




# EXCELLIA Solutions

## Charte de sécurité de l'information

Pour les utilisateurs


CH.SMSI.01

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 2 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	<b>Date :29/10/2024</b>

## 1.Conditions générales d'utilisation des actifs informationnels

Les conditions générales d'utilisation des actifs informationnels de EXCELLIA, présentées ci-dessous, doivent être respectées :

- 1) Les actifs informationnels matériels (postes de travail, imprimantes, etc.) et logiciels (applications, progiciels, systèmes d'exploitation, bases de données, etc.) de EXCELLIA sont strictement réservés aux seuls besoins de l'activité de EXCELLIA et ne devraient jamais être utilisés à des fins personnelles.
- 2) L'accès au SI de EXCELLIA est soumis à une habilitation préalable, après autorisation du responsable hiérarchique.
- 3) L'accès au SI de EXCELLIA est arbitré par les trois principes de sécurité suivants :
  - a. **Besoin d'en connaître** : principe selon lequel l'accès à l'information est limité aux personnes qui en ont besoin pour le bon déroulement des tâches qui leur ont été officiellement affectées.
  - b. **Besoin d'utiliser** : principe selon lequel l'accès aux moyens de traitement de l'information (matériel informatique, applications, procédures, salles) est contrôlé et n'est attribué que pour la réalisation des tâches affectées à l'utilisateur.
  - a. **Moindre privilège** : principe selon lequel l'accès à l'information et aux moyens de traitement de l'information n'est donné qu'avec les privilèges minimums nécessaires à la réalisation des tâches officiellement affectées à l'utilisateur.
- 4) L'utilisateur ne doit pas mettre en péril, de manière volontaire ou par négligence, la **confidentialité**, l'**intégrité** ou la **disponibilité** du SI de EXCELLIA.
- 5) L'utilisateur ne doit pas contourner, de manière volontaire ou par négligence, les dispositifs et les mesures de sécurité mises en œuvre par EXCELLIA.
- 6) L'utilisateur doit informer sa hiérarchie et le RSSI de tout incident ou anomalie de **sécurité** constaté(e), dès sa détection (les modalités de signalement des incidents de sécurité sont décrites au niveau **de la procédure de gestion des incidents**).

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 3 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	<b>Date :29/10/2024</b>


## 2.Règles de sécurité

### 2.1. Engagements de confidentialité

- 1) Les niveaux retenus par EXCELLIA pour la classification de la confidentialité de l'information sont :
  - a. **Public** : Données qui peuvent circuler librement à l'extérieur de EXCELLIA.
  - b. **Interne** : Données qui peuvent circuler librement à l'intérieur de EXCELLIA et n'est accessible qu'au personnel de EXCELLIA et / ou ses partenaires.
  - c. **Confidentiel** : Données qui ne doivent être communiquées qu'aux personnes / entités directement concernées.
  - d. **Restreint** : Données ne doivent être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître et dont la divulgation à des personnes non autorisées pourrait porter atteinte aux intérêts de EXCELLIA.
- 2) L'utilisateur ne doit pas tirer profit personnel des informations auxquelles il a accès au cours de l'exercice de ses fonctions.
- 3) L'utilisateur ne doit pas tenter de lire, modifier, copier ou supprimer des données de EXCELLIA sans une autorisation préalable.
- 4) L'utilisateur ne doit pas tenir des conversations confidentielles dans des locaux publics ou sur des réseaux de communications non sécurisés.
- 5) Toute tentative d'accès non autorisée par un utilisateur expose ce dernier à des mesures disciplinaires (cf. §0).

### 2.2. Gestion des informations secrètes d'authentification


- 1) Les mots de passe des utilisateurs sont personnels et confidentiels. Les utilisateurs ne doivent en aucun cas communiquer ou divulguer leurs mots de passe.
- 2) L'utilisateur est responsable de toutes les activités associées à ses identités numériques (logins, etc.) ;
- 3) L'utilisateur s'engage à ne pas utiliser et ne pas tenter d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 4 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	Date :29/10/2024

- 4) L'utilisateur doit modifier son mot de passe dans les cas suivants :
  - a. A la première connexion à un système / application ;
  - b. Lorsqu'il soupçonne une compromission du système / de l'application ou une divulgation de son mot de passe ;
- 5) L'utilisateur ne doit pas utiliser les mêmes mots de passe pour les activités professionnelles et extra-professionnelles ;
- 6) L'utilisateur ne doit pas utiliser un mot de passe qui fait partie de son nom ou de son prénom ;
- 7) Les mots de passe sont confidentiels et ne doivent pas être écrits sur un document papier ou enregistrés en clair sur un support numérique (poste de travail, clef USB, téléphone mobile, etc.) ;
- 8) L'utilisateur doit informer son chef hiérarchique et le RSSI de toute tentative de violation de son compte / mot de passe ;
- 9) Tout utilisateur est responsable des ressources auxquelles il a accès, il est strictement interdit de divulguer ou exporter, sous n'importe quel format, des données confidentielles liées à EXCELLIA.

### 2.3. Usage du matériel informatique


- 1) Le matériel informatique de EXCELLIA doit être manipulé conformément aux exigences de sécurité définie par la PSI.
- 2) À la fin de la journée de travail, chaque utilisateur est tenu de :
  - a. Éteindre son poste de travail ;
  - b. Éteindre tous les périphériques connectés à son poste de travail tels que l'écran et l'imprimante.
- 3) L'utilisateur ne doit en aucun cas installer ou tenter d'installer des applications sur son poste de travail qui ne sont pas utiles pour la réalisation des tâches qui lui ont été affectées dans le cadre de son travail.

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 5 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	<b>Date :29/10/2024</b>

- 4) L'utilisateur s'engage à ne pas perturber le fonctionnement du réseau. Il s'interdit l'installation de logiciels ou de programmes depuis une disquette, la messagerie ou internet. Il s'interdit toute action qui pourrait saturer le réseau ou lui nuire.
- 5) L'utilisateur ne doit jamais connecter des équipements personnels au poste de travail de EXCELLIA.
- 6) L'utilisateur doit scanner tous les supports amovibles connectés au poste de travail avant de les utiliser.
- 7) Ne sont, notamment, pas autorisés les pratiques suivantes :
  - a. Le téléchargement de vidéo, d'images, des sites, des logiciels non liés à l'activité professionnelle de l'utilisateur
  - b. La diffusion de tracts par messagerie
  - c. Le « spam » (diffusion d'un document en grand nombre)
  - d. Les forums ne sont autorisés que dans le cadre de groupes de travail reconnus par l'Institution
- 8) L'utilisateur accepte que EXCELLIA puisse avoir un contrôle technique sur son PC à tout moment.
- 9) Tout constat de violation, tentative de violation ou soupçon de violation d'un système informatique doit être signalé au service informatique.

## 2.4. Télétravail

- 1) Les utilisateurs, y compris les administrateurs et les tiers, du SI de EXCELLIA doivent se connecter via un réseau privé virtuel (VPN) ou un autre moyen d'accès sécurisé approuvé par EXCELLIA.
- 2) Les utilisateurs doivent utiliser des mots de passe forts et uniques pour accéder aux systèmes de EXCELLIA, et ils doivent être incités à les changer périodiquement.
- 3) Les employés de EXCELLIA sont tenus d'utiliser exclusivement des appareils mobiles professionnels pour accéder aux systèmes d'information de EXCELLIA lors d'une connexion à distance. L'usage d'appareils mobiles personnels est formellement interdit, sauf en cas de déploiement d'une solution de gestion des appareils mobiles (Mobile Device Management - MDM).


	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 6 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	<b>Date :29/10/2024</b>

## 2.5. Politique du bureau propre et de l'écran verrouillé

- 1) L'utilisateur doit protéger convenablement les informations électroniques et non électroniques mises à sa disposition en utilisant par exemple des coffres forts, des armoires ou tout autre dispositif de rangement sécurisé ;
- 2) L'utilisateur doit verrouiller ou fermer ses sessions système et/ou applicatives dès qu'il s'absente de son bureau ([Win][ L] pour verrouiller l'ordinateur) ;
- 3) L'utilisateur doit se déconnecter des applications ou des services en réseau distants lorsqu'il n'a plus besoin de ces connexions, et ne doit pas se contenter seulement d'éteindre son poste de travail.

## 2.6. Signalement des événements et des failles liées à la sécurité de l'information

- 1) Les utilisateurs et les tiers sont tenus de signaler tout évènement ou faille liés à la sécurité de l'information.
- 2) Les éléments ci-dessous représentent des exemples d'évènements liés à la sécurité de l'information :
  - a. Une violation de l'intégrité de l'information, de sa confidentialité ou de sa disponibilité ;
  - b. Une erreur humaine ;
  - c. Le non-respect des politiques ou des procédures de sécurité de EXCELLIA ;
  - d. Une violation des dispositions relatives à la sécurité physique ;
  - e. Un dysfonctionnement logiciel ou matériel ;
  - f. Une violation d'accès.
- 3) En cas de détection par un utilisateur d'un incident lié à la sécurité de l'information, il doit :
  - a. Noter immédiatement tous les détails importants (par exemple le type de la violation, le dysfonctionnement observé, les messages affichés à l'écran, etc.) ;

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 7 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	Date :29/10/2024

- b. Signaler immédiatement le problème au point de contact (défini par la procédure de gestion des incidents) et ne pas prendre d'initiative personnelle d'investigation / de résolution.


## 2.7. Le respect du droit de propriété intellectuelle

- 1) Conformément à la loi n° 94-36 du 24 février 1994 modifié et complété par la Loi n° 2009-33 du 23 juin 2009, relative à la propriété littéraire et artistique, l'utilisateur :
  - a. Doit s'abstenir de faire des copies des logiciels commerciaux pour quelque usage que ce soit. La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement. L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi judiciairement ;
  - b. Déclare connaître et accepter que tout logiciel / document créé par un ou plusieurs employés dans l'exercice de leurs fonctions appartient à EXCELLIA, à qui sont dévolus tous les droits reconnus aux auteurs.

## 2.8. Utilisation correcte des actifs

### 2.8.1. Utilisation d'Internet

- 1) L'accès à Internet est strictement réservé aux utilisateurs ayant reçu une autorisation préalable conformément à la **Procédure de contrôle des accès logiques** ;
- 2) L'accès à Internet à partir des équipements informatiques de EXCELLIA ne doit se faire qu'à travers les moyens d'accès fournis par EXCELLIA ;
- 3) L'utilisateur doit faire preuve d'une vigilance particulière à l'égard du contenu des échanges qu'il réalise à travers Internet. Il est, par ailleurs, totalement interdit de :
  - a. Visualiser, télécharger, transmettre ou conserver des contenus inappropriés, tels que ceux qui peuvent être offensants, discriminatoires, diffamatoires, ou contraires aux principes d'éthique et de respect de la personne humaine.
  - b. Transmettre ou de publier sur Internet des informations de EXCELLIA classifiées « Internes », « Confidentielles » ou « Restreintes ».

	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 8 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	<b>Date :29/10/2024</b>

- c. Transmettre ou de publier sur les réseaux sociaux (Facebook, LinkedIn, Twitter, Instagram, etc) ou à travers les outils de chats (Messenger, Telegram, etc) des informations de EXCELLIA classifiées « Internes », « Confidentielles » ou « Restreintes ».

### 2.8.2. Utilisation de la messagerie électronique


- 1) Le service de messagerie électronique de EXCELLIA est destiné strictement à un usage professionnel. Pour cela, chaque utilisateur ayant accès à ce service est tenu de :
  - a. Ne pas utiliser la messagerie professionnelle pour échanger des courriels personnels ;
  - b. Ne pas utiliser sa messagerie privée pour échanger des courriels professionnels sauf lorsque la messagerie professionnelle n'est pas disponible et uniquement pour l'échange d'information classées « Public » ou « Interne » ;
  - c. Ne pas ouvrir de pièces jointes d'un message provenant d'une source douteuse ;
  - d. Ne pas transmettre ou publier des messages de harcèlement (sexuel ou moral), de menaces ou d'insultes ;
  - e. Ne pas transmettre des rumeurs ou de fausses alertes ;
  - f. Ne pas Transférer, en clair, des pièces jointes contenant des informations de EXCELLIA classées « Confidentielles » ou « Restreintes ».

## 3. Sanctions disciplinaires


Les utilisateurs ne respectant pas les règles et obligations définies dans la présente charte sont passibles de sanctions :

- └ Ils peuvent – sur demande et/ou autorisation de la Direction Générale - être déconnectés par les administrateurs du système et/ ou son supérieur hiérarchique ;
- └ Leur(s) compte(s) peut (vent) être désactivé(s), sur décision de la Direction Générale ;



	<b>Système de Management de Sécurité de l'Information</b>	<b>Réf : CH.SMSI.01</b> <b>Version : 0.1</b> <b>Page 9 sur 10</b>
	<b>Charte de Sécurité de l'Information pour les utilisateurs</b>	Date :29/10/2024

- } En cas d'infraction prouvée, le directeur Cloud a la latitude de procéder à une suspension provisoire de ce(s) compte(s) en attendant la décision de la Direction Générale ;
- } Ils peuvent être traduits devant le conseil disciplinaire ;
- } Ils peuvent faire l'objet de poursuites pénales engagées à la suite d'enfreinte grave à la législation en vigueur dont notamment :
- } Les articles 199bis et 199ter du code pénal
- } Loi n°2004-5 du 3 Février 2004 portant sur l'organisation du domaine de la sécurité informatique et la fixation des règles générales de protection des systèmes informatiques et des réseaux
- } Loi n°2004-63 du 27 Juillet 2004 relative à la protection des données à caractère personnel.

	Système de Management de Sécurité de l'Information	Réf : CH.SMSI.01 Version : 0.1 Page 10 sur 10
	Charte de Sécurité de l'Information pour les utilisateurs	Date :29/10/2024

## 4. Engagement personnel

Je soussigné(e)

Nom : .....

Prénom : .....

Matricule : .....

Utilisateur du SI de EXCELLIA, déclare ma connaissance de la totalité de la présente Charte de Sécurité de l'Information pour les utilisateurs de EXCELLIA et m'engage au respect de toutes les règles de sécurité qui y sont mentionnées.

En cas de violation, je suis conscient de mon exposition aux sanctions comme mentionné dans l'article 3 de la présente Charte.

Je déclare avoir **lu et approuvé** la charte de sécurité de l'information de EXCELLIA.

Date : .....

Signature : .....