité à l'égard des informations et des documents auxquels il accède ;
- respecter le droit d'auteur et les licences d'utilisation.

## 6 OBLIGATIONS DU CRIANN

Le CRIANN s'engage à :

- respecter les lois et règlements en vigueur ;
- assurer le fonctionnement et la disponibilité des services numériques ;
- maintenir la qualité du service fourni dans la limite des moyens alloués ;
- informer les usagers des règles et les bons usages tels qu'ils sont définis dans la présente charte et dans les politiques annexes ;
- veiller à respecter la confidentialité des correspondances électroniques et des fichiers auxquels son personnel a accès dans le cadre de leur activité ;
- veiller à la bonne utilisation des Systèmes d'Information, notamment :
  - en prenant toute mesure nécessaire pour assurer ou préserver le bon fonctionnement et/ou la disponibilité nominale des moyens informatiques et service numérique dont il a la charge ;
  - en conservant temporairement des journaux ("logs) sur l'activité du réseau et des systèmes, qui font par ailleurs l'objet d'une surveillance automatisée ;
- assurer la sécurité des ressources exploités par son personnel ;
- favoriser l'instauration d'une « culture sécurité ».

## 7 RESPECT DE LA LÉGISLATION CONCERNANT LES DONNÉES NOMINATIVES

Toute constitution de données nominatives, à l'aide des moyens informatiques, doit faire l'objet, préalablement à leur mise en œuvre, d'une déclaration ou d'une demande d'avis auprès de la Commission nationale informatique et libertés (CNIL). Les données à caractère personnel ne sont conservées que dans la limite des délais prévus par les textes applicables.

Le CRIANN est garant du respect de la loi "Informatique et Liberté" et à ce titre prépare les documents de déclaration ou de demande d'avis préalablement à la mise en œuvre en traitements automatisés d'informations nominatives. Les déclarations et demandes d'avis sont signées et adressées à la CNIL par la direction.

Si, dans l'accomplissement de son travail, l'Utilisateur est amené à constituer des fichiers tombant sous le coup de la loi "Informatique et Liberté", il doit auparavant en avoir demandé l'autorisation au CRIANN et doit lui fournir tous les éléments nécessaires pour l'élaboration des documents de demande d'avis à la CNIL.

Par ailleurs, conformément aux dispositions de cette loi, chaque Utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du SI.

Ce droit s'exerce auprès du Directeur du CRIANN.

## 8 CESSATION DU STATUT D'UTILISATEUR

En référence à l'article 4.1 du présent document, les autorisations d'accès aux Systèmes d'Information du CRIANN seront révoquées s'il y a changement de statut de l'Utilisateur (départ, changement de fonction, etc.).

En cas de changement de statut, l'Utilisateur doit impérativement prévenir le CRIANN. L'Utilisateur sera alors notifié des conséquences opérationnelles, notamment sur pour ce qui concerne fonctionnement du service de courrier électronique et de l'accès à ses données.

Le changement de statut de l'Utilisateur pourra conduire à la suppression complète de ses accès à certains services numériques du CRIANN.

## 9 SANCTIONS

Sans préjuger d'éventuelles poursuites par le CRIANN ou par les parties lésées, en cas de non-respect de ses obligations, l'Utilisateur peut se voir appliquer les sanctions suivantes :

### 9.1 Mesures d'urgence

Le CRIANN peut, en cas d'urgence, prendre toute mesure pour stopper la perturbation de ses services informatiques. Par exemple :

- déconnecter un Utilisateur, avec ou sans préavis selon la gravité de la situation ;
- isoler ou neutraliser toute donnée qui mettrait en péril les moyens informatiques ou qui est en contradiction avec cette charte.

## 9.2 Mesures donnant lieu à information

En cas de non-respect de cette charte, le CRIANN :

- prend contact avec l'Utilisateur et/ou son responsable hiérarchique ;
- peut limiter ou retirer ses codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes.

## 9.3 Mesures disciplinaires

L'Utilisateur qui enfreint une des règles énoncées dans la présente charte encourt des sanctions disciplinaires et/ou judiciaires.

\_\_\_\_\_  
Nom, prénom

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature