EMCSI SAS au capital de 3000 euros
32 rue du Port 95000CERGY
administration@emcsi.fr
931 593 495 R.C.S. Pontoise
emcsi.fr

Charte des usages numériques

Version du : 15/09/2024 Réf. : DR_CI_v20241001

PARTIE 1 : PREAMBULE

Article 1.0 - Objectifs

Cette « Charte des usages numériques », dite « Charte informatique » explicite certains droits et devoirs des Usagers du Système d'information d'EMCSI.

Cette charte étant annexée aux CGV d'EMCSI, elle constitue une part intégrante de celles-ci.

Cette Charte établit certaines sanctions applicables en compléments d'éventuelles autres sanctions judicaires ou réglementaires.

Concernant le Personnel d'EMCSI : Bien qu'elle ne s'applique pas exclusivement au personnel d'EMCSI, cette Charte constitue, en outre, d'une part une annexe au Règlement Intérieur et d'autre part un complément à La Politique de Sécurité Informatique de la société.

Article 1.1 – EMCSI

EMSCI est la SAS (Société par Actions Simplifiée) au capital de 3 000 euros immatriculée A 931 593 495 au R.C.S. (Registre du Commerce et des Sociétés) de Pontoise, la société établissant la présente Charte.
EMCSI est une Entreprise de Services Numériques (ESN) proposant principalement les services suivants :

- Licences d'utilisation de nos logiciels et services applicatifs, en **mode SaaS**
- **Maintenance** et tierce maintenance évolutive, réglementaire, sécuritaire et corrective
- **Evolutions** sur demande des caractéristiques des produits et **développements** sur mesures
- **Support** et **assistance** à l'utilisation et à l'exploitation
- **Interventions** techniques d'extraction ou de configuration de données
- **Formation** à l'utilisation des outils
- **Audits** et conseils concernant le système d'information et les processus métiers
- Audits et **conseils** concernant l'utilisation de nos solutions
- Hébergement et **exploitation** des serveurs (bases de données et services)
- **Hébergement** des postes clients (virtualisés)
- Assistance ou délégation de l'**administration** et du **paramétrage** des outils
- **Délégation de la saisie** (administration des ventes) complétant ou se substituant aux opérateurs : facturation, hotline back office de gestion des abonnements, hotline de commande de petites annonces, gestion des domiciliations, relances abonnés …
- Vente de **licences** ou de solutions logicielles ou matérielles

Article 1.2 – Définition des parties prenantes et du vocabulaire

Salariés

Les « Salariés » sont chacune des personnes physiques travaillants pour EMCSI en échange d'une rétribution ou d'un salaire et dans le cadre d'un contrat (à durée déterminée ou indéterminée) avec un lien de subordination. Les salariés peuvent être à temps plein ou à temps partiel. Pour cette Charte, les salariés d'EMCSI en cours de période d'essai sont inclus dans la définition des « Salariés ».

Personnels

Pour la présente Charte le terme « Personnel » ou « membres du Personnel » comprend les Salariés ainsi que les personnes non salariées travaillant ou exerçant une mission ou une tâche pour EMCSI. Sont également inclus, sans que cette liste soit limitative, les éventuels sous-traitants, intérimaires, stagiaires, bénévoles, alternants et autres intervenants…
Il ne s'agit donc ici pas exclusivement du « personnel salariée ». Sont inclues notamment les personnes sans lien de subordination. Donc, Bien qu'étant annexée au Règlement Intérieur, cette Charte concerne et engage aussi des personnes non-salariés d'EMCSI.

Clients

Pour la présente Charte le terme « Clients » regroupe l'ensemble des personnes morales et physiques bénéficiant des prestations et ou solution proposée par EMCSI. Sont inclus incluent l'ensemble des organisations concernées, avec leurs établissements, filiales, succursales et maison mères (holdings, groupes, …) et leurs personnels ainsi que leurs sous-traitants.
Les éventuelles personnes physiques commandant des prestations à la Société sont également inclues dans cette définition.
Les bénéficiaires, stagiaires, élèves et apprenants d'actions de formation ou de sensibilisation organisées ou réalisés par EMCSI ou ses sous-traitants font également partie des Clients pour cette Charte. Les commanditaires, employeurs et financeurs des bénéficiaires d'actions de formation sont également considérés comme Clients par la présente Charte.

Usagers

Les « Usagers » regroupent l'ensemble du Personnel incluant les Salariés, et l'ensemble des Clients. Les personnes en phase de candidature ou de pré-embauche, utilisant certaines Ressources informatiques d'EMCSI sont également considérées comme « Usagers ».
Lorsque les solutions ou services qu'EMCSI propose en ligne (sur Internet) sont utilisées par des clients de ses clients, les utilisateurs sont considérés comme des Usagers. Dans ce cas, il revient au Client de communiquer et de faire accepter et respecter la présente Charte pour les clauses qui concernent ces personnes.
Pour cette Charte, les termes « Utilisateur » et « Usager » sont synonymes.

Ressources informatiques

Le terme « Ressources informatiques » recouvre l'ensemble des systèmes, matériels, logiciels, applications, modules, plateformes, sites internet, web services, bases de données, codes sources, fichiers, flux, documents, publications, courriels, articles, podcasts, tutos, commentaires et données numériques propriété ou non d'EMCSI, mis à la disposition, directement ou indirectement des Usagers d'EMCSI. Cette charte ne se restreint pas aux ressources présentes dans les locaux d'EMCSI et inclut également, entre autres, les ressources hébergées sur internet ou chez des prestataires ou sous-traitants ainsi que les terminaux ordinateurs, tablettes, smartphones, objets connectés et périphériques divers, fixes, portables, mobiles et nomades et tout ce qu'ils

contiennent, gèrent, partagent ou diffusent. Ces énumérations sont illustratives et non exhaustives. Les formulations « Ressources informatiques », « Ressources numériques », « outils et ressources numériques », « informatique et réseaux » sont considérées comme synonymes. Les « ressources informatiques » englobent donc l'ensemble du Système d'Information (SI), y compris les « Services Numériques » définis ci-après.

Services Numériques

Le terme « Services Numériques » dans les présentes Conditions Générales de Vente s'entend, sans que cette énumération soit limitative, pour : tout progiciel ou logiciel, toute application, module, plateforme, site, fonctionnalité, traitement, script, webservice, interface, page, fenêtre, fonction, librairie, API, Plugin, batch, macro, bot, prompt, automatisme, procédure, classe, trigger, compilé ou non, ou base de données ou format de fichier, mis à disposition du Client par le Prestataire. Ceci inclut également la documentation de ces éléments, ainsi que les codes sources.
Les « Services Numériques » constituent ainsi un sous-ensemble des « Ressources informatiques ».

Equipements individuels

Pour la présente Charte, les « équipements individuels » ou « matériel informatique individuel », sont les ordinateurs portables ou fixes (PC ou MAC ou Chromebook), tablettes et smartphones mis à disposition des Usagers par la Société ou par leur employeur. Par extension, cette notion comprend également les périphériques et accessoires (tels que claviers, souris, ...) et les supports de stockage amovibles lorsque leur usage est autorisé.

PARTIE 2 : CONTEXTE D'APPLICATION ET ENGAGEMENTS

Article 2.1 – Application

La présente charte s'applique à tout Usager qui utilise les ressources informatiques d'EMCSI, tant localement que par tout autre moyen de connexion.

La perte de qualité justifiant la qualification d'Usager (membre du personnel, prestataire, apprenant, élève, apprenant ou autre) entraîne la suppression de l'habilitation à utiliser des Ressources Numériques.

Article 2.2 – Référentiel documentaire

Cette Charte est annexée d'une part au Règlement Intérieur et d'autre part aux Conditions Générales de Vente.

Cette Charte complète et précise, tant le Règlement intérieur que les conditions générales de vente (CGV) tout en faisant partie, contractuellement, de chacun de ces documents, en tant qu'annexe.

Cette présente Charte complète en outre la politique de sécurité informatique (PSI) sans se substituer à elle.

Des chevauchements sont possibles. En cas de conflit d'interprétation, la Loi prévaut sur les contrats, les contrats (ou conventions) prévalent sur les conditions générales qui prévalent sur le règlement intérieur qui prévaut sur tout le reste. C'est à la direction d'EMCSI qu'il revient de déterminer les textes applicables.

Cette présente Charte est jointe systématiquement aux CGV, contrats et conventions et elle est disponible :

- Sur le site internet d'EMCSI en téléchargement ;
- Dans les environnements numériques d'information des salariés et des clients ;
- Dans les locaux du siège.

Article 2.3 – Engagements

Chaque Usager s'engage à respecter cette Charte qui est obligatoire et qui lui est opposable.

En cas d'irrespect de la Charte, EMCSI décidera et fera appliquer, si elle le juge pertinent, des sanctions, mesures disciplinaires ou pénales et actions adaptées, notamment possiblement des actions en justice en vue d'une mise en cause civile et/ou pénale.

Sans que cette énumération soit limitative, EMCSI peut exiger des dédommagements pour non-respect de cette Charte et/ou pour réparation de préjudices. EMCSI peut en outre, de plein droit interdire à tout contrevenant l'interdiction d'accès aux ressources numériques et supprimer son éventuelle adresse électronique, son espace de stockage et ses abonnements et accès aux services.

L'article « 5.6 Cas de non-respect » de la présente Charte précise certaines les actions, sanctions, réparations ou dédommagements pouvant être prises.

PARTIE 3 : ACCES AUX RESSOURCES

Article 3.1 – Accès temporalisé

Chaque utilisateur reçoit, une fois qu'il a contractualisé avec EMCSI et pour la durée d'application de son contrat, en contrepartie de la signature de la présente charte, un droit d'accès individuel à certaines ressources informatiques d'EMCSI.

Les ressources informatiques d'ERSN auxquelles les utilisateurs ont accès dépendent de la nature de leur relation avec ERSN (apprenant, membre du personnel, financeur…).

Article 3.2 – Accès individuel

Le droit d'accès est strictement nominatif, personnel et incessible.

Chaque utilisateur est responsable de l'utilisation qui en est faite.

L'utilisateur prévient la Direction ou le Responsable de la sécurité Informatique s'il soupçonne la violation de son compte. L'adresse du Responsable de la sécurité Informatique est : tech-lead@emcsi.fr.

Article 3.2 – Accès limité

L'utilisation des ressources informatiques d'EMCSI a pour objet exclusif de mener les activités directement liées l'objets du contrat avec EMCSI.

Ainsi, par exemple :

Concernant les stagiaires ou apprenants ou étudiants bénéficiant d'actions de formation :
L'utilisation des Ressources informatiques a pour objet exclusif de mener des activités pédagogiques, d'enseignement, d'évaluation, de recherche, incluant la gestion et le suivi administratif et qualitatif de ces dernières et exclut tout autre utilisation.

Concernant les sous-traitants :
L'utilisation des Ressources informatiques par les sous-traitants a pour objet exclusif de réaliser l'objet du contrat de sous-traitance et des éventuelles des lettres de mission.

Concernant les salariés :
L'utilisation des Ressources informatiques par les salariés et assimilés, a pour objet exclusif de réaliser l'objet de leur contrat et plus précisément les tâches et missions qui leurs sont confiées.

Concernant les clients pour le support :
Les clients d'EMCSI qui utilise des certaines Ressources numériques dans l'unique but de solliciter le support (plateforme https://tickets.emcsi.fr/) n'ont accès qu'aux ressources directement liées aux prestations de support de de maintenance assurées par EMCSI.

Concernant les clients pour les services hébergés :
Les clients d'EMCSI bénéficiant de services numériques commercialisés par EMCSI selon le modèle SaaS (*Software as a Service*), directement ou via un hébergeur fournisseur d'EMCSI, bénéficient d'accès à des ressources particulières. Ces accès sont définis et limité par les accords commerciaux spécifiques et généraux entre EMCSI et chacun de ces Clients.

PARTIE 4 : LES REGLES DE BON USAGE

Chaque utilisateur s'engage à respecter les obligations légales et réglementaires ainsi que celles propres à cette Charte, dont notamment les règles suivantes :

Article 4.1 – Conditions d'accès aux ressources informatiques et aux locaux

4.1.1 Comportement général

Tout utilisateur accepte de se plier aux contraintes particulières définies par les différents services d'EMCSI pour l'accès à leurs locaux et aux Ressources informatiques, et à avoir un comportement civil et respectueux d'autrui.

4.1.2 Il est notamment interdit :

- d'usurper l'identité d'autrui ou de s'approprier le mot de passe d'un autre utilisateur ;
- de masquer sa véritable identité ;
- de modifier, d'altérer, ou de copier des informations n'appartenant pas à l'Usager ;
- de consulter ou partager ou diffuser de sa propre initiative sans autorisation express préalable des informations ne lui appartenant pas ;
- d'accéder à des applications, des données autres que celles pour lesquelles il a reçu un droit d'accès ;
- de se livrer à des actes de piratage, de cyber-malveillance et de cybercriminalité.

4.1.3 Concernant les documents et fichiers en général

Il est notamment interdit concernant l'usage d'internet et la gestion de documentaire sur les réseaux ou les matériels d'EMCSI, de consulter ou de publier des documents, fichiers, posts ou messages sous quelque format que ce soit :

- à caractère diffamatoire, injurieux, obscène, raciste, xénophobe ;
- à caractère pédophile ou pornographique ;
- incitant aux crimes, délits ou à la haine ;
- incitant à fabrication, ou l'usage ou la consommation de substances ou objets illégaux ou dangereux ;
- à caractère commercial dans le but de vendre des substances ou objets illégaux.

Article 4.2 – Respect de l'intégrité du système informatique dans son ensemble et de chacune de ses composantes

Il est notamment interdit :

- d'effectuer des opérations pouvant nuire au fonctionnement normal du réseau ;

- d'introduire ou de substituer ou d'altérer ou de consulter ou d'exfiltrer frauduleusement des données ;

- d'installer des logiciels ou des utilitaires sans demande ou autorisation expresse et formelle, même sur son compte ;

- de contourner les restrictions d'utilisation d'un Service Numérique;

- d'effectuer des activités accaparant les ressources informatiques d'ERSN (stockage de gros fichiers) et d'envoyer des courriers en masse (Spam) ;

- de détériorer le matériel mis à disposition (PC, terminaux, imprimantes...).

Article 4.3 – Respect des règles de propriété intellectuelle

Il est notamment interdit :

- d'effectuer la copie de Logiciels ou autres Services Numériques disponibles sur le réseau ;

- d'effectuer la copie de codes sources de logiciels ou se sites disponibles sur le réseau ;

- d'effectuer la copie de données ou de fichiers disponibles sur le réseau ;

- d'effectuer la copie d'œuvres protégées par le droit d'auteur, incluant entre autres, les supports, illustrations et exercices de cours, les documentations techniques et réglementaires.

Article 4.4 – Protection de la personne

4.4.1 Protection de la dignité humaine

Il est notamment interdit :

- de diffuser ou copier des textes ou des images susceptibles de porter atteinte à la représentation ou à l'intimité de la vie privée ;

- de fabriquer, d'enregistrer ou de transmettre un message ou des données numériques à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine.

4.4.2 Droit de la presse (loi du 29 juillet 1881) et liberté d'expression

Il est notamment interdit :

- de porter atteinte à l'intégrité de toute personne, à sa sensibilité, notamment par l'intermédiaire de messages injurieux ou diffamatoires et d'images ou vidéos provocantes ;

- de diffuser des informations faisant l'apologie du racisme, des crimes contre l'humanité, de l'antisémitisme, du négationnisme, de la pornographie, de la pédophilie et de la xénophobie ;

- d'harceler, insulter, humilier, diffamer, agresser, ridiculiser qui que ce soit (personnes physiques et morales et marques) et d'enregistrer, ou de diffuser des textes ou des images ou sons, susceptibles d'y contribuer ;

- de constituer, d'enregistrer, de copier, de partager, de diffuser tout message ou fichier ou flux numérique illicite ou de manière illicite ou cherchant à favoriser ou réaliser une action illicite ;

- de diffuser des informations, données ou fichiers incitant aux crimes et aux délits.

Pour cela il convient de s'adresser à la direction des données ou à la direction des systèmes d'information d'EMCSI à l'adresse dsi@emcsi.fr, pour poser toute question ou obtenir toute information, procédure ou autorisation sur ces sujets.

4.4.3 Protection de données à caractère personnel

Tout utilisateur souhaitant constituer ou utiliser un fichier intégrant des données à caractère personnel doit s'assurer du respect de la loi française Informatique et Libertés du 17 janvier 1978 et du règlement général européen sur la production des données (RGPD) européen.

Pour cela il convient de s'adresser à la direction des données ou à la direction des systèmes d'information d'EMCSI à l'adresse support@emcsi.fr ou à l'adresse tech-lead@emcsi.fr, pour poser toute question ou obtenir toute information, procédure ou autorisation sur ces sujets.

4.5 Règles relatives aux moyens de cryptologie

L'Usager ne peut utiliser sur le réseau d'EMCSI des moyens de cryptologie, de cryptographie ou de chiffrement qui n'auraient pas fait l'objet d'une autorisation préalable expresse et formelle.

4.6 Assistance aux usagers

4.6.1 Assistance aux Clients

Les Clients peuvent solliciter EMCSI via :

- La saisie et le suivi de tickets sur la plateforme internet d'assistance et d'échange d'EMCSI : https://tickets.emcsi.fr
- L'envoi d'un courriel à : support@emcsi.fr

Les sollicitations peuvent concerner tout sujet lié aux ressources numériques.

4.6.2 Cas des actions de formation

Concernant les actions de formation qu'elles soient en présentiel ou en tout ou partie en distanciel :

- Le contact d'assistance technique est : support@emcsi.fr
- Le contact d'assistance pédagogique est : formations@emcsi.fr
- Pour tout besoin d'assistance il la plateforme internet https://tickets.emcsi.fr est également disponible.

Concernant les actions de formation en présentiel le formateur est l'interlocuteur principal pour tout besoin d'assistance technique ou pédagogique. En cas de difficulté, le personnel administratif (adminitration@emcsi.fr) et la direction (direction@emcsi.fr) sont également à disposition des apprenants, des commanditaires et des financeurs.

4.6.3 Cas des membres du Personnel

Pour alerter ou bénéficier d'une assistance concernant les ressources informatiques, les membres du Personnel peuvent s'adresser à la direction technique (tech-lead@emcsi.fr) ou à la direction (direction@emcsi.fr).

PARTIE 5 : CONTROLES, RESPONSABILITES ET SANCTIONS

5.1 Sources des obligations

Les obligations des Usagers au regard des Ressources informatiques sont établies par la Loi, les textes réglementaires et la présente Charte avec ses éventuelles annexes.

Cas des salariés :

Certaines obligations, responsabilités et sanctions des Usagers salariés sont établies par le règlement intérieur. La présente Charte étant annexée au règlement intérieur, les salariés sont concernés par de celle-ci, qui leur est opposable.

Cas des clients :

La Présente Charte fait partie des CGV dont elle est annexe.

5.2 Nécessités techniques

Pour des nécessités de maintenance et de gestion technique, la Direction des Systèmes d'Information se réserve le droit :

- d'accéder sur le réseau qu'elle administre aux informations nécessaires à des fins de diagnostic et d'administration du système en respectant scrupuleusement la confidentialité de ces informations ;
- d'établir des procédures de surveillance de toutes les actions réalisées et de toutes les tâches exécutées sur les systèmes et machines et ressources informatiques en général, afin de déceler les violations ou les tentatives de violation de la présente Charte.

5.3 Secret de la correspondance

EMCSI s'engage à respecter le secret de la correspondance.

5.4 Droit d'appréciation

EMCSI se réserve le droit d'apprécier du respect par les utilisateurs des règles de bon usage décrites dans la présente charte.

5.5 Responsabilisé individuelle des Usagers

Chaque Usager accède et utilise les Ressources informatiques, dont le réseau, sous sa propre responsabilité.

5.6 Cas de non-respect

Le non-respect des règles et obligations définies dans les dispositions législatives et réglementaires et dans la présente charte ainsi que le non-signalement des tentatives de violation de son compte ou d'incident de sécurité font encourir à l'Usager :

- l'interdiction d'accès aux ressources numériques d'EMCSI ;
- l'interdiction d'accès aux salles informatiques et diverses ressources informatiques ;
- la suppression de son éventuelle adresse électronique et de son éventuel espace de stockage ;
- la suppression de ses éventuels abonnements et accès à des services numériques ;
- concernant les salariés et assimilés, des sanctions disciplinaires : la Direction a pleine autorité pour engager une procédure disciplinaire, notamment conformément aux dispositions du décret 92-657 du 13/07/1/92 relatif à la procédure disciplinaire dans les établissements d'enseignement supérieur ;
- des sanctions pénales et civiles : des poursuites pénales et civiles prévues par les textes législatifs et réglementaires désignés ci-après peuvent être engagées à l'encontre de l'Usager ;
- la rupture de plein droit du contrat liant l'Usager ou l'employeur de l'Usager à EMCSI. Il peut s'agit par exemple, sans que cette liste soit limitative, d'une convention de sous-traitance, d'un contrat ou d'une convention de formation, d'un contrat de travail, d'une convention de stage, d'un contrat de maintenance applicative, ...

PARTIE 6 : HYGIENE NUMERIQUE

Il est demandé aux utilisateurs de respecter les principes de bon sens de vigilance et de responsabilité et règles générales d'hygiène numérique dont notamment :

6.1 Principes généraux d'hygiène numérique

- la fermeture systématique des sessions de connexion (ou « déconnexion ») ;
- ne jamais laisser un terminal (PC, téléphone, ...) allumé sans surveillance ;
- ne jamais laisser un terminal (PC, téléphone, ...) dans un local ou une pièce sans surveillance sans que l'entrée soit verrouillée (serrure fermée, digicode, ...) ;
- définir des mots de passe robustes et privilégier les modes d'authentifications forts ;
- ne jamais communiquer ni « laisser trainer » ses mots de passe ;
- ne jamais utiliser le même mot de passe pour des usages distincts ;
- ne jamais ouvrir un courriel suspect ni cliquer sur un lien suspect ;
- s'assurer que les informations importantes soient sauvegardées en plusieurs lieux ;
- s'assurer de la conformité (validité, format, propriété, actualité, licité, intégrité, non infection) d'une information ou d'un fichier avant de l'introduire dans un système ;
- respecter le niveau de confidentialité des documents tels que défini par leurs auteurs ;
- respecter sa propre intimité et dignité en ne communiquant que des informations utiles et appropriées.

6.2 Principes généraux concernant les équipements individuels

Usage professionnel

Les équipements individuels sont destinés exclusivement à un usage professionnel.
Réciproquement, l'utilisation d'équipements autres que ceux mis à disposition par la Société ou par l'employeur de l'Usager est proscrit.
L'utilisation de matériel non géré par la société pose divers problèmes de sécurité et est globalement proscrit. L'utilisation de matériels pour des usages non prévus ou non contrôlés par la Société pose également des problèmes ou risques de sécurité expliquant son interdiction.
Une dérogation s'entend dans le cas particulier et unique où l'Usager est un client particulier de la Société utilisant son propre matériel pour bénéficier des services de la Société.

Usage individuel

Les équipements individuels ne doivent pas être partagés ni prêtés, même à un autre usager, sans accord préalable formel et circonstancié de la direction ou du RSSI.
Les équipements individuels ne doivent pas être laissés sans surveillance de la personne qui en a la charge, même éteints ou déconnectés. Ils doivent demeurer inaccessibles à toute personne non habilitée.
Par exemple, des personnes mal intentionnées ou manipulées peuvent infecter ou substituer des accessoires (claviers, souris, clés usb, ...) avec des keylogers ou portes dérobées ou chevaux de Troie ou divers autres malwares.

Identification et authentification individuelles

L'identification des Usagers, notamment concernant les équipements doit être individuelle.
Les identifiants d'utilisateurs doivent être uniques et propres à chaque utilisateur.

La direction ou le responsable du système d'information doivent être systématiquement informés de toute création ou de tout changement d'identifiant d'utilisateur. Les identifiants sont centralisés.

Chiffrement des disques

Les terminaux (PC, ordinateurs Apple, smartphones, tablettes, ...) doivent être systématiquement configurés pour que le chiffrement des supports de stockage soit activé (via BitLocker ou FileVault pour les ordinateurs). Les usagers doivent s'assurer que le chiffrement est activé ou s'adresser à l'assistance aux usagers (coordonnées mentionnées à l'article

Gestion des documents

Les documents professionnels doivent demeurer sur les serveurs ou espaces de stockages d'EMCSI ou mise à disposition des Usagers par EMCSI. Il convient donc :

- De ne pas transmettre des documents par courriels et de privilégier les liens, exceptés les documents à destination externes destinés exclusivement au destinataire et les documents publics ;
- De ne pas utiliser de supports amovibles (tels que clés USB, disques externes, cartes mémoire, ...) pour transférer ou archiver des documents ;
- De ne pas stocker de fichier constituant une ressource numérique sur les disques locaux (dits « disques durs ») ou mémoires des terminaux (ordinateurs, tablettes, smartphones) en dehors des « drives » mis à disposition par EMCSI.

6.2 Règles concernant les mots de passe

EMCSI demande aux Usagers, outre les bonnes pratiques ainsi que les principes généraux rappelés en Partie 6, de respecter les « 30 Règles d'or d'utilisation et de gestion des mots de passe » disponibles en ANNEXE I.

PARTIE 7 : DONNEES DES TIERS

Les données des tiers sont les fichiers, documents et contenus de bases de données confiés à EMCSI par des tiers ou mis à la disposition d'EMSCI et de ses éventuels sous-traitants par des tiers. Ces tiers pouvant être, sans que cette liste d'exemple soit limitative, des partenaires, des sous-traitants, des clients, des stagiaires ou des apprenants. Cette partie concerne tous types de données hormis les données publiques et les données propriété d'EMCSI, et n'est pas spécifique aux données à caractère personnel.

7.1 Principe du moindre privilège

Le principe du moindre privilège énoncé à l'Article 7.3 de la Politique de Sécurité du Système d'Information (PPSI) d'EMCSI s'applique notamment aux données des tiers.
Ainsi seuls les usagers expressément habilités peuvent accéder aux données des tiers pour un usage exclusivement conforme à ce qui est requis pour l'exécution des taches ou missions.

7.2 Principe de non copie des données de tiers

Sauf suite à une demande légitime du tiers concerné ou à l'exécution d'une opération d'administration ou d'exploitation contractuelle les Usagers ont interdiction de copier ou de transférer sur un autre système ou un autre support ou sur un autre format des données d'un tiers.

7.3 Copies de secours et archives

Lorsque des données de tiers sont archivées, les archives sont systématiquement chiffrées et conservés sous accès restreint.

Les archives de données de tiers sont systématiquement effacées après le délai convenu auprès du tiers. Ce délai ne peut excéder 13 mois excepté les exceptions prévues par la loi.

7.4 Pseudonymisation des jeux de test

Hormis le cas des sauvegarde et d'archivage, lorsque des données de tiers sont copiées dans un autre système ou une autre base (par exemple à des fins de test ou de formation) les données de tiers sont alors systématiquement pseudonymisée, même s'il ne s'agit pas de données à caractère personnel.

PARTIE 8 : REFERENCES LEGALES

- loi n°88-19 du 5 janvier 1988, ou Loi Godefrain, relative aux fraudes informatiques reprise par les articles 323-1 et suivants du code pénal ;
- dans le code pénal :
  - articles 226-15 et suiv. relatifs au secret des correspondances
  - articles 226-1 et suiv. relatifs à l'atteinte à l'intimité de la vie privée
- loi du 29 juillet 1881 modifiée relatives aux infractions de presse ;
- infractions au code de la Propriété intellectuelle :
  - articles 335-2 et suiv. relatifs à la contrefaçon d'une œuvre de l'esprit
  - articles 521-4 relatif à la contrefaçon d'un dessin ou d'un modèle
  - articles 716-9 relatif à la contrefaçon de marque
- loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications ;
- concernant les données à caractère personnel :
  - loi n°78-87 du 6 janvier 1978
  - la loi n°2004-801 du 6 août 2004
  - l'article L. 226-13 du Code pénal et la Directive Européenne du 24 octobre 1995
  - règlement européen de protection des données (dit RGPD) entré en vigueur le 25 mai 2018
  - la loi sur la protection des données personnelles publiée au Journal officiel du jeudi 21 juin 2018
- concernant le harcèlement sexuel et moral :
  - articles L. 1152-2, L.1153-2 et L. 1153-4 du code du travail

PARTIE 9 : ENTREE EN VIGUEUR ET EVOLUTION DE LA CHARTE

9.1 Date d'entrée en vigueur

La première version de la Charte des usages numériques est entrée en vigueur le 1er septembre 2024.

La date d'entrée en vigueur de la version courante est précisée dans le tableau d'historique des version, article « 9.3 Historique des révisions».

La date d'entrée en vigueur fait par ailleurs partie de la référence versionnée du document. Par exemple la Charte référencée « DR_CI_v20240901 » est entrée en vigueur le 1er septembre 2024.

9.2 Evolutions de la Charte

La Charte est amenée à évoluer. Elle peut notamment être revue afin de prendre en compte :

- Les décisions issues de la politique de qualité et d'amélioration continue de la Société ;
- Les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- Les résultats d'analyses de risques ainsi que les actions découlant de contrôles, d'inspections ou d'audits ;
- Les évolutions des contextes organisationnel, juridique, réglementaire et technique.

9.3 Historique des révisions

Révision	Entrée en vigueur	Réf.	Évolutions Majeures
14/08/2024	01/09/2024	DR_CI_v20240901	Version initiale
15/09/2024	01/10/2024	DR_CI_v20241001	Ajout de la partie 7 « Données des Tiers »

PARTIE 10 : ACCESSIBILITE DE LA CHARTE

La version en vigueur de la Charte des Usages Numériques est disponible librement, en version numérique :

- Sur simple demande au siège d'EMSCI
- Sur simple demande par courriel à administration@emcsi.fr
- Sur le site internet d'EMCSI : https://emcsi.fr
- En téléchargement direct à l'adresse : https://emcsi.fr/documents/cgu_emcsi

ANNEXE I - LES 30 REGLES D'OR D'UTILISATION ET DE GESTION DES MOTS DE PASSE

EMCSI
Etudes
Maintenance
Conseil
Services
Informatique

Les 30 Règles d'or d'utilisation et de gestion des mots de passe

- ✓ Ne jamais autoriser un mot de passe identique au login
- ✓ Ne jamais laisser les mots de passe préinstallés
- ✓ Proscrire les mots de passe triviaux: 1234, azerty, toto ...
- ✓ Un mot de passe robuste doit être long (un minimum de 16 symboles est recommandé) et contenir des symboles de natures variées (mixer les chiffres et les lettres minuscules et majuscules et des caractères accentuées et des symboles (+ - € % * # ; ! ? : [ ] § = & , @ $ µ ...). Un niveaux de complexité et une longueur minimale doivent être imposés par les administrateurs.
- ✓ Déterminer des mots de passe qu'il est impossible de deviner. Eviter les noms propres ou communs présents dans les dictionnaires et toute information personnelle telle que prénom, surnom, anniversaire, nom de rue ou d'animal... Les mots de passe les plus robustes sont ceux déterminés de manière aléatoire.
- ✓ Utiliser des mots de passe différents pour chaque usage pour limiter la propagation des vulnérabilités.
- ✓ Adapter la robustesse de chaque mot de passe à son usage. Les mots de passe de la messagerie (et de l'administration système) doivent être plus robustes que les autres. Si le mot de passe de la messagerie est compromis, d'autres mots de passe peuvent être réinitialisés par les pirates qui prennent ainsi le contrôle de tous les accès.
- ✓ En cas de nombreux mots de passe (donc dans les situations courantes), utiliser un outil gestionnaire de mots de passe, dit « coffre-fort de mots de passe ».
- ✓ Ne pas enregistrer les mots de passe dans des systèmes non maitrisés ou non européens (navigateur internet, système d'exploitation du smartphone, ...).
- ✓ Ne jamais, jamais (sans exception) les stocker en clair (non chiffrés) ni les noter ou ni les imprimer.
- ✓ Ne pas utiliser le texte destiné à se remémorer le mot de passe pour y indiquer le mot de passe ni aucune information qu'un attaquant pourrait utiliser pour déterminer le mot de passe.
- ✓ Ne jamais confier son mot de passe à un tiers, même de confiance. Préférer lui donner un accès personnel avec son propre mot de passe.
- ✓ Ne jamais transmettre un mot de passe en clair par messagerie (SMS, e-mail, chat, ...), même lors d'une assistance à distance.
- ✓ Ne pas saisir de mot de passe sur un site internet non sécurisé (https) ou si la connexion n'est pas sécurisée (wifi public).
- ✓ Utiliser des canaux sécurisés (wifi privé sécurisé, connexion VPN, protocoles TLS ...)
- ✓ Les administrateurs doivent mettre à disposition de la direction une copie à jour et fortement sécurisée de leurs mots de passe (et procédures), pour garantir la continuité de l'administration technique en cas d'indisponibilité.
- ✓ Eviter de saisir un mot de passe à partir d'un matériel qui n'est pas le vôtre (ordinateur public ou partagé, ...)
- ✓ En cas de doute, remplacer vos mots de passe.
- ✓ Lors d'un changement de mot de passe, éviter d'incrémenter un compteur (pass1, pass2, pass3 ...) car les pirates ont déjà eu la même idée avant vous.
- ✓ Limiter le nombre de tentatives d'authentification, avec si possible un délai minimal croissant entre les tentatives.
- ✓ Configurer un archivage des authentifications ainsi que l'envoi d'alertes en cas d'authentifications particulièrement sensibles ou avec un élément nouveau (changement de terminal ou de pays) ou un élément possiblement suspect.
- ✓ Configurer le verrouillage systématique des terminaux (smartphones, PC, tablettes) à chaque redémarrage et à chaque sortie de veille.
- ✓ Configurer un chiffrage systématique (déverrouillable par mot de passe) des supports de stockage amovibles (clés USB et disques externes) et des fichiers confidentiels.
- ✓ Limiter la durée de validité des sessions. Ceci inclut le délai d'activation du mode veille sur les terminaux mobiles et fixes.
- ✓ Limiter les informations retournées à l'utilisateur en cas d'échec d'authentification, pour fournir le moins d'informations possible à d'éventuels malfaiteurs. Ainsi par exemple on évite de préciser si le problème vient du nom de l'utilisateur ou du mot de passe ou de la qualité de la connexion. En cas d'authentification multifacteur on ne précise pas le ou les facteurs invalides.
- ✓ Privilégier l'authentification multifacteur (double ou la triple authentification). Cela revient à utiliser des systèmes d'authentification additionnels (carte à puce contenant une clé privée, carte SIM d'un téléphone, biométrie, ...) en complément et non à la place des mots de passe, dès que cela est possible et systématiquement pour les accès les plus critiques (opérations bancaires, administration des systèmes,....).
- ✓ Eviter l'authentification exclusivement biométrique. N'utiliser la biométrie que combinée à d'autres facteurs.
- ✓ Privilégier les moyens d'authentification « forts » et maitrisés. Il est préférable qu'au moins l'un des facteurs de l'authentification multifacteur soit « fort » (tels que ceux s'appuyant sur la possession d'une clé cryptographique secrète).
- ✓ La maîtrise de l'environnement de création, du renouvellement, de la transmission et du stockage des éléments d'authentification contribuent à la robustesse du dispositif et doivent être en cohérence avec le niveau de sécurité souhaité.
- ✓ Fermer les comptes et accès des personnes et logiciels dès l'arrêt de la collaboration, même en cas de collaboration intermittente (définir les périodes, jours et horaires d'accès)