Référentiel Qualité, Environnement et Sécurité du SI

PSSI -

Charte utilisateur de bon usage du SI

	Nom(s), Fonctions(s)	Date	Visa
Préparé par	JACQUET Pierre, Directeur Qualité	25/02/2021	✓
Vérification	BERTRAND Pierrick, DRH	25/02/2021	✓
Approbation	FEVRIER François, RSSI, Pilote du processus PSSI	25/02/2021	✓

Référence :	SMI-000261-DOC
Version :	1.4
Etat :	Valide
Confidentialité :	C2 - DIFFUSION CONTROLEE
Date de la dernière mise à jour	14/04/2021
Nombre de pages	17

HISTORIQUE DES MODIFICATIONS

Modèle : SMI-000003-MOD_1.0

Version	Date	Auteur	Nature et origine de la modification
1.0	26/11/2019	JACQUET Pierre	Version initiale
1.1	14/04/2020	JACQUET Pierre	Mise à jour format
1.2	21/01/2021	JACQUET Pierre	Prise en compte de modifications avant diffusion sous Welcome
1.3	25/02/2021	Christophe ILLGEN	Correction objet
1.4	14/04/2021	Christophe ILLGEN	Correction §10.2

DIFFUSION

Diffusion interne
Fonction
Ensemble des collaborateurs du Groupe Astek

Diffusion externe	
Fonction ou Nom	**Société**
Pas de diffusion externe	

SOMMAIRE

1 PRESENTATION DU DOCUMENT

1.1 Objet

Cette charte est assimilable à **« un code de bonne conduite »** » élément de base de la politique de sécurité du système d'information, et présente une valeur règlementaire uniquement pour les dispositions qui sont annexées ou intégrées au règlement intérieur de l'entreprise. Elle définit les bonnes pratiques à adopter par chaque utilisateur du SI de l'Entreprise. Leur bonne application doit contribuer à la préservation de la sécurité du système d'information.

Elle couvre l'ensemble des moyens matériels, logiciels, applications, base de données, réseaux de télécommunications et informatique nomade mis à la disposition de son personnel par le Groupe Astek.

Elle présente également les risques auxquels s'exposent les personnes contrevenantes.

1.2 Domaine d'application

Cette charte s'adresse à tout utilisateur du Système d'Information de l'Entreprise.

1.3 Documents de référence

Documents ayant servi de référence à la rédaction du présent document.

Repère	Titre du document	Référence
P_MDE	Procédure de maîtrise des documents et des enregistrements	SMI-000041-PROC
DR_1	Système de Management de la Sécurité de l'Information	NF ISO 27001
DR_2	Normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management	NF ISO 27002
DR_3	Politique de Sécurité du SI du Groupe Astek	SMI-000054-POL
DR_4	Règlement Intérieur	RI DRH

1.4 Documents associés

Documents auxquels on renvoie dans ce document.

Repère	Titre du document	Référence
/		

1.5 Terminologie et abréviations

Abréviations spécifiques utilisées dans ce document :

Abréviation	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DPO	Data Protect Officer (ou Délégué à la Protection des données) : personne de l'Entreprise en charge de la conformité au Règlement européen sur la protection des données personnelles (RGPD) (NB : à distinguer de la Direction des Projets et des Offres (DPO))
DQS	Direction Qualité et Sécurité
DSI	Direction des Systèmes d'Information
EBI	Expression de Besoin Informatique
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information

Termes particuliers utilisés dans le cadre de ce document :

Terme	Description
Actif	Tout élément représentant de la valeur pour l'Entreprise, notamment l'ensemble des données et des systèmes nécessaires au bon fonctionnement de l'Entreprise ; un actif peut être de l'information, un logiciel, un ordinateur, un service, etc.
Déni de Service	Le déni de service (ou DoS : Denial of Service) est une attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs. Les serveurs de messagerie peuvent être victimes de ces attaques.
Entreprise	Le Groupe Astek et ses filiales.
HelpDesk	Site permettant aux utilisateurs d'interagir (demandes, incidents, etc.) avec le Service Desk. (https://helpdesk.groupeastek.com)
Messagerie électronique	Service mis à disposition du Groupe pour échanger des mails en interne ou vers l'extérieur. La solution actuelle est Office365.
Moyen d'authentification	Moyen mis à disposition par la DSI pour s'authentifier sur son poste de travail ou à un service : compte d'accès, token physique ou logiciel, etc.
Phishing	Technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations sensibles ou personnelles par usurpation de l'émetteur lors de l'envoi d'un mail. Nommée également « hameçonnage ».
Service Desk	Centre d'assistance aux utilisateurs du SI.
Spam	Mail non sollicité envoyé à des fins de publicité ou de démarche commerciale.
Système d'Information	Ensemble des moyens humains, techniques et organisationnels permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et externes de l'Entreprise, quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, graphique, …).
Utilisateur	Toute personne (salarié, sous-traitant, client …) autorisée à accéder, utiliser ou traiter des ressources du Système d'Information de l'Entreprise dans le cadre de son activité professionnelle.
Welcome	Site permettant d'accéder aux procédures de l'entreprise et en particulier aux procédures Qualité et Sécurité (https://welcome.groupeastek.com/)

2 CONTEXTE ET OBJECTIFS

2.1 Contexte

L'Entreprise met en œuvre un Système d'Information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique. La mise à disposition et l'utilisation des moyens informatiques sont indispensables à l'activité de l'Entreprise. Ils améliorent la productivité, la communication et l'efficacité du Groupe.

Tout utilisateur est amené, dans le cadre de son activité pour l'Entreprise à utiliser des moyens informatiques, notamment les équipements bureautiques mis à sa disposition. Certaines applications informatiques lui permettent de manipuler des données numériques très sensibles telles que : données clients, données bancaires et de facturation, données de R&D, données RH, etc.

Aussi, si des précautions essentielles ne sont pas prises, l'Entreprise s'expose à des risques sécuritaires importants, avec des conséquences qui peuvent être fortement dommageables, en termes d'image du Groupe, de chiffre d'affaires ou de respect de la réglementation.

2.2 Les moyens informatiques

On entend par moyen informatique, dans le présent document :

- Un ordinateur fixe ou portable et ses périphériques associés ;
- Un accès à Internet depuis un ordinateur ;
- Un accès au système d'information du Groupe (serveurs, services, etc.) ;
- Un accès distant au système d'information du Groupe (via un VPN) ;
- L'accès aux outils de communication du Groupe (Helpdesk, Welcome, SIMUS, etc.) ;
- Un téléphone fixe ou mobile ;
- Une imprimante / scanner ;
- Un compte d'accès aux services Office 365 (messagerie, espaces partagés, etc.) ;
- Des moyens d'authentification aux différents services.

2.3 Objectifs

Le présent guide a pour objectif de permettre à l'ensemble des collaborateurs et sous-traitants, un usage optimal des moyens mis à leur disposition tout en garantissant la sécurité des systèmes d'information du Groupe Astek.

Ainsi, il contient les bonnes pratiques à respecter par l'ensemble des utilisateurs du SI du Groupe Astek ainsi que les règles de sécurité en vigueur afin de réduire les risques pesant sur celui-ci. Ceci de façon à **faire de chaque utilisateur un acteur essentiel à la préservation de la sécurité du SI du Groupe**.

3 REGLES GENERALES D'USAGE DES MOYENS INFORMATIQUES

3.1 Mise à disposition des moyens informatiques

Les moyens informatiques sont mis à disposition des collaborateurs et des sous-traitants par la DSI du Groupe afin de remplir leur mission pour le Groupe et uniquement à cette fin. Seule la DSI est habilitée à fournir du matériel informatique.

Chaque utilisateur reçoit des moyens informatiques (comptes d'accès, matériel) en relation avec son projet / sa fonction à titre individuel. A ce titre, ils doivent être utilisés uniquement par la personne à qui ils ont été confiés et ne doivent pas être transmis ou cédés à un tiers.

3.2 Accès au système d'information

Seuls les matériels informatiques fournis par la DSI et dûment autorisés peuvent être connectés au réseau interne du Groupe, à l'exception du wifi invité. Toute connexion ou tentative de connexion d'équipements non autorisés est strictement interdite, sauf dérogation validée par le RSSI du Groupe.

3.3 Identifiants et mots de passe

La DSI fournit à chaque collaborateur ou sous-traitant, dès son arrivée, un compte utilisateur constituant un droit d'accès pour :

- La messagerie professionnelle ;
- Le déchiffrement et l'ouverture du poste de de travail (dans le cas où l'utilisateur dispose d'un poste),
- L'accès aux services de base (HelpDesk, Simus, 0365).

Ce droit d'accès est valable pendant tout le temps du contrat du collaborateur ou du sous-traitant.

- Il lui est personnel et incessible.
- Le mot de passe doit être modifié dès de sa première utilisation.
- Le mot de passe doit être renouvelé régulièrement, la fréquence étant définie et revue par le RSSI en cohérence avec les préconisations de l'ANSSI.
- Les mots de passe choisis doivent présenter un taux de robustesse suffisant en cohérence avec les préconisations du RSSI, elles-mêmes basées sur celles de l'ANSSI.

Les identifiants et les mots de passe sont personnels et strictement confidentiels. Ils ne doivent pas être communiqués intentionnellement ou non à un tiers

3.4 Utilisation des moyens informatiques

L'utilisation des moyens informatiques se fait en toute hypothèse :

- Dans le strict respect des principes généraux énumérés par le présent guide ;
- Conformément aux instructions du Service Desk, de la DSI et de la DQS ;
- Dans le respect des lois et règlements en vigueur portant sur les systèmes d'information en France.

Il est ainsi formellement interdit aux utilisateurs du SI :

- D'utiliser tout moyen informatique à des fins contraires à l'ordre public.
- D'envoyer des messages adressés en grand nombre et de manière non sollicitée.

Chaque utilisateur est responsable de l'application des précautions de sécurité définies par le Groupe, pendant la durée de son contrat ou de sa mission.

Chaque utilisateur doit signaler sans délai au Service Desk tout incident de sécurité suspecté ou avéré survenu sur les moyens informatiques mis à sa disposition.

3.5 Utilisation à titre professionnel / privé

Le système d'information et de communication est un outil de travail ouvert à des usages professionnels.
L'Entreprise facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel, mais l'Entreprise tolère l'utilisation à titre privé, dans les conditions décrites ci-dessous :

- L'utilisation est raisonnable, occasionnelle et ne se fait pas au détriment de l'activité professionnelle ;
- L'utilisation se fait dans le respect des lois ;
- L'utilisation se fait en accord avec le contrat de travail (ou de sous-traitance) et le règlement intérieur de l'entité **[DR_4]** ;
- L'utilisation se fait sans but commercial ;
- L'utilisation ne porte pas atteinte à l'image de l'Entreprise.

Les données privées ou personnelles devront être explicitement désignées et il appartient à l'utilisateur de procéder à cet effet. A défaut, elles seront considérées comme données professionnelles. Par exemple : en plaçant les données personnelles dans un dossier « privé » ou « personnel », ou en indiquant « *personnel* » dans le sujet d'un courrier électronique considéré comme privé.
L'utilisateur devra aussi effacer toute donnée personnelle s'il doit rendre les ressources mise à sa disposition (fin de projet, changement de PC) et avant la fermeture de son compte informatique, lors de son départ définitif de l'Entreprise. Un rappel de cette règle sera fait lors du départ de l'Entreprise d'un salarié.

3.6 Confidentialité et protection des données

La protection des données de l'Entreprise et de ses clients face aux menaces de perte, vol ou modification est du devoir de tous. La Direction du Groupe Astek ne peut pas en être le seul garant. L'utilisateur doit évaluer le niveau de confidentialité des données dont il est le propriétaire et utiliser les outils de protections adaptés, dans le cadre des recommandations du Groupe Astek :

- Tout utilisateur s'engage à protéger et à garder strictement confidentiel l'ensemble des informations, données et éléments de propriété intellectuelle classifiés « Confidentiel », « Confidentiel Entreprise » ou « Secret Entreprise », développés ou détenus par l'Entreprise, quel que soit leur support ;
- Tout utilisateur est responsable des accès qu'il donne volontairement sur ses données (droits des fichiers), et se doit de fournir les accès aux documents adaptés au niveau de confidentialité souhaité ;
- Tout traitement portant sur des données à caractère personnel d'un tiers doit faire l'objet d'une déclaration dans le registre des traitements de l'Entreprise (par application du RGPD); cette action étant accompagnée par le DPO du Groupe.

Les actes suivants sont interdits dès lors qu'ils ont été commis sciemment :

- Le détournement volontaire d'informations propres à l'Entreprise (ex : utilisation de données clients à des fins autres que celles prévues dans le cadre de la mission, etc.) ;
- L'utilisation du système d'information dans le but de concurrence déloyale (ex : envoi d'information commerciale à un concurrent, envoi d'offre avant-vente à un concurrent, …) ;
- Le stockage d'information professionnelle (documents de travail, code source, etc.) sur un poste personnel qui n'est pas fourni par l'Entreprise.

A défaut de classification sur l'axe confidentialité, l'actif (donnée, fichier, répertoire, …) devra être considéré comme une donnée de niveau « Confidentiel ».

4 BON USAGE DU POSTE DE TRAVAIL

4.1 Utilisation standard du poste de travail

L'utilisation du poste de travail informatique, et de l'ensemble des périphériques et terminaux associés, implique le respect constant des consignes et procédures de sécurité (authentification par mot de passe, activation de l'anti-virus, etc.), ainsi que du présent guide.

Par défaut, l'utilisateur ne dispose pas des droits administrateurs de son poste. Par dérogation justifiée par un besoin opérationnel fort et validée par le RSSI du Groupe, un second compte d'administration peut être confié à l'utilisateur. Dans tous les cas, aucun utilisateur n'est autorisé à modifier la configuration de son poste de travail, les dispositifs de sécurité (notamment l'anti-virus) et les droits d'accès, sans l'accord préalable du RSSI du Groupe.

Les mise à jour des logiciels et du système d'exploitation sont réalisées automatiquement par la DSI. Il est néanmoins nécessaire de respecter les consignes de la DSI de façon à ce que ces mises à jour puissent être correctement et régulièrement déployées (exemple : ne pas éteindre le poste de travail tel jour, etc.).

Chaque utilisateur doit prendre soin du poste de travail confié et informer le Service Desk de toute anomalie constatée sur celui-ci.

4.2 Utilisation de supports amovibles

Les supports amovibles de données (dont notamment CD-Rom, DVD-Rom, clés USB) constituent un vecteur de transmission de virus et/ou de divulgation d'informations confidentielles à l'extérieur du Groupe.
Chaque utilisateur doit donc être extrêmement vigilant à l'usage et à la protection de ces supports dès lors qu'ils contiennent des données du Groupe quelle qu'en soit leur nature.

Les supports informatiques contenant des informations sensibles (CD Rom, clé USB…) doivent être stockés, dès lors qu'ils sont sans surveillance, dans un meuble ou bureau fermant à clé.

4.3 Utilisation du poste de travail dans les locaux du Groupe Astek

Lorsque vous travaillez dans les locaux du Groupe Astek, les règles suivantes doivent être observées :

- Dans le cas d'un poste de travail portable, attacher le poste à l'aide du câble antivol fourni par la DSI ;
- En cours de journée, verrouiller sa session de travail lorsque le poste de travail n'est plus sous surveillance ;
- Eteindre son poste de travail avant le départ (fin de journée, vacances, déplacement, etc.) sauf en cas de maintenance demandée par la DSI (cf. §4.1). Ainsi les données sont chiffrées et la confidentialité de celles-ci garantie ;

4.4 Utilisation du poste de travail en mobilité

Rappel : chaque utilisateur est responsable du matériel qui lui a été confié par le Groupe Astek. Il est garant de sa protection, en particulier contre le vol.

Lorsque vous êtes en mobilité (déplacement professionnel, télétravail), les règles suivantes doivent être observées :

- Utiliser l'accès distant VPN mis à disposition par la DSI pour vous connecter au SI ;
- Ne pas utiliser de WIFI public sans utiliser l'accès VPN ;
- Ne pas laisser sans surveillance le poste de travail ;
- Lorsque vous travaillez dans un lieu public (train, avion, gare, etc.) utiliser le filtre de confidentialité (si vous n'en n'avez pas, merci de faire une EBI sur le site helpdesk ou par mail à madsi@groupeastek.fr) mis à disposition par la DSI ;
- Arrêter le poste de travail lorsque vous êtes en cours de déplacement et que vous n'utilisez pas celui-ci. (De façon à pouvoir bénéficier du chiffrement des données présentes sur le disque).

5 BON USAGE DES OUTILS DE MESSAGERIE

5.1 Règles générales

Les outils de messagerie (messagerie électronique et messagerie instantanée) sont des outils importants pour l'activité du Groupe. Ils sont également des vecteurs importants de risques d'intrusion ou de fuite de données. Les consignes de sécurité suivantes sont donc particulièrement importantes pour l'intégrité du SI et la protection de l'ensemble des données.

Il est ainsi **interdit aux utilisateurs de transférer les messages professionnels échangés dans le cadre de leur mission sur leur messagerie personnelle**.

Il est recommandé à chaque utilisateur de limiter la communication de l'adresse de messagerie qui lui a été attribuée dans le cadre de sa mission en dehors de tout contexte professionnel. Ceci afin de réduire les risques de Spam, usurpation d'identité, phishing, etc.

5.2 Emission de messages électroniques

Les règles suivantes doivent être appliquées lors de l'envoi d'un mail :

- L'envoi de messages doit être en conformité avec les lois et règlements en vigueur.
- L'envoi de messages à l'ensemble du personnel du Groupe est strictement réservé aux seules personnes habilitées.
- Les messages contenant des informations classifiées de niveau « confidentiel », « confidentiel Entreprise » ou « Secret Entreprise » doivent être transmises de façon chiffrée à l'aide des moyens mis à disposition par le Groupe.
- Les documents explicitement classifiés comme « Confidentiel Entreprise » ou « Secret entreprise » ne doivent pas être communiqués à des personnes externes au Groupe.
- Les fichiers volumineux peuvent être envoyés via le service mis à disposition par la DSI : https://dl.astek.fr.

5.3 Réception de messages électroniques

Il est recommandé à chaque utilisateur :

- De ne pas ouvrir de messages électroniques ou de fichiers joints sans s'être préalablement assuré que cela puisse être fait sans danger et qu'ils aient bien identifié l'expéditeur.
- De ne pas ouvrir et de ne pas transférer tout message d'origine inconnue. Les messages classifiés "SPAM" ou "message indésirable" doivent être scrupuleusement contrôlés avant ouverture. En cas de doute il est préférable de demander assistance au Service Desk.

Chaque utilisateur doit, autant que cela soit techniquement possible, faire en sorte de ne pas recevoir de messages non conformes aux lois et règlements et ils ne doivent pas les relayer.

5.4 Absence

Afin d'assurer la continuité de service en cas d'absence, l'utilisateur doit activer un message d'absence en y précisant les coordonnées de la personne à contacter pendant l'absence ainsi que la fin de la période d'absence.

6 UTILISATION D'INTERNET

6.1 Utilisation depuis le SI du Groupe Astek

Les moyens de contrôle du Groupe enregistrent et vérifient tout le trafic internet entrant et sortant du Groupe, aussi bien local que distant, notamment la messagerie électronique, l'échange de fichiers, la navigation sur Internet.

La plupart des sites non autorisés fait l'objet d'un filtrage par un dispositif régulièrement mis à jour. Sauf dérogation validée par le RSSI du Groupe, l'accès à tout site identifié par les dispositifs de filtrages sera refusé par le dispositif. Les utilisateurs ne doivent pas passer outre les dispositifs de filtrage et plus généralement tout dispositif de sécurité mis en place sur les moyens informatiques du Groupe.

Ainsi, il est totalement interdit de naviguer volontairement sur des sites ou d'échanger des contenus portant sur des propos déviants ou polémiques tels que : Pédopornographique, Pornographie, Racisme, Incitation à la violence, Prosélytisme, Propos diffamatoires ou discriminatoires, ou portant atteinte à la vie privée ou aux droits des personne.

6.2 Réseaux sociaux

Il est demandé à chaque utilisateur d'adopter un comportement loyal envers l'Entreprise et ses clients lors de l'utilisation des réseaux sociaux, que ces réseaux soient professionnels ou non professionnels.

7 UTILISATION DU SMARTPHONE

Il est autorisé de consulter sa messagerie professionnelle depuis son smartphone personnel.

Nous vous demandons d'appliquer les recommandations de sécurité suivantes :

- Verrouiller votre session automatiquement à l'aide d'un mot de passe ou empreinte ;
- Signaler un incident de sécurité en cas de perte ou de vol de votre smartphone. (De façon à ce que la DSI puisse notamment réinitialiser les accès à votre compte).

8 UTILISATION DE MOYEN INFORMATIQUE PERSONNEL

Il est interdit de connecter tout moyen informatique personnel ou tiers au réseau interne du Groupe, sauf dérogation accordée par le RSSI.

Il est cependant autorisé d'accéder, depuis l'extérieur et à l'aide d'un poste personnel, aux sites et services accessibles en mode web depuis l'extérieur (Office365, Simus, Welcome, etc.).

9 CONTACTS ET PROCESSUS UTILES

Besoin	Contexte	Processus
Signaler un incident de sécurité	Chacun doit être vigilant et signaler tout constat, tentative ou soupçon de violation d'une ressource du système d'information (vol, mail frauduleux, etc.)	Utilisation du formulaire « *SSI - Signalement Incident Sécurité* » depuis Helpdesk Envoyer un mail à securite@groupeastek.fr
Demander une dérogation	L'exercice de votre activité n'est pas compatible avec l'application des Politiques de sécurité	Utilisation du formulaire « *SSI - Demande de Dérogation* » depuis Helpdesk
Contacter le RSSI	Vous avez besoin de contacter le RSSI pour signaler un évènement ou demander des informations liées à la Sécurité du SI	Envoyer un mail à RSSI@groupeastek.fr

10 SURVEILLANCE, CONTROLE ET NON-RESPECT

10.1 Surveillance et contrôle

Dans le respect des principes de transparence et de proportionnalité, l'attention des utilisateurs est attirée sur le fait que les dispositifs de sécurité informatique (pare-feu, système de contrôle…) mis en place par l'Entreprise enregistrent les traces d'activité des systèmes, rendant possible leur analyse a posteriori. L'objectif de ces traces est d'assurer un bon niveau de sécurité et de pouvoir mener une investigation en cas de détection d'un incident de sécurité ou d'un incident de disponibilité.

10.1.1 Contrôles automatiques

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées, bloquées et conservées les données relatives :

- A l'utilisation des logiciels applicatifs mis en place par l'Entreprise et géré par la DSI de l'Entreprise ou un de ces prestataires, afin de contrôler les accès, les modifications, les suppressions de fichiers et le caractère licite des logiciels,
- Aux connexions entrantes et sortantes aux réseaux internes, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie (spam, accès depuis un lieu exotique, …) et surveiller les tentatives d'intrusion ou de fuite d'information et les activités, telles que la consultation de sites web ou le téléchargement de fichiers,
- Aux connexions vers les réseaux clients pour surveiller toute tentative d'intrusion et les activités telles que l'accès aux ressources clients,
- Aux échanges de données à travers des périphériques amovibles (clés USB, disques durs…) ;
- Aux comportements malveillants sur les actifs fournis par l'Entreprise (ex : réalisation de scan de vulnérabilité, tentative d'attaque de type Déni de Service, …),
- Aux entrées dans les bâtiments de l'Entreprise par l'intermédiaire d'un lecteur de badge d'accès.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leurs activités et leurs échanges sur le SI. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements et pour assurer la sécurité, dans le respect des règles en vigueur.
Les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai de 6 mois après leur enregistrement.
L'ensemble de ces données seront accessibles uniquement par les membres de l'équipe DSI de l'Entreprise.

10.1.2 Contrôles manuels

En cas d'incident de disponibilité ou de sécurité impactant l'Entreprise ou un de ses clients, un membre de l'équipe DSI (mandaté par la Direction) peut procéder à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs. Par contrôle manuel, nous entendons des actions de recoupement de logs réalisés par une personne et non par un outil.
Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition, sur le réseau de l'Entreprise ou sur sa messagerie. La Direction ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la représentativité du personnel qu'en présence de l'utilisateur ; celui-ci ayant été dûment appelé et éventuellement représenté par un représentant du personnel sauf accompagné d'un officier de la police judiciaire.

10.2 Non-respect

L'Entreprise ne pourra pas être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se serait pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrits dans la présente charte.

En cas de non-respect des règles définies dans la présente charte, l'entreprise pourra limiter les usages par mesure conservatoire.

Par ailleurs, les personnels encourent des sanctions disciplinaires en cas de violation des dispositions législatives, règlementaires et statutaires en vigueur définies dans le Règlement Intérieur **[DR_4]**, ainsi que d'éventuelles poursuites prévues par la législation en vigueur.