



CHARTRE D'UTILISATION DU SYSTEME D'INFORMATION DE L'ENTREPRISE

Table des matières

I.	Définitions	3
II.	Objet de la Charte d'utilisation du Système d'Information	4
III.	Champ d'application.....	5
1.	Utilisateurs concernés	5
2.	Système d'information et de communication.....	5
IV.	Usage des Ressources	5
1.	Règles générales et déontologiques.....	5
2.	Usage professionnel	7
3.	Usage privé ou non professionnel	7
V.	Règles spécifiques	8
1.	Internet.....	8
2.	Stockage de données / Fichiers / Intranet.....	8
3.	Messagerie électronique.....	9
4.	Matériel informatique.....	10
5.	Logiciels et bases de données.....	10
VI.	Procédure à respecter en cas de perte ou de vol d'un équipement.....	11
VII.	Absence et départs des Utilisateurs.....	11
1.	Gestion des absences (congrés, arrêt de travail, ...).....	11
2.	Gestion des départs	11
VIII.	Sécurité / Accès aux Ressources	12
IX.	Travail en mobilité.....	14
X.	Confidentialité.....	14
XI.	Données personnelles / Droit des Utilisateurs	15
XII.	Mesures de contrôle	15
XIII.	Sanctions	16
XIV.	Contacts	16

I. Définitions

Cellule Assistance : désigne l'équipe concernée par les demandes d'assistance réalisées par les Utilisateurs.

Charte : désigne la présente charte d'utilisation du Système d'information de l'Entreprise.

CNIL : désigne la Commission National de l'Informatique et des Libertés.

D2ID : désigne la Direction de l'Informatique et de l'Innovation Digitale.

Données personnelles : désigne toute information se rapportant à une personne physique identifiée ou identifiable.

Données sensibles : désigne les données de l'Entreprise ou d'un de ses clients, partenaires ou fournisseurs pour laquelle sa divulgation entraînerait un impact significatif sur le plan financier, stratégique, juridique ou en termes d'image pour l'Entreprise ou son client.

L'Entreprise : désigne la société de production GSF concernée.

EDR : Désigne le logiciel permettant la détection et la protection des serveurs et postes de travail contre les menaces de sécurité informatique.

Intranet : Désigne l'espace en ligne interne permettant à l'entreprise de de partager des documents ou des informations privées.

Logiciels métiers : désigne les logiciels spécifiques/techniques mis à disposition de l'Entreprise pour exercer l'activité professionnelle liée à l'Utilisateur (exemple : HR Access).

Ressources : désigne l'ensemble des équipements nécessaires à la connexion au Système d'Information.

RGPD : Désigne le Règlement Général sur la Protection des Données UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

RSSI : désigne le Responsable de la Sécurité des Systèmes d'Information.

SSI : Désigne la Sécurité des Systèmes d'Information.

Système d'information : désigne l'ensemble des processus, ressources organisationnelles, matérielles et logicielles, permettant d'acquérir, générer, traiter, stocker, diffuser et/ou détruire des informations au sein de l'Entreprise, quel que soit leur format (électronique, papier, oral, etc.).

Utilisateur : désigne toute personne habilitée, dans le cadre de ses missions, à accéder aux ressources informatiques ou de télécommunication de l'Entreprise. Il s'agit donc de tout collaborateur, quel que soit son site de rattachement, sa fonction ou son mode de connexion aux ressources de l'Entreprise (local ou distant).

VPN : désigne Virtual Private Network, soit réseau privé virtuel.

II. Objet de la Charte d'utilisation du Système d'Information

L'Entreprise met à la disposition de tous les Utilisateurs de son Système d'Information un ensemble de ressources informatiques (postes de travail, smartphones, espaces collaboratifs, applications métier, etc.) ainsi que des informations et des données nécessaires à l'accomplissement de leurs missions.

Pour faire face à une menace omniprésente, l'Entreprise définit, par le biais de cette Charte :

- / Ses enjeux de sécurité dont la protection des données de ses clients et de ses salariés ;
- / Les règles d'usage et de sécurité que l'ensemble des Utilisateurs s'engage à respecter au quotidien ;
- / Les mesures de contrôles de la bonne application de cette Charte par les Utilisateurs ;
- / Les sanctions disciplinaires en cas de manquement aux règles définies ;
- / Les obligations de l'Utilisateur lors de son départ ;
- / Les droits des Utilisateurs liés au traitement de leurs données à caractère personnel.

L'Entreprise encourage fortement l'utilisation d'outils de travail performants et à la pointe des nouvelles technologies, notamment parce qu'ils concourent à l'amélioration de la qualité et de la productivité du travail.

Néanmoins si leur utilisation est détournée de sa destination professionnelle au sein de l'Entreprise, ces outils peuvent causer des dommages engageant la responsabilité, non seulement du salarié Utilisateur mais aussi de son employeur. Chacun doit donc être conscient des responsabilités qui lui incombent et des risques qu'il fait encourir à l'Entreprise du fait d'une utilisation inappropriée de l'outil informatique, ainsi que des ressources du réseau Internet et de l'Intranet.

Par ailleurs, l'usage de la messagerie électronique interne ou externe, la participation à des forums, l'accès à ou le téléchargement d'éléments textuels, photographiques, audio ou vidéo sont susceptibles de mobiliser de manière substantielle les capacités du réseau et des postes de travail. Ces actes peuvent perturber l'utilisation par les autres membres du personnel de cet outil de travail et par voie de conséquence l'activité de l'Entreprise.

C'est pourquoi la présente Charte entend fixer les règles nécessaires et adaptées de conduite générale, et préciser de manière transparente les responsabilités des Utilisateurs, notamment en termes de sécurité, confidentialité, respect des lois et règlements et bon usage, tout en préservant le Système d'Information, et en respectant les droits et libertés de chacun.

Elle pourra être complétée par des procédures d'application pratique.

III. Champ d'application

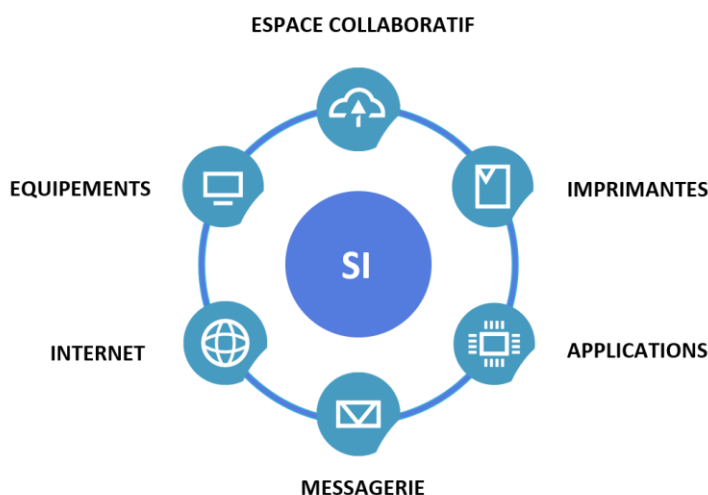
1. Utilisateurs concernés

La présente Charte s'applique de plein droit à tous les Utilisateurs autorisés par l'Entreprise et qui utilisent le Système d'Information mis à leur disposition, que cette utilisation se fasse en accès local, à distance par l'utilisation d'un modem ou au travers d'un réseau informatique, ainsi que des ressources extérieures accessibles via les réseaux informatiques mis à leur disposition.

2. Système d'information et de communication

Chaque Utilisateur détient un accès au Système d'Information de l'Entreprise.

Cela concerne l'accès et l'usage des outils suivants :



Remarque : l'item « Applications » inclut tous les services Office 365.

IV. Usage des Ressources

1. Règles générales et déontologiques

L'Utilisateur est amené à utiliser plusieurs Ressources dans le cadre professionnel ou non-professionnel. Certaines règles sont à respecter dans ces deux cas.

L'Utilisateur doit notamment s'assurer que ces actions soient conformes avec les réglementations en vigueur (Loi Informatique et Liberté, RGPD,...).

Il est par ailleurs rappelé qu'aucun fichier ne pourra contenir d'éléments à caractère pornographique, pédophile, révisionniste, offensant, diffamatoire, injurieux, discriminatoire, raciste, ou contraire à l'ordre public et aux bonnes mœurs.

Ainsi que tout élément révélant une quelconque appartenance politique, syndicale ou religieuse. Plus largement, tous traitements de Données sensibles qui ne trouveraient pas de fondement dans le cadre des fonctions de l'Utilisateur sont interdits.

De plus, chaque Utilisateur s'engage à respecter les règles de déontologie informatique et notamment à ne pas effectuer toutes opérations visant à nuire à une personne physique ou à l'Entreprise, notamment, sans que cette liste soit exhaustive :

- / De télécharger des fichiers (musique, vidéo, autre ...) sans autorisation préalable des administrateurs,
- / De se connecter ou essayer de se connecter sur un site à caractère pornographique, pédophile ou révisionniste, ou tout site dont le contenu est contraire à l'ordre public et aux bonnes mœurs.
- / De rédiger des messages électroniques ou fichiers, y compris relevant de l'utilisation privée, comprenant des éléments de nature offensante, diffamatoire, injurieuse, raciste, discriminatoire, pédophile, pornographique ou pouvant être assimilés à du harcèlement ou violant le secret professionnel ou contraires au respect de l'intimité de la vie privée ou contraires aux dispositions de la Loi du 29 juillet 1881 sur la liberté de la presse, et ce, tant à l'égard des autres Utilisateurs de l'Entreprise que de tout tiers extérieur à l'Entreprise.
- / De tenter de lire, de copier, de divulguer ou de modifier les fichiers, et les messages, d'un autre Utilisateur sans y avoir été explicitement autorisé, même si ces données ne sont pas protégées.
- / De masquer sa véritable identité,
- / De s'approprier le mot de passe d'un autre Utilisateur,
- / De tenter d'intercepter des communications entre tiers,
- / De porter atteinte à l'intégrité d'un autre Utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants : les données véhiculées et mises sur le réseau à l'initiative des Utilisateurs du réseau doivent être licites. A ce titre, les Utilisateurs doivent respecter l'ensemble des dispositions légales,
- / De connecter un PC simultanément au réseau téléphonique et au réseau informatique de l'Entreprise,
- / De divulguer des informations pouvant porter préjudice à l'Entreprise, à des tiers quels qu'ils soient (partenaires, fournisseurs, clients, tout autre tiers) y compris d'autres Utilisateurs de l'Entreprise non habilités à les recevoir,
- / De participer, sans autorisation expresse de la Direction, à des forums non professionnels pouvant engager la responsabilité de l'Entreprise, via Internet.
- / De nuire de quelque façon que ce soit à l'image de marque de l'Entreprise par une utilisation frauduleuse ou illicite concourant au dénigrement ou au détournement de clientèle.

Ceci concerne notamment des opérations qui pourraient avoir pour conséquences :

- / De modifier ou de détruire intentionnellement des informations sur un des systèmes connectés au réseau,
- / D'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau,
- / De causer des dommages à l'Entreprise ou à tout tiers et/ou engager la responsabilité de l'Entreprise.

- / La réalisation d'un programme informatique ou son utilisation visant à nuire à une personne physique ou à l'Entreprise est également interdite.
- /

2. Usage professionnel

L'utilisation du Système d'Information n'est autorisée que dans le cadre exclusif de l'activité professionnelle des Utilisateurs, conformément à la législation en vigueur.

L'accès au système d'information de l'Entreprise est donc fourni à chacun des Utilisateurs le nécessitant pour l'exercice de leur activité professionnelle et il appartient à chacun d'adopter un comportement professionnel et responsable.

3. Usage privé ou non professionnel

Les usages des Ressources à des fins non professionnelles sont tolérés, mais ils doivent demeurer exceptionnels, sous la responsabilité exclusive de l'Utilisateur, et à conditions :

- / Qu'il ne nuise pas aux performances et bon fonctionnement des Ressources,
- / Qu'il ne nuise pas aux missions de l'Utilisateur,
- / Qu'il ne soit pas contraire à la législation et à l'éthique,
- / Qu'il respecte les limites prévues par l'administration (ex. l'URSSAF, CNIL) et par l'employeur : cet usage doit être « raisonnable » et « réservé aux besoins ordinaires de la vie privée et familiale »,
- / Qu'il soit fait mention de la notion de "Personnel" ou "Privé" lorsque l'Utilisateur souhaite user des Ressources professionnelles à des fins privées, de manière à prévenir la D2ID de la nature particulière s'attachant à cette messagerie.

Les équipements ayant été exonérés de rémunération pour copie privée, les salariés ne doivent pas faire usage de ceux-ci à des fins de copie privée pour la reproduction d'œuvres littéraires ou artistiques.

En cas d'usage privé abusif (du fait de la fréquence des messages reçus et/ou envoyés, du volume des données échangées, du type-taille-format des pièces jointes, du transfert de messages professionnels, de copie, de reproduction d'œuvres, etc ...), ou contraire aux dispositions légales ou en cas d'utilisation abusive ou malveillante de la mention "privé" ou "personnel", l'Entreprise sera en droit d'en tirer toutes les conséquences sur le plan disciplinaire et/ou judiciaire.

Les abus qui pourraient être constatés par la D2ID seront sanctionnés dans le cadre des dispositions du paragraphe XIII de la présente Charte.

V. Règles spécifiques

La mise à disposition d'outils informatiques n'implique pas que les collaborateurs de l'Entreprise sont joignables à n'importe quel moment de la journée ou de la semaine. Chaque Utilisateur équipé d'un terminal de l'Entreprise conserve son « droit à la déconnexion » et l'ensemble des Utilisateurs doit respecter le droit à la vie privée de chacun. Hors périodes d'astreintes et heures normales de travail, le défaut de réponse d'un Utilisateur ne pourra en aucun cas lui être reproché.

1. Internet

La consultation de sites web sur Internet ne doit pas gêner de façon significative la bonne marche du travail des autres Utilisateurs.

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

La D2ID peut limiter la durée de consultation, imposer des configurations de sécurité, des limites de taille au téléchargement ou filtrer des contenus dans le souci de protection du Système d'Information.

L'intrusion ou la modification non autorisée de sites externes ainsi que la captation d'informations confidentielles sont strictement interdites.

Il est précisé que, dans le cadre de sa mission de protection du Système d'Information, la D2ID exerce un contrôle sur les sites les plus visités.

Une consultation ponctuelle et dans les limites raisonnables du web, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'organisation est tolérée. Toutefois cette navigation ne devra pas entraver l'accès professionnel, ni gêner la bonne marche du travail de l'Utilisateur.

2. Stockage de données / Fichiers / Intranet

Les informations appartenant à l'Entreprise ne doivent être stockées que sur les supports et matériels prévus à cet effet. Outre les lecteurs disponibles sur tout ordinateur fourni par l'entreprise, d'autres espaces de stockage sont accessibles sur le réseau interne ou depuis l'environnement Office 365.

Ces espaces tels que l'environnement Office 365, l'Intranet ou les serveurs de fichiers permettent le partage de documents professionnels en interne ou pour certains d'entre eux, le stockage de documents professionnels confidentiels.

Les nouveaux outils mis à disposition des Utilisateurs de l'Entreprise, notamment des applications de la suite Office 365 (OneDrive, Teams, Sharepoint...) offrent des possibilités de synchronisation.

Les Utilisateurs s'assurent d'utiliser ces fonctionnalités selon les règles définies par la D2ID. Les espaces de stockage communs (serveurs de fichiers, outils collaboratifs, Intranet, etc.) sont réservés à un usage professionnel.

En conséquence, les documents et fichiers stockés dans ces espaces ne peuvent être utilisés à des fins non professionnelles ou pour de tierces personnes.

De même, l'Utilisateur s'engage à ne pas aller consulter des données qui ne seraient pas nécessaires à l'exécution de ses propres missions.

L'Utilisateur ne doit pas utiliser les différents espaces de stockage commun pour stocker et/ou partager tout fichier, donnée ou autre qui ne serait pas strictement professionnel.

L'Utilisateur doit veiller à restreindre l'accès à ses fichiers (ex. : partage Windows de répertoire ou OneDrive) aux Utilisateurs strictement nécessaires.

3. Messagerie électronique

Compte tenu de son extrême facilité d'utilisation, une attention toute particulière doit être portée à la rédaction et à la diffusion d'un message électronique (E-mail). Le message électronique peut engager la responsabilité de l'Entreprise et peut être reconnu par un tribunal comme preuve valable pour établir un fait ou un acte. En cas d'émission vers l'extérieur de l'Entreprise, l'émetteur ainsi que la société doivent pouvoir être clairement identifiés.

L'usage de la messagerie (envoi et réception de messages) ne devra pas gêner le trafic normal en termes de volume des messages échangés, de taille des messages échangés, et de format des pièces jointes. La participation à une chaîne d'E-mail est proscrite.

La diffusion d'annonces personnelles est possible, dans certains cas tolérés par la Direction.

a. Contenu du message électronique

Sur le fond :

Les messages électroniques expédiés devront respecter les droits des tiers, conformément aux dispositions énoncées à l'article IV « Usage des Ressources ».

Sur la forme :

Les messages électroniques doivent respecter les règles d'usage pour toute communication écrite, étant rappelé qu'ils peuvent être lus par d'autres que leurs destinataires. Il est ainsi recommandé :

- d'en mentionner l'objet de façon suffisamment explicite ;
- de ne les adresser qu'aux personnes réellement concernées par le sujet, et corrélativement de limiter l'utilisation des adresses " groupées ", a fortiori de proscrire toute diffusion de messages " en chaîne " ;
- de ne pas joindre inutilement de fichiers attachés ;
- d'utiliser les outils de compression pour les fichiers volumineux ;

La D2ID peut limiter le format, le type et la taille des messages électroniques.

L'Utilisateur doit en particulier veiller au bon usage des documents à fort contenu graphique.

Tout message d'origine douteuse ou inconnue doit être signalé à la D2ID conformément aux procédures en vigueur.

b. Règles de conservation de la messagerie

La taille des boîtes aux lettres est limitée.

L'Utilisateur est averti lorsque sa boîte se rapproche de la saturation. Il est de la responsabilité de l'Utilisateur d'archiver les messages importants si besoin et supprimer les messages inutiles.

A saturation, l'Utilisateur ne pourra plus ni émettre, ni recevoir de message.

c. Contrôle de la messagerie

La D2ID pourra effectuer des contrôles techniques sur l'utilisation de la messagerie dans l'Entreprise. A ce titre, il pourra établir des statistiques sur le nombre, l'origine et la destination de messages reçus et envoyés, par poste, service ou établissement.

En cas d'anomalies relevées par la D2ID, celle-ci pourra demander des explications aux personnes concernées.

4. Matériel informatique

Des équipements professionnels sont mis à disposition par l'Entreprise à tous ses collaborateurs en ayant le besoin pour accéder à son Système d'Information (PC pro, smartphone pro ...).

La connexion de tout autre équipement (équipement réseau, serveurs ...) non fourni par la D2ID doit faire l'objet d'une demande d'autorisation à cette dernière avant accès au réseau interne (demande à la Cellule Assistance via la création d'un SOS).

Par ailleurs, seule la D2ID est autorisée à acquérir et à mettre en œuvre de nouveaux moyens informatiques (matériels et logiciels). En cas de besoins exprimés par un Utilisateur pour un nouveau matériel ou logiciel, il devra demander l'autorisation préalable à son responsable hiérarchique. La Cellule Assistance se chargera de son acquisition et de son installation selon les procédures en vigueur. Cette disposition vise en particulier à respecter les règles relatives au droit d'auteur (licences logicielles), mais concerne aussi les logiciels gratuits.

Le matériel informatique, par essence coûteux et fragile, doit être manipulé avec soin.

En fin de journée, les ordinateurs portables laissés au sein des locaux de l'Entreprise doivent être enfermés à clé dans des bureaux, dans un placard fermant à clé, ou sécurisés de manière adéquate de toute autre façon.

Chaque Utilisateur est informé que l'assurance exclut de sa garantie le vol ou la disparition du matériel informatique survenu dans des véhicules automobiles et s'engage à ne pas les laisser, sans surveillance, à l'intérieur d'un véhicule.

L'Utilisateur veillera, également, lors de ses déplacements, à ne pas mettre son ordinateur portable dans la soute à bagages, et d'une manière plus générale, à ne pas le confier à un tiers.

L'Utilisateur aura soin de ne pas exposer, par négligence, le matériel informatique, mis à sa disposition, à des détériorations telles que poussières dues à des travaux, liquide renversé, exposition aux intempéries, etc...

Il est rappelé que tout matériel informatique sortant du parc informatique de l'Entreprise aux fins de rachat par un Utilisateur ou issu d'un don doit être préalablement " nettoyé " des logiciels et données, propriété de l'Entreprise.

Les Smartphones et Tablettes sont des moyens d'accès aux données et systèmes de l'entreprise, de ce fait, ils doivent être considérés comme des PCs, et bénéficier des mêmes précautions d'utilisation.

5. Logiciels et bases de données

Les logiciels et bases de données sont, comme les autres œuvres de l'esprit (écrit, musique, photo, etc...) protégés par le droit d'auteur, et le droit des Producteurs de bases de données (Code de la Propriété Intellectuelle).

Sont également protégées les marques, y compris les logos. En cas de violation de ces dispositions, l'Utilisateur et l'Entreprise s'exposent à des sanctions civiles et pénales.

De tels agissements peuvent notamment consister en :

- / Téléchargement d'œuvres littéraires, cinématographiques, musicales ou photographiques ;
- / Téléchargement de logiciels, l'utilisation de logiciels sans licence ou en infraction avec les conditions prévues par la licence ;
- / Extraction de données ainsi que leur réutilisation ou mise à disposition, par tout moyen et sous quelque forme que ce soit ;
- / Reproduction, modification et/ou l'utilisation de toute marque sans l'autorisation de son titulaire.

La législation interdit à tout Utilisateur de faire, directement ou indirectement, des copies de logiciels quel qu'en soit l'usage. Les copies de sauvegardes sont la seule exception. Elles doivent être effectuées dans les conditions prévues par le code de la Propriété Intellectuelle. Les copies illicites constituent un délit de contrefaçon engageant la responsabilité de l'auteur. La D2ID se réserve la possibilité d'effacer du Système d'Information toute trace de ces fichiers et œuvres introduites dans le Système, en violation des droits de propriété intellectuelle d'autrui.

VI. Procédure à respecter en cas de perte ou de vol d'un équipement

L'Utilisateur doit apporter une vigilance constante vis-à-vis de ses équipements, et ce particulièrement dans les lieux publics.

En cas de perte ou de vol, il est impératif d'informer le supérieur hiérarchique et de suivre les démarches décrites dans les procédures en vigueur en cas de perte ou de vol d'un équipement informatique de l'Entreprise.

VII. Absence et départs des Utilisateurs

1. Gestion des absences (congés, arrêt de travail, ...)

Afin d'éviter que des informations soient inaccessibles durant l'absence d'un des Utilisateurs salariés de l'Entreprise et si les données ne sont pas stockées dans des espaces partageables, la Direction se réserve la faculté de s'arroger, via la D2ID, les moyens d'authentification de l'Utilisateur et d'accéder aux ressources mises à sa disposition et ce, dans la seule fin d'assurer la continuité de l'activité et dans le respect de la vie privée de l'Utilisateur.

En outre, la Direction se réserve le droit de demander à la D2ID la suspension temporaire des droits et accès de l'Utilisateur durant le temps de son absence et ce, afin de s'assurer que le droit à la déconnexion de ce dernier soit réellement exercé.

2. Gestion des départs

Avant son départ de l'Entreprise, l'Utilisateur est tenu de restituer en bon état, toutes les informations, matériel et équipements informatiques qui lui ont été confiés.

Le droit d'accès de l'Utilisateur au Système d'Information sera supprimé. Il sera transféré si nécessaire vers un autre Utilisateur pour des raisons de service, après notification à la D2ID par la Direction ou le Service concerné.

Dans le cadre de son départ de l'Entreprise, l'Utilisateur devra :

- / S'assurer de la capitalisation de l'ensemble des données à caractère professionnel en sa possession sur les espaces collaboratifs ou les supprimer si ces dernières ne sont pas nécessaires à la continuité des services de l'Entreprise, y compris sur les équipements personnels (pour rappel, les données professionnelles appartiennent à l'Entreprise et ses clients) ;
- / Supprimer l'ensemble des données personnelles présentes sur son poste de l'Utilisateur et les partages de fichiers ;
- / Restituer l'ensemble du matériel et des équipements informatiques qui lui ont été fournis, notamment :
 - Badge (le cas échéant)
 - Poste de travail
 - Smartphone professionnel
 - Clés USB
 - Accessoires (sac à dos, claviers, souris, etc.)

L'ensemble des informations contenues sur son poste de travail ainsi que les répertoires associés sur les serveurs de fichiers seront récupérés par l'Entreprise. Par ailleurs la boîte aux lettres de cet Utilisateur sera fermée et les mails reçus après son départ seront rejetés.

VIII. Sécurité / Accès aux Ressources

L'Utilisateur doit respecter toutes les consignes de sécurité diffusées par la D2ID. Il doit signaler immédiatement, à la Cellule Assistance, toute anomalie dans le fonctionnement du Système d'Information, notamment en ce qui concerne la messagerie ou la connexion à l'Intranet et à l'Internet. Il est responsable des dommages que sa négligence pourrait causer au Système d'Information. À tout moment chaque Utilisateur peut suivre l'évolution de sa demande de signalement d'anomalie auprès de la Cellule Assistance, et peut donc avoir accès à sa demande, ainsi qu'à son traitement, jusqu'à la clôture.

a. Usage sécurisé du Système d'Information et gestion des incidents de sécurité

L'Entreprise dispose d'une politique de gestion de incidents de sécurité et d'un processus de gestion de crise. La politique concerne l'ensemble des équipements matériels, applicatifs, logiciels, réseaux et systèmes du Système d'Information de l'Entreprise. Elle concerne également les personnes en charge de la sécurité du Système d'information et l'Utilisateur. Ce périmètre comprend :

- L'ensemble des postes de travaux Windows, sédentaires ou portables, autonomes ou intégrés au domaine ;
- Les serveurs internes tels que les serveurs de fichiers, serveurs applicatifs, serveurs de messagerie interne, serveurs d'infrastructure, serveurs d'administration, ...

- Les serveurs périmétriques tels que les passerelles de messagerie (serveurs SMTP) et passerelles Internet (proxys Web ...)
- Les équipements mobiles communiquant avec internet tels que les Smartphones et tablettes

La politique s'applique lors d'une panne ou anomalie suite à une intervention humaine ou logique. Elle s'applique également en cas d'alertes via un moyen de détection logique de vulnérabilité (antivirus...).

En tant que premier relais de la sécurité informatique de l'Entreprise, l'Utilisateur peut faire face à des événements de sécurité et doit être à même de réagir en conséquence, ainsi :

- Si l'Utilisateur pense que ses mots de passe ont été utilisés
- Si le PC de l'Utilisateur commence à agir de manière suspecte
- Si l'Utilisateur rencontre un comportement informatique suspect ou un logiciel défectueux
- Si le PC de l'Utilisateur ou son smartphone est perdu ou volé

Il doit respecter les procédures mises en place par la D2ID et contacter l'équipe SSI selon les différents canaux disponibles listés dans la procédure en vigueur.

b. Les logiciels de sécurité

L'Utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement du Système d'Information, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus.

L'Utilisateur ne doit pas empêcher le bon fonctionnement des logiciels de sécurité (EDR, anti-virus ...) sur son poste de travail et Smartphone.

c. Connexion au Système d'Information (ressources et services)

L'utilisation du Système d'Information de l'Entreprise est réservée aux activités propres à chaque service pour mener les missions qui lui sont confiées.

Le droit d'accès est temporaire, personnel et incessible, il disparaît lorsque l'Utilisateur quitte l'Entreprise. Chaque Utilisateur est responsable de l'utilisation qui en est faite.

Il est rappelé que le Système d'Information mis en place permet d'identifier avec certitude chaque Utilisateur.

En règle générale, il est du ressort de la hiérarchie (Responsables opérationnels et Directeurs) de signaler à l'Administrateur désigné, toute modification intervenant au niveau du droit d'accès d'un Utilisateur telles que :

- / Création, suppression ou transfert temporaire du droit d'accès (absence, congés, ...) ;
- / Modification de fonction entraînant une modification du droit d'accès ; etc...

L'Utilisateur doit veiller à ne pas laisser accéder à son terminal une personne non autorisée (par verrouillage de l'écran avec mot de passe ou par fin de session) en particulier lors des interruptions de service ou en fin de journée, sauf demande expresse de la D2ID.

Le Service Informatique peut mettre en place les stratégies permettant de renforcer l'efficacité du mot de passe qui seront diffusées sous la forme de consignes de sécurité.

IX. Travail en mobilité

Il appartient à l'employeur de fournir aux collaborateurs en télétravail placés sous son autorité, l'accès aux outils numériques nécessaires (matériel bureautique, accès aux serveurs professionnels, messageries et logiciels métiers) pour pouvoir exercer leur activité et communiquer avec leur supérieur hiérarchique ainsi que leur collectif de travail et les usagers, le cas échéant. L'Entreprise assure la maintenance et l'entretien des équipements et outils informatiques mis à la disposition de l'Utilisateur.

L'Utilisateur en télétravail doit disposer d'un espace de travail adapté à un bon usage permettant l'installation dans des conditions sécurisées du matériel professionnel mis à sa disposition par l'Entreprise.

Cet espace doit être doté d'un accès à internet compatibles avec l'activité professionnelle.

Lorsque l'Utilisateur se trouve dans un tiers lieu, c'est-à-dire un espace partagé / public de télétravail, qui se distingue des lieux à usage privé depuis lesquels il est habituellement autorisé à télétravailler, celui-ci doit se conformer aux règles suivantes :

- Éviter de partir en déplacement avec des Données sensibles ;
- Privilégier l'accès aux Données sensibles via des connexions sécurisées plutôt qu'un stockage sur les équipements nomades (ordinateur portable, téléphone mobile, etc.) ;
- Éviter autant que possible la consultation de documents sensibles depuis des lieux publics et doter les équipements (ordinateur, tablette, téléphone) d'un filtre de confidentialité ;
- Éviter de se connecter aux réseaux non maîtrisés (Wi-Fi d'hôtel, de gare ou de café, bornes de recharge en libre-service, salle de réunion extérieure, etc.) et garder son VPN actif ;

Lors des déplacements en transport, à l'étranger ou chez des tiers, une vigilance particulière s'impose. Les Utilisateurs doivent notamment respecter les mêmes règles que celles dans les tiers-lieux.

L'Utilisateur peut se rapprocher du RSSI de l'Entreprise pour des services complémentaires en vue d'un déplacement professionnel à l'Etranger.

X. Confidentialité

Les degrés de confidentialité des informations auxquels sont confrontés nos collaborateurs influencent fortement les mesures à prendre lors de la création, de la réception ou plus généralement de la transmission et le stockage de ces informations.

Pour permettre à chacun d'identifier rapidement le niveau de sensibilité d'un document, il est important de le marquer visuellement (classer).

Par défaut tout document est considéré comme « Interne », c'est-à-dire accessible, partageable, modifiable et stockable seulement par des Utilisateurs le requérant dans le cadre de leurs fonctions, encadrées par un contrat.

L'accès par les Utilisateurs aux informations et documents conservés sur le Système d'Information est limité aux fichiers attachés à leur poste de travail et aux fichiers publics ou partagés. Cette règle s'applique également aux conversations privées de type messagerie électronique dont l'Utilisateur n'est pas destinataire, ni directement, ni en copie.

Malgré les sécurités, la confidentialité des informations diffusées via les Ressources ne peut être assurée. Les informations très confidentielles ne doivent donc pas être transmises par ces moyens. Pour les transmissions internes, les informations confidentielles pourront être protégées par les options de protection par mot de passe intégrées dans les outils bureautiques (Word, Excel, ...). L'utilisation d'autres moyens de chiffrement notamment de logiciels spécifiques, est interdite sauf accord expresse de la D2ID.

XI. Données personnelles / Droit des Utilisateurs

L'Utilisateur dispose d'un :

- Droit d'accès : l'Utilisateur a le droit de demander à l'Entreprise si ses données à caractère personnel sont utilisées dans un ou plusieurs traitements et d'y accéder.
- Droit de rectification : l'Utilisateur a le droit de demander la modification de ses données à caractères personnel inexacts ou incomplètes.
- Droit à l'effacement : l'Utilisateur a le droit de demander l'effacement de ses données à caractère personnel. Il est cependant à noter que, dans certains cas, ses données à caractère personnel ne pourront pas être supprimées (par exemple, si elles sont nécessaires à la gestion de son contrat, si une obligation réglementaire ou légale oblige l'Entreprise à les conserver, etc.)
- Droit d'opposition : l'Utilisateur a le droit de s'opposer à tout moment à l'utilisation de ses données à caractère personnel aux fins d'un ou plusieurs traitements. Le responsable du traitement ne les traitera plus, à moins qu'il n'existe des motifs légitimes ou pour l'exercice ou la défense de droits en justice.
- Droit à la portabilité des données : l'Utilisateur a le droit de demander à recevoir les données à caractère personnel qu'il a fournies. Elles lui seront adressées.
- Droit à la limitation du traitement : l'Utilisateur a le droit de demander, dans certains cas spécifiques, la suspension du traitement portant sur une ou plusieurs de ses données à caractère personnel.

Pour plus d'informations : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3>

Conformément au RGPD, chaque Utilisateur peut exprimer ses demandes d'exercice de droits cités ci-dessus sur simple demande transmise à l'adresse suivante : dpo@gsf.fr.

Chaque Utilisateur a également la possibilité d'introduire une réclamation auprès de la CNIL.

XII. Mesures de contrôle

Chacun des Utilisateurs doit s'assurer que l'usage des moyens mis à sa disposition s'effectue dans le respect des règles de sécurité, de confidentialité, de bonnes mœurs et dans le respect des lois et règlements. Chacun des Utilisateurs est responsable de l'usage fait.

L'ensemble des services utilisés génère, à l'occasion de leur emploi, "des fichiers de traces". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements constatés.

Ces fichiers conservent des informations par exemple concernant la messagerie (expéditeur, destinataire, date), mais aussi heures de connexion aux applications de gestion, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc.

Ce type de traces existe pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord de la Direction, ces fichiers peuvent être mis à la disposition ou transmis à la justice.

Les Utilisateurs sont avertis que la D2ID peut avoir accès à l'ensemble des composants du Système d'Information à n'importe quel moment et ce afin d'en effectuer tout acte de contrôle, ou de protection, d'identifier toute fraude et d'assurer au mieux la sécurité et le bon fonctionnement de son réseau.

La D2ID, pourra, si les circonstances l'exigent et sous respect des dispositions légales et jurisprudentielles applicables, de la confidentialité, du droit à la vie privée de chacun, et du principe du contradictoire, analyser toute activité effectuée par le biais du Système d'Information, notamment utilisation des ressources matérielles et logicielles, échanges via le réseau, ainsi que toute activité relative à l'usage du Système d'Information.

XIII. Sanctions

L'Entreprise se réserve le droit de suspendre à tout moment, après avoir averti l'Utilisateur afin que ce dernier puisse dupliquer, le cas échéant, ses fichiers personnels, l'accès au Système d'Information (sites Internet notamment) en cas d'inobservation des présentes règles par l'Utilisateur, et de bloquer à tout moment, et sans avertissement préalable, l'accès aux sites dont le contenu est jugé illégal ou offensant.

L'application de la présente Charte est obligatoire pour tous les utilisateurs du Système d'Information. En cas de violation des règles listées dans ce document :

- L'Utilisateur de l'Entreprise s'expose aux sanctions décrites dans le règlement intérieur de l'Entreprise eu égard à la gravité des faits reprochés et/ou à leurs conséquences, et proportionnées au préjudice subi ou qui aurait pu être subi par l'employeur.
- L'Utilisateur s'expose également, le cas échéant, à des poursuites pénales, la Direction étant habilitée à prendre toute mesure pour veiller au respect des présentes et lutter contre les fraudes.

XIV. Contacts

Les règles de sécurité précisant les principes de ce Code sont définies dans les référentiels et procédures de protection de l'information et de la sécurité des systèmes d'Information. Elles sont consultables sur l'Intranet de l'Entreprise.
