

Annexe I au Règlement Intérieur du groupe ESDI

La présente Charte informatique régit notamment l'utilisation du système d'information, la sécurité de ce système et la protection des données.

La présente Charte informatique détaille notamment les points suivants :

- 1.** La bonne utilisation du système est de la responsabilité de tous. Cette bonne utilisation vise avant tout à assurer la sécurité de l'outil de travail de la société.
- 2.** Tout constat de vol ou disparition de matériel, ainsi que de faille informatique ou acte malveillant, doit être immédiatement rapporté.
- 3.** Tous les mots de passe et login (ordinateur, compte, téléphone) sont strictement personnels.
- 4.** Il est interdit d'utiliser ou d'installer des logiciels dans le cadre de l'utilisation du Système d'Information.
- 5.** Il est interdit de connecter des supports informatiques provenant de l'extérieur, notamment clef USB, au Système d'Information.
- 6.** Il est interdit d'utiliser les réseaux sociaux ou de participer à des forums via le Système d'Information.
- 7.** Le matériel et l'ensemble du Système d'Information sont par principe réservés à un usage exclusivement professionnel.
- 8.** Les règles de la présente Charte informatique s'appliquent également dans le cadre de l'intervention sur les réseaux de nos clients.
- 9.** Le matériel appartient à l'entreprise et demeure sa propriété.
- 10.** En cas d'atteinte aux règles et principes rappelés par la présente Charte ou issus du droit applicable, la responsabilité juridique de l'Utilisateur pourra être engagée et des mesures disciplinaires prises.

La lecture exhaustive de cette Charte s'impose à tous.

Le respect de la présente Charte est obligatoire et engage la responsabilité de chacun.

Contenu

1	Généralités	3
1.1	Présentation générale	3
1.2	Administrateur du Système d'Information.....	4
1.3	Avis du Comité Economique et Social	4
2	Définition du Système d'Information	4
3	La protection du Système d'Information	4
3.1	Accès, mots de passe et sécurité	4
3.2	Les pare-feux.....	5
3.3	Contrôle et maintenance par l'Administrateur.....	5
3.4	Introduction de Matériels et Logiciels	5
3.5	Alertes	6
4	L'accès et l'intervention sur les réseaux de nos clients	6
5	L'usage du matériel informatique et des éléments du Système d'Information	7
6	La messagerie	8
6.1	Adresse électronique.....	8
6.2	Message électronique et pouvoirs internes	8
6.3	Contenu du message électronique	8
6.4	Protection des Informations	8
6.5	Règles de conservation de la messagerie.....	9
6.6	Utilisation privée de la messagerie.....	9
7	La navigation sur le web	9
7.1	Navigateur.....	9
7.2	Participation à des forums et publications sur les réseaux sociaux	9
7.3	Téléchargement de logiciels, ou d'œuvres protégées	9
7.4	Consultation de sites illicites	9
7.5	Consultation d'internet à des fins privées	10
7.6	Contrôles de l'usage	10
8	Intranet	10
8.1	Mise en place et fonctionnement de l'Intranet	10
8.2	Données nominatives et personnelles.....	10
9	Respect de la loi Informatique et Libertés et du RGPD	10
10	Place du Comité Economique et Social dans le Système d'Information	11
10.1	Outils d'information mis à disposition	11
10.2	Règles de communication	11
11	Responsabilité et Sanctions	12
12	Affichage et formalités – Entrée en vigueur	12

1 Généralités

1.1 Présentation générale

L'objet de la présente Charte informatique est de rappeler les règles d'utilisation du système d'information de l'entreprise détaillé au point 2 ci-dessous (« Système d'Information »), et notamment des outils informatiques.

Cette Charte s'applique à l'ensemble du personnel des entreprises constituant l'Union Economique et Sociale ESDI c'est-à-dire toutes les entités du Groupe ESDI (« l'UES ESDI » ou « ESDI ») ainsi qu'aux stagiaires, intérimaires et salariés d'entreprises extérieures exécutant un travail au sein des entreprises constituant l'UES ESDI, c'est à dire à tous les utilisateurs autorisés du Système d'Information d'ESDI (« Utilisateurs »).

La présente Charte est annexée au règlement intérieur auquel elle s'intègre. Son non-respect peut donc donner lieu à des sanctions. En cas de doute sur son interprétation, il appartient à chacun d'interroger son supérieur hiérarchique et d'en référer au service technique.

Le cadre juridique de la sécurité de l'information est complexe et impératif. Chaque Utilisateur se doit de respecter les règles juridiques applicables et les règles rappelées dans la présente Charte, notamment en matière :

- de respect des règles déontologiques et professionnelles,
- de respect des procédures de travail,
- de respect de l'organisation et des règles de délégation,
- de communication d'informations,
- d'utilisation des moyens informatiques mis à sa disposition dans le cadre de sa fonction.

L'Utilisateur s'engage notamment à :

- ne pas introduire, ni utiliser, ni installer sur le matériel de l'entreprise, des logiciels informatiques provenant de l'extérieur ou pour lesquels l'entreprise ne possède pas de licence,
- ne pas copier les logiciels installés sur le matériel de l'entreprise,
- ne pas utiliser de supports informatiques provenant de l'extérieur sans les avoir soumis préalablement au contrôle du service informatique,
- ne pas communiquer les codes d'accès, code sources et sauvegardes à toute personne autre que celles habilitées par l'entreprise.

Les Utilisateurs veillent à faire accepter valablement l'ensemble des règles posées dans la présente Charte à toute personne à laquelle ils permettraient d'accéder au Système d'Information.

Il est rappelé que l'Utilisateur est par ailleurs soumis à l'ensemble des règles rappelées par le Règlement Intérieur, comme les règles de confidentialité. Dès lors, il est tenu d'observer une discrétion et un secret professionnel absolus sur les activités de l'entreprise et les informations et opérations dont il a connaissance à l'occasion de son travail.

Les informations chiffrées sur les clients qui peuvent être affichées sur les écrans au sein des espaces de travail sont à ce titre des informations confidentielles. Elles ne doivent pas être diffusées en dehors de l'entreprise.

1.2 Administrateur du Système d'Information

Le responsable du Système d'Information d'ESDI, c'est-à-dire le service technique, est désigné « Administrateur » du Système d'Information. Il veille à la protection, à la maintenance, au bon fonctionnement du Système d'Information, respecte la présente Charte et s'assure du respect par ses subordonnés de cette dernière. Il agit en concertation avec le service RH d'ESDI et avec son Délégué à la Protection des Données (« DPO ») afin de se mettre en conformité avec les dispositions légales, effectuer toute formalités ou déclarations.

1.3 Avis du Comité Economique et Social

La présente charte a été soumise à l'avis du Comité Economique et Social, qui a été informé et consulté conformément aux dispositions du Code du travail.

2 Définition du Système d'Information

On entend par Système d'Information de l'entreprise :

- Matériel : l'ensemble des ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique en ce compris les serveurs, hubs, câbles du réseau, fax, photocopieurs, téléphones, fixes ou portables, badges,
- Logiciel : l'ensemble des logiciels contenus dans ou faisant fonctionner, inter opérer ou protégeant lesdits ordinateurs et matériels informatiques, en ce compris les protocoles de communication TCP/IP,

permettant les opérations :

- la constitution et la création,
- l'échange, la circulation, la diffusion,
- la duplication, reproduction et stockage,

de:

- données, fichiers, base de données,
- bases de connaissances,
- intranet, extranet,
- images, sons, textes,
- flux quelconques d'information,

entre :

- les « Utilisateurs » entre eux,
- les « Utilisateurs » et l'extérieur,

et ce quelle que soit la finalité du flux d'information.

Le Système Informatique de l'entreprise comprend les fichiers, données et bases de données, système de messagerie, intranet, extranet.

3 La protection du Système d'Information

3.1 Accès, mots de passe et sécurité

L'accès au réseau est protégé par des mots de passe, identifiants, codes d'accès et login (« mots de passe »). Ces mots de passe sont donnés de manière individuelle. En aucune manière ils ne peuvent être donnés à un collègue ou à un tiers, ni notés sur l'ordinateur de l'Utilisateur. L'Utilisateur doit les mémoriser. En cas d'oubli, seul l'Administrateur du réseau pourra communiquer de nouveau le mot de passe à l'Utilisateur. Un autre mot de passe peut être donné à l'Utilisateur pour accéder ou faire fonctionner la messagerie électronique, ou pour accéder à des fichiers en partage réservé.

De la même manière, la connexion au réseau via le téléphone fixe est protégée par un mot de passe. Ce mot de passe est personnel et ne doit en aucun cas être communiqué à un collègue ou à un tiers.

De manière générale, tout dispositif d'identification personnelle au sein de l'entreprise devra faire l'objet d'un usage strictement personnel. De nouveau, il est rappelé que les mots de passe sont personnels et ne doivent en aucun cas être communiqués à un collègue ou à un tiers.

3.2 Les pare-feux

ESDI dispose de pare-feux face à l'intrusion de virus. Il est impératif que chaque Utilisateur procède selon les instructions de l'Administrateur à une mise à jour régulière de ou des anti-virus, afin que le Système d'Information soit protégé de manière efficace.

3.3 Contrôle et maintenance par l'Administrateur

Les Utilisateurs sont avertis que l'Administrateur peut avoir accès à l'ensemble des composants du Système d'Information à n'importe quel moment et ce afin d'effectuer tout acte de protection du Système d'Information. La protection du Système d'Information s'entend de la :

- conservation, et sauvegarde, l'absence de diffusion non autorisée des informations commerciales, techniques, administratives, artistiques, industrielles, marketing, et autres informations appartenant à l'entreprise,
- preuve de la date de création ou de la diffusion desdites informations,
- protection de l'intégrité des données et du fonctionnement du Système d'Information,
- absence d'intrusion dans le Système d'Information d'informations ou de matériels violant les règles relatives au droit d'auteur, copyright, par exemple pour défaut de licence d'utilisation,
- mise à jour, maintenance, correction, réparation des Matériels et Logiciels.

Dans le cas, où un composant du Système d'Information ne se trouverait pas dans l'enceinte de l'entreprise, l'Utilisateur qui en a la garde s'oblige à le restituer ou le confier à l'Administrateur à première demande de sa part.

L'Administrateur pourra mettre en place des outils de contrôle et de surveillance répondant strictement à la finalité de la protection du Système d'Information. Il est rappelé que les délégués du personnel pourront saisir immédiatement l'employeur, en l'espèce le Directeur des Ressources Humaines, ayant délégation, s'ils constatent qu'il existe une atteinte aux droits des personnes ou aux libertés individuelles dans l'entreprise qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché.

3.4 Introduction de Matériels et Logiciels

Les médias de stockage amovibles (clefs USB, CD, disques durs, etc...) présentent des risques très forts vis-à-vis de la sécurité : absence de cryptage par défaut, risques importants de contamination par des programmes malveillants et risque de perte de données. Leur connexion au Système d'Information est interdite par principe.

Seul l'Administrateur est autorisé à introduire dans le Système d'Information de nouveaux Matériels ou Logiciels. En cas de besoins exprimés par un Utilisateur pour un nouveau matériel ou logiciel, il devra demander l'autorisation préalable à l'Administrateur avant son admission dans le Système d'Information. Dans des cas exceptionnels, l'Administrateur, peut autoriser l'accès d'un matériel identifié, sur demande et par une autorisation écrite.

3.5 Alertes

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits ou malveillants, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité du Système d'Information doit être signalé immédiatement à son responsable hiérarchique ainsi qu'au service technique.

4 L'accès et l'intervention sur les réseaux de nos clients

ESDI met en œuvre les mécanismes de protection adaptés sur les systèmes d'information mis à la disposition des utilisateurs des clients d'ESDI, notamment à travers des comptes nominatifs systématiques. L'Utilisateur est informé que les informations d'authentification qui lui sont attribuées constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

Les niveaux d'accès aux systèmes d'information ouverts à l'Utilisateur sont définis en fonction de missions qui lui sont confiées. Il est responsable de l'utilisation des systèmes d'information auxquels il accède avec les droits qui lui sont conférés par son (sa) responsable. En cas d'évolution de ses missions une nouvelle autorisation est délivrée par son (sa) responsable.

La sécurité des ressources mises à la disposition de l'Utilisateur lui impose le respect des règles suivantes :

- Se conformer aux directives de sécurité concernant les usages :
 - relatifs à la connexion :
 - appliquer les consignes de gestion des mots de passe d'ESDI ou de ses clients,
 - garder strictement confidentiel ses informations d'authentification,
 - ne pas utiliser les informations d'authentification d'un autre Utilisateur, ni chercher à les connaître,
 - ne pas enregistrer ses informations d'authentification sur des applications ou espaces non maîtrisés par ESDI,
 - ne pas masquer sa véritable identité, ne pas usurper l'identité d'autrui, ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas, s'interdire d'accéder ou de tenter d'accéder à des ressources du Système d'Information ou des systèmes d'information, pour lesquelles il n'a pas reçu d'autorisation explicite,
 - ne pas se connecter à des sites Internet malveillants ou sans rapport direct avec l'activité du client,
 - s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations du matériel ou du logiciel,
 - verrouiller ou fermer toutes les sessions en cours sur son poste de travail, en cas d'absence, même momentanée,
 - s'assurer que toute personne externe susceptible d'accéder au Système d'Information de ESDI y est autorisée par le responsable de structure.
 - relatifs aux données et documents professionnels :
 - protéger les informations qu'il est habilité à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Lorsqu'il crée un document, l'Utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.),
 - n'opérer les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des ressources partagées ESDI ou validées par ESDI,

- ne pas utiliser des supports de données tels que (ordinateur, clé USB, CDROM, DVD, cloud, etc...) sans respecter les règles de sécurité d'ESDI et prendre les précautions nécessaires pour s'assurer de leur innocuité,
 - respecter les règles définies par ESDI, obtenir l'autorisation de son (sa) responsable de structure pour tout traitement de données réalisé sur un support externe,
 - s'assurer que son poste de travail est verrouillé lorsqu'il s'absente de son bureau afin de se prémunir contre les risques de vol de documents sensibles. De la même manière s'assurer que les dispositions contractuelles avec des intervenants extérieurs comportent les clauses rappelant les rôles et les obligations des acteurs concernés.
- Respecter les consignes de sécurité concernant le matériel ou les logiciels :
 - ne pas modifier les paramètres du poste de travail,
 - ne pas installer, télécharger ou utiliser des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites de confiance, ou sans autorisation de son (sa) responsable de structure,
 - ne pas copier, modifier, détruire les logiciels propriétés d'ESDI,
 - respecter les dispositifs mis en place par ESDI pour lutter contre les virus et les attaques par programmes informatiques,
 - utiliser les moyens de protection mis à disposition contre le vol (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils contiennent (ordinateur portable, disque dur, clé USB, smartphones, tablettes, etc.),
 - ne pas désactiver, ni altérer le fonctionnement ou désinstaller l'outil de cryptage lorsqu'il a été installé par ESDI,
 - adapter la sécurité (physique et logique) des équipements nomades en fonction de la sensibilité de l'information qu'ils traitent et stockent,
 - signaler le plus rapidement possible au (à la) chargée de la sécurité des SI tout logiciel ou dispositif suspect ainsi que toute perte, tout vol ou toute compromission suspectée ou avérée
 - d'un équipement stockant des données professionnelles,
 - de ses informations d'authentification (identifiant, mot de passe, code pin, clés privées, etc.).

5 L'usage du matériel informatique et des éléments du Système d'Information

Les matériels et logiciels informatiques, et plus largement le Système d'Information, sont réservés à un usage exclusivement professionnel et ne doivent pas être utilisés à des fins personnelles, sauf autorisation préalable de la Direction, conformément aux dispositions du règlement intérieur notamment. Ils ne doivent pas être sortis de l'entreprise sans autorisation préalable du service technique.

L'entreprise tolère un usage exceptionnel, à des fins autres que professionnelles, des ordinateurs et des technologies de l'information, notamment internet dès lors que l'utilisation intervient en dehors du temps de travail effectif, n'affecte pas le bon fonctionnement du service et ne porte pas atteinte à l'intérêt collectif de l'entreprise, et dans le strict respect des dispositions des articles 6 et 7 ci-dessous. Cette utilisation, à des fins personnelles, depuis le lieu de travail, est tolérée pendant les temps de pause ou pour des besoins urgents de la vie privée du salarié.

Elle doit être occasionnelle et raisonnable (tant dans la fréquence que dans la durée), conforme à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité du Système d'Information ainsi qu'à l'image de marque de l'entreprise.

Tout défaut d'entretien, toute utilisation non-conforme du matériel ou des biens confiés pourra justifier la mise en œuvre d'une procédure disciplinaire pouvant aller jusqu'à la cessation de la collaboration.

Lors de son départ définitif de l'entreprise, chacun est tenu de restituer en bon état tout élément du Système d'Information qui lui auront été confiés en vue ou dans le cadre de l'exécution de son travail.

Au surplus, le matériel informatique devra être restitué sur simple demande justifiée de l'employeur.

6 La messagerie

6.1 Adresse électronique

Chaque Utilisateur dispose d'une messagerie électronique composée du prénom et du nom. En cas d'homonymie, l'Administrateur fixera la règle d'attribution. En cas de changement de nom, l'Utilisateur pourra demander à l'Administrateur une nouvelle messagerie électronique. L'utilisation d'un pseudonyme ou l'usage d'un faux nom est expressément prohibée, sauf autorisation de l'Administrateur qui s'assurera du bien-fondé de cette utilisation.

6.2 Message électronique et pouvoirs internes

Malgré son extrême facilité d'utilisation, une attention toute particulière doit être portée à sa rédaction et à sa diffusion. Le message électronique (email ou mel) est un écrit pouvant engager la responsabilité de la société, mais aussi de l'Utilisateur. L'ensemble des bonnes pratiques et des règles rappelées notamment dans la présente Charte et dans le règlement intérieur doivent être respectées.

Les règles hiérarchiques et d'organisation des pouvoirs internes de signatures devront être respectées. Aucun message électronique ne devra être envoyé par un Utilisateur à un destinataire extérieur à l'entreprise, si l'Utilisateur n'en a pas l'autorité.

6.3 Contenu du message électronique

Tout message sera réputé comme professionnel sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé, ou s'il est stocké dans un espace privé de données.

L'Utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages de masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

Les Utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, à caractère violent, pornographique ou contraire aux bonnes mœurs, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

6.4 Protection des Informations

Les risques d'interception des messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du Système d'Information aux Informations à caractère non confidentiel, non stratégique et non sensible.

6.5 Règles de conservation de la messagerie

La messagerie électronique ne sera conservée sur le serveur concerné de l'entreprise que pour une durée déterminée par l'Administrateur. Au-delà, les messages sont susceptibles d'être archivés ou effacés.

6.6 Utilisation privée de la messagerie

L'Utilisateur peut utiliser la messagerie électronique de l'entreprise à des fins privées. Il est rappelé qu'il aura soin dans la mesure du possible de classer ses messages privés (reçus ou envoyés) dans un fichier à part portant la mention "privé" de manière à prévenir l'Administrateur de la nature particulière s'attachant à cette messagerie.

Conformément à la présente Charte, l'usage privé de la messagerie (envoi et réception de messages) devra gêner le moins possible le trafic normal des messages professionnels, et ce en termes de volume des messages échangés, de taille des messages échangés et de format des pièces jointes.

Les abus, qui pourraient être constatés par l'Administrateur seront sanctionnés.

7 La navigation sur le web

7.1 Navigateur

L'Administrateur peut limiter la durée de connexion, imposer des configurations de sécurité du navigateur, imposer des limites de taille au téléchargement de contenu par note de service.

7.2 Participation à des forums et publications sur les réseaux sociaux

Elles sont par principe interdites. La participation à des forums au nom d'ESDI peut engager la responsabilité d'ESDI. L'Utilisateur doit disposer des autorisations internes expresses afin de s'exprimer au nom d'ESDI et devra préalablement prendre contact avec l'Administrateur d'ESDI.

Plus généralement, la participation à des forums via le Système d'Information d'ESDI, même en son nom personnel par l'Utilisateur, est interdite.

De la même manière, l'utilisation des réseaux sociaux, comme la connexion, consultation ou publication sur les réseaux sociaux via le système d'ESDI est interdite.

7.3 Téléchargement de logiciels, ou d'œuvres protégées

Le téléchargement de logiciels ou d'œuvres protégées, sans autorisation des ayants-droits, est de nature à engager la responsabilité d'ESDI et comme tels sont strictement interdits.

L'Administrateur se réserve la possibilité d'effacer du Système d'Information toute trace de ces logiciels et œuvres introduites dans le Système, en violation des droits de propriété intellectuelle d'autrui.

7.4 Consultation de sites illicites

La consultation et le téléchargement du contenu de sites à caractère pornographique, pédophile sont contraires aux bonnes mœurs et peuvent revêtir le caractère d'une infraction pénale. Cette activité est strictement interdite. L'Administrateur se réserve le droit de dénoncer tout acte délictueux aux autorités, et ce sans préjudice de l'application des sanctions prévues à la présente Charte.

7.5 Consultation d'internet à des fins privées

Il est rappelé que la consultation de sites web à titre privé est autorisée dans la mesure où cette navigation n'entrave pas l'accès professionnel et qu'elle ne gêne pas la bonne marche du travail de l'Utilisateur.

Il est précisé que le téléchargement de fichiers musicaux ou vidéo de tous formats ne rentrant pas dans l'accès professionnel et gênant la bonne marche du Système d'Information en raison de l'encombrement qu'il génère est strictement prohibé.

7.6 Contrôles de l'usage

Il est précisé que l'Administrateur exerce un contrôle sur les durées des connexions, les sites les plus visités, dans le cadre de la mission de protection du Système d'Information.

L'Utilisateur est informé que les traces de la navigation sont temporairement archivées.

L'entreprise se réserve le droit :

- de contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte,
- de suspendre l'usage du service d'hébergement des pages Web par un Utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'Utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

L'entreprise peut, en fonction des contraintes professionnelles et de la gravité de la faute, décider d'une mesure de suspension temporaire ou définitive des comptes de l'Utilisateur. La suspension débutera à compter de la constatation de la faute, nonobstant l'engagement de la procédure disciplinaire.

Toute utilisation abusive des systèmes d'informations, à des fins personnelles ou malveillantes, entraînera des sanctions disciplinaires pouvant aller jusqu'au licenciement pour faute grave conformément aux dispositions du Règlement intérieur et à la législation en vigueur.

8 Intranet

8.1 Mise en place et fonctionnement de l'Intranet

L'Intranet fonctionne sous la responsabilité informatique de l'Administrateur. Aucun Utilisateur ne peut introduire ou tenter d'introduire un élément de contenu sur l'Intranet sans l'autorisation de l'Administrateur. Les Utilisateurs pourront formuler toute suggestion à ce dernier quant au contenu ou fonctionnement de l'Intranet.

8.2 Données nominatives et personnelles

L'Utilisateur sera averti avant diffusion sur l'Intranet de données nominatives et personnelles le concernant et en particulier de son image figurant dans la messagerie ou au Trombinoscope. L'Utilisateur pourra demander à avoir accès à ses données nominatives et personnelles et pourra demander leur rectification, en prenant contact avec le DPO d'ESDI (DPO-ESDI@ESDI.fr).

9 Respect de la loi Informatique et Libertés et du RGPD

Le Règlement Général sur la Protection des Données personnelles (« RGPD ») s'applique à ESDI et à l'ensemble de ses services.

Ce règlement encadre notamment l'utilisation, la durée de conservation et la protection des données personnelles. Il est de la responsabilité de chacun de respecter les règles diffusées à cet égard. Dans ce cadre, il est rappelé que la collecte, le traitement, la conservation des données personnelles et leur transmission éventuelle à des tiers doit s'effectuer de manière loyale. Les données ne peuvent être traitées à l'insu de la personne concernée.

La création de tout traitement automatisé de données personnelles de personnes physiques doit être référencée auprès du DPO afin d'être intégrée au registre des traitements de données personnelles.

En complément des informations relatives au RGPD qui ont été diffusées, tout Utilisateur et toute personne peut poser une question ou adresser une demande au DPO d'ESDI à l'adresse suivante : DPO-ESDI@ESDI.fr.

10 Place du Comité Economique et Social dans le Système d'Information

10.1 Outils d'information mis à disposition

Le Comité Economique et Social de l'UES ESDI disposera d'une adresse électronique (cse@esdi.fr) et d'un répertoire au sein du Système d'Information.

Le Comité Economique et Social gèrera son répertoire de manière autonome. L'Administrateur garantit au Comité Economique et Social un accès permanent (sous réserve de la maintenance du Système d'Information et autres opérations de protection du Système d'Information) à ce répertoire par tous les Utilisateurs.

Le répertoire peut être complété, après autorisation préalable de l'Administrateur par des pages d'informations sur l'Intranet.

10.2 Règles de communication

Le Comité Economique et Social devra dans sa communication au personnel d'ESDI :

- veiller au respect des dispositions de la loi sur la liberté de la presse,
- se limiter quant à l'objet de la communication à ce qui rentre dans le cadre de ses attributions,
- respecter les consignes de l'Administrateur en termes de format, de taille, des messages ou de pages intranet.

En cas de non-respect de ces dispositions, l'Administrateur pourra retirer l'autorisation après avoir préalablement entendu le Comité Economique et Social en ses explications.

11 Responsabilité et Sanctions

L'Utilisateur doit avoir conscience que même au sein de l'entreprise, quel que soit l'usage du matériel informatique et du Système d'Information, il est soumis à la Loi et que ses actes sont susceptibles, d'engager la responsabilité de son employeur mais également sa responsabilité personnelle pour les délits qu'il commet (contrefaçon, injure, piratage, fraude, acte malveillant...) ou les préjudices qu'il cause.

L'Utilisateur qui ne respecterait pas les règles juridiques applicables, notamment celles rappelées dans la présente Charte, pourra voir sa responsabilité engagée à titre personnel dès lors qu'il est prouvé que les faits fautifs lui sont imputables.

Cette responsabilité pourra être engagée non seulement par toute personne ayant subi un préjudice du fait du non-respect de ces règles, mais aussi par l'entreprise en sa qualité d'employeur.

Le non-respect des dispositions de la Charte peut entraîner notamment des sanctions disciplinaires dans le cadre de l'application du règlement intérieur et selon la procédure qui y est spécifiée.

12 Affichage et formalités – Entrée en vigueur

En tant que partie du règlement intérieur, la présente Charte informatique sera affichée conformément à l'article R. 122-12 du Code du travail et accessible sur l'intranet de l'UES ESDI. Elle sera déposée au secrétariat-greffe du conseil de prud'hommes de Belfort.

La présente Charte d'utilisation entrera en vigueur le 13 Mai 2019

La présente Charte sera communiquée avec l'avis du Comité Economique et Social à l'inspecteur du travail.