Charte
Informatique et sécurité de l'information

Version publique

Historique des modifications				
Version	**Date**	**Objet de la mise à jour**	**Page concernée**	**Rédacteur**
1	12/04/2023	Création	/	RSSI

Liste de diffusion	
Diffusion	Public
Destinataires	– Tous
Classement du document	– CircetDoc\Sécurité de l'information\04 – Chartes – Teams DSI\05SSI\04 – CHARTES

Visa			
	Responsable	**Date**	**Visa**
Rédacteur	Benoît FANTINO	12/04/2023	BFA
Approbateur	Comité Sécurité	12/04/2023	COS

TABLE DES MATIERES

1. OBJECTIFS DE LA CHARTE

Le système d'information (SI) de Circet France et de ses filiales comprend un ensemble de ressources qui sont mises à la disposition des utilisateurs pour l'accomplissement de leurs missions professionnelles.

Circet définit et met en œuvre les moyens appropriés pour assurer le bon fonctionnement et la sécurité de son SI, en adéquation constante avec l'évolution de la technique, du cadre réglementaire et des risques qu'une négligence ou mauvaise utilisation des ressources peut faire courir à la fois à Circet (tels que par exemple des pertes financières ou une atteinte à l'image) et également à l'utilisateur lui-même.

La présente charte définit les droits et les devoirs de tout utilisateur du SI et plus particulièrement :

- le bon usage des ressources mises à disposition,
- les principes et règles de sécurité,
- les responsabilités de chacun,
- les dispositions de contrôle mises en œuvre par Circet.

2. CHAMP ET PERIMETRE

2.1. Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de Circet, quels que soient leurs statuts, y compris les associés, salariés, intérimaires, stagiaires, employés de sociétés prestataires ou visiteurs occasionnels.

Les utilisateurs veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au SI.

2.2. Système d'information et de communication

Les principes et règles définis par la présente charte s'appliquent aux données ainsi qu'aux ressources mises à disposition des utilisateurs par Circet tels que :

- les **équipements informatiques** : ordinateurs fixes ou portables, terminaux mobiles et appareils assimilables (smartphones, tablettes numériques...),
- les **logiciels**, **fichiers et répertoires**, données et bases de données, système de **messagerie**, intranet, extranet,
- les supports d'information **amovibles** (clés USB, disque-durs externes, cartes SD, CD-ROM, etc.),
- les équipements en réseaux : **serveurs**, **équipement d'interconnexion**, **imprimantes** et **photocopieurs** et tout autre équipement électronique connectés au réseau,
- les téléphones VoIP, équipements de visioconférence, caméras IP.

3. REGLES DE SECURITE ET DE BON USAGE DES RESSOURCES

3.1. Conditions d'accès

L'accès aux ressources du SI de Circet n'est autorisé que dans le **cadre de l'activité professionnelle** des collaborateurs, définie par leur fonction et dans les limites de délégation qui leur sont accordées.

Un usage à titre privé de ces ressources, **ponctuel et raisonnable,** est toléré pour les nécessités de la vie courante, dès lors qu'il ne porte aucun préjudice à l'activité professionnelle et qu'il n'est pas susceptible d'affecter le bon fonctionnement du SI ou de mettre en cause les intérêts ou la réputation de Circet.

L'accès aux ressources du SI est soumis à l'usage d'un **authentifiant individuel strictement personnel** (login et mot de passe personnels) dont l'utilisation engage la responsabilité de l'utilisateur. Les autorisations et droits d'accès peuvent être révoqués à tout moment, et prennent fin en cas de suspension momentanée ou définitive de l'activité professionnelle, en conformité avec le code du travail.

L'utilisateur doit :
- Choisir des mots de passe robustes (8 caractères, en utilisant au moins 4 types de caractères parmi les majuscules, minuscules, chiffres, caractères spéciaux),
- Préserver la confidentialité de son mot de passe (mémorisation, saisie à l'abri des regards) et le renouveler régulièrement,
- Signaler au service informatique de Circet toute violation ou tentative de violation suspectée de son compte et de manière générale tout dysfonctionnement lié à son authentification,
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.

L'utilisateur ne doit pas :
- Communiquer ou céder en aucune manière, même temporairement, son authentifiant ou son mot de passe à un tiers,
- Ecrire son mot de passe ou l'enregistrer sur un support non protégé (tel qu'un post-it ou dans un navigateur Web),
- Usurper l'identité d'un autre utilisateur ou tenter de s'approprier son authentifiant, ni contourner les restrictions d'accès aux ressources mises à disposition par Circet.

3.2. Postes de travail

Les postes de travail sont configurés selon des standards définis par le service informatique de Circet qui intègrent les mesures de sécurité nécessaires à la protection du SI. Leurs conditions d'usage au quotidien ne doivent pas remettre en cause l'efficacité de ces dispositifs de sécurité.

L'utilisateur doit :
- Connecter au réseau de Circet uniquement des postes de travail fournis par le service informatique de Circet,
- Sauvegarder ses données bureautiques, dont la perte serait préjudiciable, sur les zones sauvegardées du réseau (tel que le partage d'agence, le partage du siège -Solliès-Pont- ou le cas échéant OneDrive),
- Être vigilant et signaler tout constat d'anomalie (dysfonctionnement ou comportement anormal, tentative d'accès),
- Limiter son usage du SI dans un contexte non professionnel et identifier clairement les informations à caractère privé et/ou personnel pour le nom du fichier ou répertoire de stockage. Pour la circonstance l'usage d'une mention « Privé » ou « Personnel » ou « Perso » sera usitée et la sécurité de ces informations est assurée par le seul utilisateur,
- Supprimer ses données personnelles de son poste de travail (mail, fichiers, photos…) avant son départ définitif de Circet.

L'utilisateur ne doit pas :
- Modifier la configuration d'un poste de travail ou le paramétrage des logiciels mis à sa disposition remettant

en cause le niveau de sécurité du poste de travail,
- Accéder, tenter d'accéder, supprimer ou modifier des informations ne lui appartenant pas,
- Installer sur un poste de travail, ou connecter au réseau, des composants matériels ou logiciels sans accord préalable formel du service informatique de Circet,
- Introduire des failles de sécurité dans l'architecture du SI, ou exploiter ou tenter d'exploiter une éventuelle faille de sécurité constatée ou en faire la publicité,
- Surcharger les supports de stockage par des données inutiles à l'activité de Circet (tels que par exemple des fichiers vidéo personnel),
- Permettre à des personnes situées en dehors du réseau de Circet, de prendre le contrôle du poste de travail à distance, en dehors des procédures référencées par le service informatique,
- Copier sur un support de stockage personnel des informations ou des documents professionnels.

3.3. Internet

L'utilisateur peut consulter les sites internet présentant un **lien direct et nécessaire avec l'activité professionnelle**, de quelque nature qu'ils soient. Toutefois, une **utilisation ponctuelle et raisonnable** est admise, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, à l'ordre public et qui ne met pas en cause l'intérêt et la réputation de Circet.

L'utilisateur doit :

- Utiliser exclusivement la connexion fournie et sécurisée par Circet,
- Observer un devoir de réserve et se garder d'émettre toute opinion ou d'exercer toute activité susceptible de porter atteinte à l'image de Circet, notamment lors de la participation à des forums ou communication sur des réseaux sociaux,
- Eviter de laisser son adresse de messagerie professionnelle sur les sites, forums et autres lieux d'Internet, afin de prémunir Circet contre la réception de mails indésirables.

L'utilisateur ne doit pas :
- Utiliser son mot de passe professionnel pour s'authentifier sur des sites personnels,
- Tenter d'accéder à internet par des moyens autres que ceux mis à disposition par le service informatiques de Circet,
- Créer ou administrer des services internet ou de communication électronique étrangers aux besoins de l'activité professionnelle ou n'ayant pas fait l'objet d'une autorisation du service informatique,
- Consulter des sites, télécharger ou échanger des informations dont le contenu est illicite ou pouvant porter atteinte à l'image de Circet (tel que par exemple à caractère violent, pornographique, diffamatoire, contraire aux bonnes mœurs, illicite, …).

Pour des raisons de sécurité, la DSI peut être amenée à :
- imposer des configurations du navigateur
- restreindre le téléchargement de certaines données
- tracer les activités des utilisateurs sur Internet
- filtrer l'accès à certains sites Internet
- déchiffrer des flux sécurisés pour l'identification de logiciels malveillants, la protection du patrimoine informationnel ou la détection de flux sortants anormaux.

Les sites bancaires, de protections sociales et les webmails ne sont pas concernés par le dispositif d'inspection du chiffrement afin de conserver le secret des correspondances et le respect de la vie privée.

3.4. Messagerie

La messagerie mise à disposition des utilisateurs est **destinée à un usage professionnel**. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail du salarié ni la sécurité du réseau informatique de Circet.

Les contenus des messages transmis engagent la responsabilité de leur émetteur qui doit préserver l'image de Circet en toutes circonstances.

En cas d'absence d'un utilisateur et afin de ne pas interrompre le fonctionnement du service, le service informatique de Circet peut ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur. Le supérieur hiérarchique n'a pas accès aux autres messages du salarié. Le salarié concerné est informé dès que possible de la liste des messages qui ont été transmis.

L'utilisateur doit :

- Faire preuve d'une vigilance accrue en cas de réception d'un **message inhabituel ou douteux** en provenance d'un expéditeur inconnu, présentant une syntaxe approximative, contenant des liens vers des sites et /ou des pièces jointes non sollicités, ou demandant d'effectuer des actions inhabituelles.
- **Eviter d'échanger des informations sensibles par messagerie** et s'il n'est pas possible de faire autrement, limiter l'envoi aux seules personnes ayant besoin d'en connaitre,
- Respecter strictement la procédure de classification de l'information de Circet, en appliquant les mesures de sécurité prescrites pour protéger l'envoi de messages et /ou documents en pièce- jointe contenant des données sensibles,
- Considérer que le transfert de messages et leurs pièces jointes, à caractère professionnel, sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes,
- Accéder à distance à sa messagerie professionnelle au travers d'un navigateur en prenant soin de supprimer ensuite les fichiers qui seraient utilisés dans ce cadre,
- Marquer les messages personnels par la mention « Privé » ou « Personnel » ou **« Perso** » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé » ou « Personnel » ou « Perso ». Les messages reçus doivent être également classés, dès réception, selon le même principe. En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

L'utilisateur ne doit pas :

- Transférer des messages de sa messagerie professionnelle vers sa messagerie personnelle (manuellement ou grâce à une procédure de renvoi automatique),
- Ouvrir un message, ou une **pièce jointe associée**, qui présente **un doute** quant à sa provenance ou son contenu,
- Donner suite ou rediffuser les messages en chaîne ou alarmistes (hoax) qui utilisent inutilement les ressources du SI,
- Envoyer en masse des messages directs ou indirects, internes ou externes, à destination des messageries de Circet,
- Cliquer sur les liens hypertextes contenus dans un message non sollicité et demandant de fournir des données confidentielles (phishing),
- Répondre aux messages électroniques commerciaux non sollicités (spam),
- Donner son consentement explicite de manière systématique pour recevoir des newsletters, abonnement ou autres n'ayant pas un caractère professionnel,
- Utiliser les listes de diffusion pour un usage externe.

3.5. Equipement personnel

La connexion d'ordinateurs personnels au réseau interne Circet n'est pas autorisée, seuls des ordinateurs professionnels Circet peuvent être branchés sur le réseau interne Circet.

L'usage d'équipement informatique peut être autorisé à titre exceptionnel pour une période convenue après :

- l'accord explicite de Circet pour cet usage,
- que l'utilisateur ait accepté formellement la mise en œuvre de mesures de sécurité sur l'équipement (par exemple la possibilité de supprimer les données de Circet ou le verrouillage à distance de l'équipement).

4. VIGILANCE AU QUOTIDIEN

La sécurité du SI de Circet repose sur l'implication de chacun.

L'utilisateur doit :

- S'engager à ne pas laisser, sur les fax, imprimantes ou photocopieurs les documents sensibles envoyés, imprimés ou photocopiés,
- S'engager à ne pas laisser accessibles ses sessions Windows en cours,
- Veiller systématiquement à la sécurisation de son poste de travail et des matériels nomades qui lui sont confiés
- Eteindre (arrêt électrique) son poste de travail lorsque l'utilisateur quitte son lieu de travail (afin de permettre les mises à jour automatiques de se déployer sans gêne),
- Prévenir sans délai sa hiérarchie ainsi que le service help desk de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication,
- Privilégier un accès VPN (Virtual Private Network), dès qu'il est dans un cas de mobilité, permettant d'établir une connexion via un canal sécurisé mis à disposition pour tous les collaborateurs internes à Circet.

5. TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

5.1. Responsabilité et devoirs des utilisateurs

Un utilisateur qui accède à ou reçoit des données à caractère personnel, qu'il s'agisse de données relatives aux collaborateurs de Circet ou à des tiers (clients, partenaires, candidats, …), s'engage à respecter strictement le Règlement Général sur la Protection des Données (UE 2016/679) et la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que consignes associées au traitement de ces données.

Le non-respect par Circet de ses obligations issues de la règlementation en matière de protection des données personnelles peut être sanctionné par des amendes pouvant aller jusqu'à 4% du chiffre d'affaires mondial ou 20 000 000 euros, le montant le plus élevé étant retenu. Par ailleurs, les infractions aux dispositions de loi n°78-17 du 6 janvier 1978 sont punies de cinq ans d'emprisonnement et de 300 000 euros d'amende (articles 226-16 et suivants du Code pénal).

5.2. Traitements des données personnelles des utilisateurs

5.2.1. Identification du responsable de traitement

Circet agissant en tant que responsable de traitement, est amenée à collecter les données personnelles

des utilisateurs pour des finalités de gestion :

- administrative du personnel fondée sur l'article 6-1(f) du RGPD, en vertu duquel le traitement est licite s'il est nécessaire aux fins des intérêts légitimes du responsable de traitement,
- de la paie fondée sur les articles 6-1(b) et 6-1(c) du RGPD, en vertu desquels le traitement est licite s'il est nécessaire à l'exécution du contrat auquel la personne concernée est partie ou s'il est nécessaire au respect d'une obligation légale,
- des annuaires internes fondée sur l'article 6-1(f) du RGPD, en vertu duquel le traitement est licite s'il est nécessaire aux fins des intérêts légitimes du responsable de traitement,
- des accès et de la sécurité aux locaux fondée sur l'article 6-1(f) du RGPD, en vertu duquel le traitement est licite s'il est nécessaire aux fins des intérêts légitimes du responsable de traitement, à savoir, la gestion de la sécurité des locaux.

Le délégué à la protection des données personnelles de Circet est Matthieu Mélin, Cabinet Astura, 26 avenue George V, 75008 Paris, adresse email : dpo@Circet.fr.

5.2.2. Destinataires des données personnelles

Les services internes de Circet, notamment le service des ressources humaines, ont accès aux données personnelles. Des destinataires externes peuvent également avoir accès aux données personnelles des utilisateurs. Il s'agit notamment :

- des organismes de sécurité sociale (à l'embauche, la déclaration préalable est établie auprès de l'Urssaf qui transmettra les informations auprès de la CPAM du domicile du salarié. Chaque mois, ainsi qu'à chaque événement (arrêt de travail, fin de contrat de travail), le dispositif de la Déclaration Sociale Nominative (DSN) permet le transfert de toutes les informations sociales nécessaires à l'exercice des droits du salarié),
- les caisses de retraite et de prévoyance,
- de pôle emploi,
- des services des impôts,
- des services de santé au travail.

Afin de mettre en place les traitements mentionnés dans le présent article, Circet a recours à dessous-traitants qui peuvent avoir accès aux données personnelles.

5.2.3. Durée de conservation des données personnelles

Les données personnelles collectées par Circet sont conservées pendant la durée de la relation contractuelle avec l'utilisateur et au-delà, dans la limite des délais de prescription légale applicables. Des durées de conservation différentes pourront, le cas échéant, être appliquées à certaines catégories de données personnelles conformément aux dispositions légales.

5.3. Droits des utilisateurs

Conformément à loi « informatique et libertés » du 6 janvier 1978 modifiée et au Règlement européen n°2016/679/UE du 27 avril 2016, les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification, de limitation, de portabilité et d'effacement relatif à l'ensemble des informations personnelles les concernant, ainsi qu'un droit d'opposition pour motif légitime du traitement de ces données.

L'utilisateur dispose également du droit de définir les directives relatives à la conservation, l'effacement ou la communication de vos données personnelles après son décès. S'il s'agit de directives générales concernant

l'ensemble des données personnelles, celles-ci peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission Nationale de l'Informatique et de Libertés (CNIL). S'il s'agit de directives particulières concernant les données personnelles collectées par Circet, celles-ci sont enregistrées auprès de cette dernière. L'utilisateur peut modifier ou révoquer ses directives à tout moment.

L'utilisateur peut exercer ces droits aux adresses suivantes en contactant le Délégué à la Protection des données de Circet, ou à défaut le service des Ressources Humaines de Circet :

- Délégué à la Protection des Données : dpo@Circet.fr
- Service des Ressources Humaines : service.rh@Circet.fr

L'utilisateur peut également introduire une réclamation auprès de la CNIL.

6. CONTROLE DES RESSOURCES

Conformément à la loi, Circet est responsable de l'utilisation faite par les utilisateurs des ressources duSI mis à leur disposition. Circet se réserve ainsi le droit d'analyser, de limiter et de contrôler l'utilisationdes ressources matérielles et logicielles ainsi que les échanges effectués via ses SI.

Afin d'assurer la sécurité de son SI ainsi que le respect des règles définies et de disposer de données statistiques, Circet peut mettre en œuvre les contrôles suivants :

- **Contrôles automatisés**
  - Le SI s'appuie sur des fichiers journaux (« logs »), créés automatiquement par leséquipements informatiques et de télécommunication. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, endétectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au SI.
  - Les utilisateurs sont informés que des registres sont créés afin de tracer l'activité SI. Le détail des connexions n'est pas examiné mais l'origine/destination des flux et leur volume de données et temps est observé afin de détecter les anomalies ou dysfonctionnements.
  - Les données personnelles relatives à ces activités ne sont pas consultées mais encontrepartie, Circet exige un autocontrôle des utilisateurs basé sur la confiance et la responsabilité individuelle. Cependant pour des raisons de sécurité et d'éthique, des contrôles pourront être effectués ponctuellement.

- **Procédure de contrôle manuel**
  - En cas de dysfonctionnement constaté par la DSI, un contrôle manuel et une vérificationde toute opération effectuée par un ou plusieurs utilisateurs peut être réalisé. Lorsque le contrôle porte sur les données d'un utilisateur et sauf risque ou événement particulier, la DSI ne peut ouvrir les données identifiées par l'utilisateur comme personnels contenus surle disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment contacté.
  - Le contenu des messages à caractère personnel des utilisateurs ne peut en aucun cas êtrecontrôlé par la DSI.
  - En cas de départ d'un utilisateur de Circet, il est de la responsabilité de l'utilisateur d'éliminer toutes les données à caractère personnel des moyens informatiques mis à sa disposition. Les données à caractère non personnel sont considérées comme propriété de l'entreprise. Circet se réserve le droit de librement

accéder et/ou supprimer les documentsou messages personnels résiduels des moyens informatiques mis antérieurement à la disposition de l'utilisateur si aucune manifestation d'intention de les récupérer n'a été émisesous huitaine après le départ.

7. RESPONSABILITE ET SANCTIONS

Il est rappelé que le non-respect des lois et textes applicables en matière de sécurité des SI (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi[1].

[1]
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004
- Dispositions Pénales : Code Pénal (partie législative) : art 226-16 à 226-24 et Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain
- Dispositions pénales : art 323-1 à 323-3 du Code pénal
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)
- Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels
- Disposition pénale : art L.335-2 du Code pénal.
- Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016