CHARTE INFORMATIQUE A l'ATTENTION DES UTILISATEURS EXTERNES



SOMMAIRE

1 **Introduction**

Introduction à la charte Informatique

Périmètre d'application

Tous Responsables

Communication

2 **Règles**

Protection des identifiants

Règles de bonne conduite

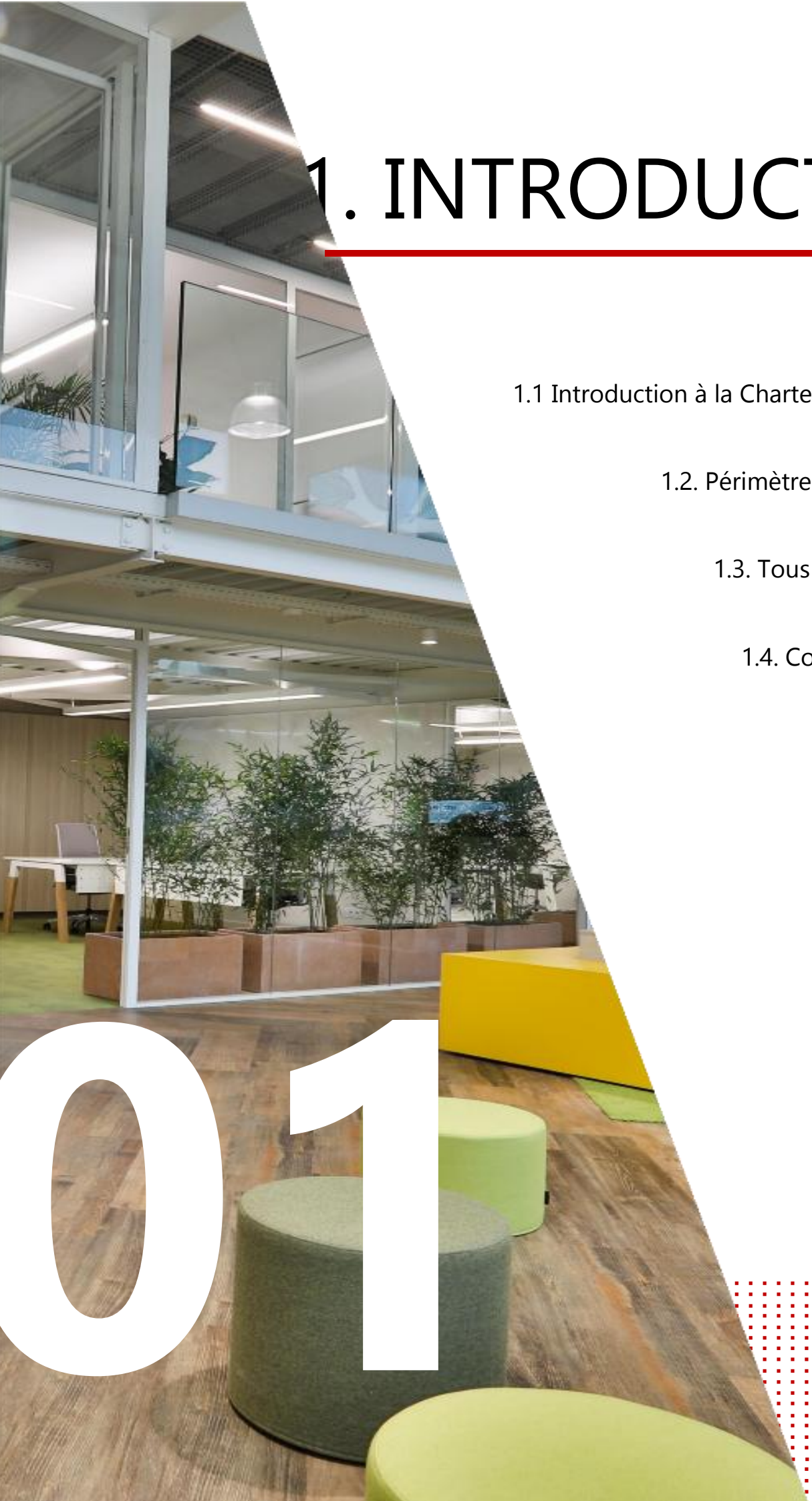
Règles relatives à l'arrivée d'un Utilisateur externe

Règles relatives au départ d'un Utilisateur externe

Les prestataires informatiques externes

Modalités d'utilisation des données professionnelles, privées et à caractère personnel

3 **Signature**



1. INTRODUCTION

1.1 Introduction à la Charte Informatique

1.2. Périmètre d'application

1.3. Tous responsables

1.4. Communication

01

1.1. Introduction à la charte informatique

GSE met en œuvre un système d'information nécessaire à l'exercice de son activité et au travail de ses collaborateurs GSE et des utilisateurs externes (sous-traitants, prestataires, clients). L'entreprise met à disposition les moyens informatiques, techniques et humains, délivre le matériel, les logiciels, les réseaux, les données et le support requis à leur utilisation.

À travers son environnement informatique, la volonté du Groupe GSE est de favoriser le bien-être au travail, la productivité, l'efficacité opérationnelle ainsi que l'innovation et la transformation digitale de l'entreprise.

C'est dans ce contexte que le Groupe GSE assure aux utilisateurs externes que les informations sont traitées, protégées et sauvegardées dans un système d'information sécurisé, robuste et mis à jour qui respecte la législation en vigueur et les règles sur la protection des données personnelles.

En complément, le Service DSI définit les principes d'utilisation, la politique de sécurité informatique, les bonnes pratiques et les règles de conduite que les utilisateurs externes doivent s'approprier et respecter. Il s'engage également à fournir la formation et la documentation nécessaires à l'utilisation du système d'information.

Seul le Service DSI est autorisé à installer les logiciels et les ressources informatiques qui demeurent la propriété exclusive du Groupe GSE. L'utilisateur externe s'engage à avoir un usage responsable du matériel mis à disposition et à le restituer sur simple demande ou à la fin de son contrat.

Les équipements informatiques et les droits d'accès au système d'information sont attribués en fonction des besoins et des missions et peuvent être modifiés ou retirés à l'utilisateur externe à partir du moment où le contexte ne l'exige plus.

L'exfiltration et l'exportation de données ou logiciels appartenant au Groupe GSE à des fins personnelles ou sur un support qui n'est pas fourni par le Service DSI sont strictement interdites. Le Service DSI se donne le droit d'auditer, de collecter et de sauvegarder toutes les transactions contrevenant à ce principe.

En accord avec la politique éthique du Groupe GSE, les données à usage privé sont strictement interdites pour tout utilisateur externe. Le Service DSI se réserve le droit de désactiver les identifiants et les accès à tout utilisateur externe contrevenant à cette règle.

1.2 Périmètre d'application

La charte informatique à l'attention des utilisateurs externes s'applique à la société GSE, société par actions simplifiée immatriculée au RCS d'AVIGNON sous le numéro 488 862 368, dont le siège social est situé Parc d'activité de l'aéroport, 310 Allée de la Chartreuse, 84140 AVIGNON, ainsi qu'à toutes ses filiales appartenant au même groupe (le « Groupe GSE »).

Cette charte informatique constitue une déclaration formelle des engagements du Groupe GSE, de leur mise en œuvre et de leur communication pour ce qui concerne son domaine d'application. Elle est complétée par plusieurs annexes spécifiques qui définissent ses orientations et ses règles sur des thématiques précises.

1.3 Tous responsables

La présente charte s'applique à toute personne utilisateur externe collaborant avec GSE quel que soit le type de mission (consultants externes, prestataires externes, fournisseurs, pilotes de chantier, sous-traitants informatiques, …) et quel que soit le lieu.

Elle ne saurait se substituer aux lois et règlements applicables.

La charte informatique précise les bonnes pratiques, les devoirs et obligations de tout utilisateur externe dans l'intérêt du Groupe GSE en la matière.

Dans la mise en œuvre de ces règles, tout utilisateur externe doit faire preuve de bon sens et de probité.

Par une bonne connaissance de celles-ci, chaque utilisateur externe doit pouvoir déterminer le moment où les limites de ces règles sont proches d'être franchies, et où il lui devient nécessaire de prendre conseil auprès de son responsable interne GSE ou du Service DSI.

1.4 Communication

L'information de la charte informatique fait partie intégrante de l'accueil des utilisateurs externes.

Toute entreprise ou tout prestataire externe se verra informé de l'existence de cette charte informatique si elle est susceptible d'avoir recours/et ou accès au système d'information, aux matériels, équipements et ou réseaux informatiques du Groupe GSE.

Tout nouvel utilisateur externe se voit remettre, lors de son arrivée dans l'entreprise, un exemplaire de cette charte informatique.

Chaque utilisateur externe s'engage à en prendre connaissance et en respecter les termes.

Les modifications et adjonctions éventuellement apportées à la présente charte feront l'objet de procédures de consultation, de communication et de publicité identiques à celles appliquées à son élaboration.

La présente charte est entrée en vigueur le 29 mai 2026.



2. Règles

2.1. Protection des identifiants

2.2. Règles de bonne conduite

2.3. Règles à l'arrivée d'un Utilisateur externe

2.4. Règles au départ d'un Utilisateur externe

2.5. Les Prestataires informatiques externes

2.6. Modalités d'utilisation des données

02

2.1. Protection des identifiants

Pour garantir la sécurité des systèmes d'information du Groupe GSE, il est impératif de gérer soigneusement les identifiants de connexion.

Chaque utilisateur externe se voit attribuer des identifiants de connexion professionnels, qui sont destinés exclusivement à l'accès aux systèmes d'information, aux réseaux internes et aux applications professionnelles.

Toute utilisation et/ou divulgation inappropriées des identifiants peuvent exposer le Groupe GSE à des risques de sécurité et de confidentialité.

Ces identifiants doivent être protégés et ne doivent jamais être partagés pour prévenir tout accès non autorisé.

Protéger ses identifiants :

2.1.1. Ne jamais divulguer, partager ou confier ses identifiants/mots de passe de connexion et d'accès avec qui que ce soit,

2.1.2. Utiliser des mots de passe complexes et les changer régulièrement conformément aux règles établies par la sécurité informatique,

2.1.3. Participer aux formations et sensibilisations organisées par l'entreprise pour reconnaître et prévenir les tentatives de phishing et d'usurpation d'identité,

2.1.4. Ne pas utiliser ses identifiants de connexion personnels pour accéder aux ressources professionnelles,

2.1.5. Ne pas utiliser ses identifiants de connexion professionnels pour accéder à des sites et applications à des fins et usages personnels,

2.1.6. Signaler immédiatement à l'équipe de sécurité informatique

- Tout dysfonctionnement, toute activité suspecte ou toute compromission des identifiants de connexion,
- Toute perte, tout vol ou toute compromission suspectée ou avérée soit d'un équipement stockant des données professionnelles, soit de ses informations d'authentification (identifiant, mot de passe, code pin, etc.),
- Toute tentative de phishing et d'usurpation d'identité.

2.1.7. Verrouiller sa session ou se déconnecter des systèmes lorsqu'on ne les utilise pas ou plus.

2.1.8. Ne pas inscrire de manière accessible ses identifiants/mots de passe sur quelque support que ce soit.

2.1.9. Ne jamais demander les identifiants/mots de passe à un collègue ou à un autre utilisateur.

2.1.10. Ne pas tenter de déchiffrer, découvrir ou s'approprier les identifiants/mots de passe d'un autre utilisateur.

2.2 Règles de bonne conduite

INTRODUCTION

Définir des règles claires de bonne conduite est essentiel pour plusieurs raisons :

- Elles permettent de sécuriser les systèmes d'information en prévenant les actions non autorisées et les comportements négligents ou non avertis pouvant causer des failles de sécurité.
- Elles garantissent la conformité aux lois et réglementations en vigueur, notamment en matière de protection des données personnelles et de respect du droit de la propriété.
- Elles favorisent un environnement de travail harmonieux et productif en établissant des comportements attendus et en réduisant les risques de conflits ou de malentendus entre les utilisateurs.
- Elles sensibilisent et responsabilisent les utilisateurs sur l'importance de la sécurité informatique, contribuant ainsi à protéger les actifs numériques de l'entreprise.

LES BONNES PRATIQUES

2.2.1. Usage limité de l'Impression : N'imprimer des documents que si cela est absolument nécessaire pour réduire les coûts et l'empreinte écologique.

2.2.2. Gestion des impressions : Ne pas laisser de documents imprimés dans les bacs de réception des imprimantes pour éviter les pertes ou les indiscrétions.

2.2.3. Respect du système d'information : Ne pas perturber intentionnellement le fonctionnement du système d'information.

2.2.4. Respect de la vie privée : Ne pas porter atteinte aux droits des personnes et à leur vie privée par l'utilisation inappropriée des ressources informatiques.

2.2.5. Paramétrage des postes de travail : Ne pas modifier les paramètres du poste de travail sans autorisation afin de maintenir la cohérence et la sécurité des configurations.

2.2.6. Installation de Logiciels : Ne pas installer et désinstaller de logiciels propriété de GSE ou non sans l'autorisation préalable du Service DSI.

2.2.7. Propriété des Logiciels : Ne pas copier les logiciels appartenant au Groupe GSE pour une utilisation non professionnelle.

2.2.8. Gestion des systèmes Partagés : Ne pas interrompre ni mettre hors tension un système partagé sans une raison valable et l'autorisation appropriée.

2.2.09. Usage des réseaux : Ne pas utiliser les réseaux informatiques, notamment Internet pour télécharger du contenu illégal ou à des fins non professionnelles.

2.2.10. Respect des Licences : Ne pas utiliser de logiciels sur des équipements GSE pour lesquels les licences d'utilisation n'ont pas été acquises par le Groupe GSE.

2.2.11. Vol ou perte de matériel : Communiquer immédiatement au Service DSI toute perte ou tout vol d'un poste de travail, d'un téléphone, tablette ou dispositif de stockage d'informations au Service DSI. Déposer une plainte auprès des autorités de police ou gendarmerie.

2.2.12. Utilisation des Équipements fournis : Privilégier l'accès aux applications et aux données du Groupe GSE à partir des équipements professionnels fournis par le Service DSI (postes de travail, iPads, téléphones portables).

2.2.13. Copie de Données : Toute copie de données sur un support externe de type USB qui n'est pas fourni et pas géré par le Service DSI est interdite.

2.3 Règles relatives à l'arrivée d'un utilisateur externe

INTRODUCTION

Dès son arrivée, l'utilisateur externe doit disposer des moyens informatiques nécessaires pour débuter efficacement son travail dans le Groupe GSE.

Bien accueillir un nouvel utilisateur externe passe ainsi par la mise à disposition de son matériel, le paramétrage de ses comptes et les accès aux différentes applications et ressources informatiques du Groupe GSE ainsi qu'une sensibilisation et formation aux bonnes pratiques.

PROCESSUS D'ARRIVÉE D'UN UTILISATEUR EXTERNE

Le processus débute par l'envoi d'un message de la part du responsable interne GSE au Service DSI.

Cette demande contient obligatoirement les informations concernant la date de début et de fin du contrat, les renseignements concernant les accès aux ressources informatiques et le nom du responsable interne GSE.

Suivant le profil de l'utilisateur externe, le Service DSI peut alors préparer et fournir pour le jour d'arrivée les éléments suivants :

2.3.1. Matériel Informatique :

- Préparation du PC (installation des OS et logiciels standards).
- Fourniture d'un écran supplémentaire, tablette, et téléphone professionnel.

2.3.2. Création de Comptes et configuration des droits d'accès :

- Création du compte utilisateur Windows.
- Création de l'adresse de messagerie professionnelle et configuration des outils de collaboration (Microsoft Teams, etc.).
- Configuration des droits d'accès aux espaces de documents partagés.
- Configuration des droits d'accès au réseau du Groupe GSE.

2.3.3. Configuration des Logiciels et Applications :

- Installation des logiciels spécifiques (ex. : suite bureautique, outils de gestion de projet, etc.).
- Paramétrage et configuration des droits d'accès aux différentes applications métiers (CRM, ERP, etc.) en fonction du poste et des responsabilités de l'utilisateur externe.

Règles

Le Service DSI met à disposition du nouvel utilisateur externe des guides d'utilisation et de la documentation.

Des sessions de formation aux différents équipements et applications ainsi qu'une sensibilisation aux bonnes pratiques de cybersécurité sont organisées régulièrement.

Le Service DSI dispose d'un système centralisé d'assistance et de support accessibles à tous, dont les nouveaux arrivants, permettant ainsi d'ajuster les besoins qui auraient été oubliés au moment de l'arrivée de l'utilisateur externe.

2.4 Règles relatives au Départ d'un utilisateur externe

INTRODUCTION

Le respect de ces règles permet d'assurer une transition fluide et sécurisée pour le Groupe GSE.

L'utilisateur externe bénéficie de droits de protection de ses données personnelles et doit respecter ses devoirs de confidentialité et de restitution de matériel.

Le Groupe GSE, pour sa part, garantit la transparence du processus tout en sauvegardant les intérêts, la sécurité de l'entreprise et la continuité de service.

LES DROITS ET LES DEVOIRS DE L'UTILISATEUR EXTERNE

2.4.1. Droits de l'utilisateur externe :

- **Accès aux Données Personnelles :** L'utilisateur externe a le droit d'accéder et de disposer de ses données personnelles conformément à la réglementation en vigueur.
- **Information sur le Processus :** L'utilisateur externe a le droit d'être informé du processus de départ, incluant les étapes et les attentes du Groupe GSE.

2.4.2. Devoirs de l'utilisateur externe :

- **Restitution du Matériel :** L'utilisateur externe est tenu de restituer tout matériel fourni par le Groupe GSE (PC, téléphone, écran, tablette, etc.) en bon état de fonctionnement. Tout dommage ou perte doit être signalé et tout frais de réparation ou remplacement qui résulteront d'une négligence ou mauvaise utilisation pourront le cas échéant être mis à la charge de l'utilisateur externe ou de la société qui l'emploie.
- **Confidentialité :** L'utilisateur externe doit respecter la confidentialité des informations du Groupe GSE même après son départ en lien avec les accords de confidentialité qui le lient ou qui lient son employeur.
- **Non-Exfiltration des Données :** Il est strictement interdit pour l'utilisateur externe d'exfiltrer des données du Groupe GSE.

Le Groupe GSE se donne le droit de poursuivre en justice tout l'utilisateur externe ou son employeur contrevenant à ces principes.

LES DROITS ET LES DEVOIRS DU GROUPE GSE

2.4.3. Droits du Groupe GSE :

- **Audit des Transactions :** Le Groupe GSE se réserve le droit d'auditer, de collecter et de sauvegarder toutes les transactions suspectes de contrevenir à la politique d'exfiltration de données. Le référent éthique est informé de la démarche.
- **Récupération des Matériels :** Le Groupe GSE a le droit de récupérer tous les matériels fournis à l'utilisateur externe et de vérifier leur état de fonctionnement.
- **Collecte des Données :** Le Groupe GSE peut collecter des données pour vérifier le respect des politiques de l'entreprise, pour rassembler des preuves à des fins d'investigations et pour assurer la continuité d'activité.
- **Accès informatique :** Le Groupe GSE peut bloquer totalement ou partiellement les accès informatiques de l'utilisateur externe si celui-ci contrevient aux règles.

2.4.4. Devoirs du Groupe GSE :

- **Information et Transparence :** Le Groupe GSE doit informer l'utilisateur externe du processus de départ et des attentes concernant la restitution des matériels et la gestion des données.
- **Protection des Données Personnelles :** Le Groupe GSE doit s'assurer que les données personnelles de l'utilisateur externe sont protégées et traitées conformément à la réglementation en vigueur.
- **Protection des données privées :** Toute donnée privée d'un utilisateur externe est interdite sur le système d'information GSE. En cas de non-respect de cette règle, le Service DSI supprime les données privées.

LE PROCESSUS DE DÉPART D'UN UTILISATEUR EXTERNE

2.4.5. Notification de Départ :

- A l'expiration du contrat liant l'utilisateur externe au Groupe GSE, le responsable interne GSE confirme la date de départ au Service DSI.
- En parallèle à cela, à la date du départ, les identifiants de l'utilisateur externe ont déjà été automatiquement désactivés et ses accès supprimés.
- Le Service DSI prend contact et communique les prochaines étapes à l'utilisateur externe.

2.4.6. Restitution des Matériels :

- L'utilisateur externe et le Service DSI s'accordent sur une date de restitution.
- Le Service DSI fournit la fiche de restitution de matériel à l'utilisateur externe.
- L'utilisateur externe restitue tout le matériel fourni par le Groupe GSE.
- Le Service DSI vérifie l'état du matériel une fois restitué.

AUDIT ET SÉCURISATION DES DONNÉES

2.4.7. Les accès informatiques de l'utilisateur externe sont bloqués et ses comptes sont désactivés immédiatement après son dernier jour de travail. Les bases de données, annuaires d'entreprise, et autres systèmes d'information sont mis à jour.

2.4.8. Les emails de l'utilisateur externe sont redirigés vers une adresse générique où le responsable interne GSE peut assurer le suivi des communications.

2.4.9. Après le départ de l'utilisateur externe, les données professionnelles sont sauvegardées pendant 3 mois et ensuite détruites sauf demande spécifique du responsable interne GSE.

2.4.10. Le Service DSI peut collecter et procéder à un audit des transactions de l'utilisateur externe pour s'assurer qu'aucune donnée n'a été exfiltrée. Ces données sont conservées pour une période maximale de 2 ans à compter de la date de départ de l'utilisateur externe. Le référent éthique est informé de la démarche.

2.4.11. L'utilisateur externe devra avoir supprimé ses données personnelles du matériel avant la date de restitution de celui-ci.

2.5 Les prestataires informatiques externes

INTRODUCTION

Les prestataires informatiques externes ont pour rôle de fournir des compétences, services ou ressources IT afin d'assurer le bon fonctionnement, la sécurité et l'évolution du système d'information du Groupe GSE.

Leurs interventions se déclinent selon plusieurs axes :

- **Maintenance Préventive et Curative :** Garantir la pérennité des équipements et logiciels par des actions préventives et curatives.
- **Sécurité des Systèmes :** Protéger les données contre les intrusions, perte et corruption.
- **Support et conseils Utilisateurs :** Apporter assistance, formation et support technique aux utilisateurs du Groupe GSE.
- **Développement et Innovation :** Mettre en place de nouvelles solutions technologiques pour améliorer les processus métiers.

Il est donc nécessaire de définir les rôles, droits et responsabilités des prestataires informatiques externes dans la gestion du système d'information du Groupe GSE.

2.5.1. Droits et devoirs des prestataires informatiques externes

2.5.1.1. Droits des prestataires informatiques externes :

- **Accès Temporaire :** Accès limité et temporaire aux systèmes nécessaires pour leur mission, avec surveillance et autorisation préalable.
- **Clarté Contractuelle :** Droits et missions définis clairement dans des contrats de service (SLA - Service Level Agreement).
- **Accès à l'Information :** Accès aux informations nécessaires pour l'exécution de leurs tâches, dans le respect de la confidentialité et des conditions contractuelles.

2.5.1.2. Devoirs des prestataires informatiques externes :

- **Confidentialité Contractuelle :** Respecter les clauses de confidentialité stipulées dans le contrat de service.
- **Respect des Instructions :** Suivre les instructions spécifiques et les protocoles de sécurité du Groupe GSE.
- **Non-Divulgation :** Ne divulguer aucune information relative aux systèmes et données du Groupe GSE à des tiers non autorisés (cf. Document Non Disclosure Agreement disponible au sein de la direction juridique).
- **Rapport et Documentation :** Fournir des rapports détaillés de leurs interventions et des travaux réalisés.
- **Engagement Qualité :** Respecter les niveaux de service définis dans les SLA, incluant les délais de réponse et de résolution.
- **Formation au Contexte :** Se former et s'informer sur les spécificités et des politiques du Groupe GSE.

2.6 Modalités d'utilisation des données professionnelles, privées et à caractère personnel

INTRODUCTION

Il convient de faire la distinction entre les données professionnelles, les données privées, et les données à caractère personnel.

Les données et documents professionnels comprennent toutes les informations, fichiers, courriels et communications qui sont produits, reçus ou utilisés dans le cadre de l'activité professionnelle. Cela inclut les documents relatifs aux projets, aux clients, aux fournisseurs, aux utilisateurs externes, aux collaborateurs internes GSE, ainsi que toute autre information liée à l'activité de l'entreprise. Elles sont la propriété exclusive du Groupe GSE.

Une donnée privée correspond à toute informations appartenant à un utilisateur externe, et exclusivement à celui-ci, et qui n'est pas liée à son activité professionnelle au sein du Groupe GSE. Cela peut inclure des courriels, des photos, des fichiers et toute autre donnée de nature privée.

Une donnée à caractère personnel correspond à toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement (1). Une donnée à caractère personnel peut être de nature professionnelle ou privée.

Cette distinction est cruciale pour garantir une utilisation appropriée et sécurisée des ressources numériques par les utilisateurs externes du Groupe GSE.

[1] Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse électronique, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc. (Source CNIL)

GESTION DES DONNÉES PROFESSIONNELLES

- Respecter la réglementation et la législation en vigueur sur la protection des données à caractère personnel.

- Ne pas stocker des informations pouvant impacter le fonctionnement et la sécurité informatique du Groupe GSE.

- Stocker les données et documents professionnels sur les espaces fournis par le Service DSI du Groupe GSE.

- Le Service DSI met en place un système pour restaurer les données et documents professionnels dans les cas où ils auraient été supprimés, altérés ou perdus.

- Ne pas copier, synchroniser ou transférer des données et documents professionnels sur un espace qui n'a pas été mis à disposition par le Service DSI du Groupe GSE.

- Ne pas accéder, modifier ou supprimer des données et documents professionnels sans y avoir été préalablement habilité.

- Ne pas partager les données des salariés, clients, fournisseurs et autres tiers du Groupe GSE avec des organismes extérieurs non habilités ou avec des personnes non habilitées.

- Ne pas accéder, modifier ou supprimer des données d'un autre utilisateur. Ces données sont considérées comme strictement confidentielles.

- Ne pas transférer et sauvegarder des données ou informations d'expériences professionnelles antérieures ou de cursus scolaires ou universitaires sur le système d'information du Groupe GSE.

- En cas d'absence prolongée, le Service DSI met à disposition du Groupe GSE les données et documents professionnels stockés sur son ordinateur et sur le réseau pour éviter toute interruption de service.

INTERDICTION DE STOCKER DES DONNÉES « PRIVÉES »

Les règles à respecter dans le cadre des données privées sont les suivantes :

- Stocker ou traiter des données privées est strictement interdit sur du matériel (PC, téléphone, tablette) ou sur les zones de stockage fournis par GSE.

- Tout contrevenant à cette règle se verra retirer les accès au SI GSE et devra remettre le matériel mis à sa disposition.

GESTION DES DONNÉES À CARACTÈRE PERSONNEL

Les règles à respecter dans le cadre de l'usage des données à caractère personnel sont les suivantes :

- Respecter la réglementation et la législation en vigueur sur la protection des données à caractère personnel.

- Limiter les traitements (2) des données à caractère personnel aux seuls traitements nécessaires à l'exécution des missions de l'utilisateur, et uniquement à ceux-là.

- Limiter la collecte des données à caractère personnel aux seules données nécessaires à la réalisation des missions de l'utilisateur.

- Contribuer à la protection des données à caractère personnel en adoptant une attitude responsable vis-à-vis de leur traitement.

- Contribuer au respect de la vie privée et des droits et libertés des personnes concernées par les traitements de données à caractère personnel, et faciliter l'exercice des droits de ces mêmes personnes.

- Consulter pour avis le délégué à la protection des données du Groupe GSE avant toute mise en production d'un nouveau traitement.

- Prévenir sans délai le délégué à la protection des données du Groupe GSE en cas de constatation, ou de toute suspicion, d'une violation (3) de données à caractère personnel. En cas de violation avérée, contribuer à en identifier l'étendue et les impacts éventuels pour les personnes concernées. Le référent éthique est informé de l'événement.

- Prévenir le délégué à la protection des données du Groupe GSE si un traitement de données à caractère personnel dont GSE est responsable n'est pas, ou ne semble pas, conforme au règlement général sur la protection des données (4). Le référent éthique est informé de la démarche.

[2] Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé. Par exemple : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement. Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions (source CNIL).

3 Une violation de données survient lorsque les données dont GSE est responsable subissent un incident de sécurité qui entraîne une violation de la confidentialité, de la disponibilité ou de l'intégrité (source UE).

4 Règlement (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.



3. Signature

03

3. Signature

Je soussigné(e) _____, déclare avoir lu attentivement la Charte informatique des utilisateurs externes mise à ma disposition.

J'en accepte pleinement les termes et m'engage à respecter l'ensemble des règles, obligations et bonnes pratiques qui y sont définies.

Je reconnais qu'en cas de non-respect de celles-ci, l'organisation pourra prendre toute mesure jugée nécessaire, conformément aux dispositions légales et aux procédures internes en vigueur. »

Date : ____ / ____ / _____

Signature précédée de la mention « Lu et approuvé »

