étic
FONCIÈREMENT
RESPONSABLE

Charte d'utilisation

Charte de l'utilisateur pour l'usage de la ***Social Change Plateform***

Social Change
PLATFORM
BETA

Table des matières

1. Introduction

La société ETIC SAS met à la disposition de tout utilisateur ayant droits des moyens de communication, des outils de gestion, ainsi que des informations et données (bases de données, images, vidéos, etc.) au travers de la ***Social Change Plateform***.

2. Objet de la charte

La présente Charte a pour vocation d'exposer les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre.

3. Définitions

Utilisateur : désigne un membre ayant droit d'accès à la SCP et en faisant usage.

Administrateur : désigne une personne en charge de la gestion d'un pôle ou d'une organisation. Cette personne à droit de regard et devoir de modération sur son entité ainsi que celles qui lui sont subordonnées. Selon sa charge, elle est en mesure d'intégrer une ou des entité(s) et/ou un ou des membre(s).

Pôle : entité étant administré par au moins 1 administrateur, en charge de la modération de son ensemble, et étant en mesure d'inviter des organisations dans son pôle et d'ajouter des administrateurs.

Organisation : entité invité par un administrateur de pôle, administré par au moins un administrateur en charge de la modération de son ensemble. Un administrateur est en mesure d'inviter un ou des membre(s) et d'ajouter un ou des administrateurs.

4. Conditions d'accès à la Social Change Plateform

L'utilisation de la ***Social Change Plateform*** est soumise à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lorsque le pôle, l'organisation ou le membre n'est plus ayant droit d'accès à la ***Social Change Plateform***.

5. *Règles d'utilisation, de sécurité et de bon usage*

L'utilisateur est responsable de l'usage qu'il fait de la ***Social Change Plateform***.

L'utilisateur ne doit se livrer, en aucune circonstance, à l'une des activités suivantes :

- Charger, stocker, publier, diffuser ou distribuer des documents, informations, images, vidéos, etc. :
  - à caractère violent, pornographique ou contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
  - de caractère diffamatoire et de manière générale illicite,
  - portant atteinte à l'intégrité et à la conservation des données,
  - portant atteinte à l'image de marque interne et externe d'une entreprise ou d'un de ses membres.

Si l'utilisateur est amené à voir ou recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt et de le signaler à l'administrateur et au correspondant sécurité de manière immédiate.

L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc.

Sont à proscrire :

- Utiliser la ***Social Change Plateform*** à des fins de harcèlement, menace ou d'injure et de manière générale violer des droits en vigueur.
- Charger, stocker ou transmettre des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle, sauf à posséder les autorisations nécessaires. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels fichiers.
- Charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, etc., qui sont protégés par les lois sur la propriété intellectuelle. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes, logiciels, progiciels, etc..
- Charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées.
- Falsifier la source d'éléments contenus dans un fichier.
- Utiliser la ***Social Change Plateform*** de manière à gêner l'accès des autres utilisateurs.

Pour rappel, certaines des activités énoncées ci-dessus peuvent constituer des infractions de nature pénale.

ETIC SAS se réserve la possibilité d'effectuer des vérifications et contrôles réguliers, dans les limites prévues par la loi.

6. Mesures de sécurité

Afin de permettre la mise en œuvre d'une parade de premier niveau, l'utilisateur doit respecter au minimum les prescriptions suivantes :

Prescription 1 : Mettre toujours un mot de passe quand il lui est demandé.

Prescription 2 : Changer de mot de passe régulièrement.

Prescription 3 : Ne jamais prêter son identifiant/mot de passe.

Prescription 4 : Utiliser un anti-virus sur tout document/fichier transmis à la ***Social Change Plateform***

Prescription 5 : Ne jamais quitter son poste de travail en laissant accessible une session en cours.

7. Préservation de l'intégrité de la Social Change Plateform

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement de la ***Social Change Plateform***.

8. Analyse et contrôle de l'utilisation de la Social Change Plateform

Pour des nécessités de maintenance et de gestion technique, l'utilisation de la ***Social Change Plateform*** ainsi que les échanges via le réseau peuvent être analysés et contrôlés par ETIC SAS dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

9. Droits et devoirs spécifiques des administrateurs

L'administrateur a techniquement tous les pouvoirs sur son pôle et/ou son organisation et/ou ses membres. Il a de ce fait des devoirs importants, en particulier celui de ne pas abuser de ses pouvoirs.

Tout administrateur a le droit :

- d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,

- d'accéder aux informations privées à des fins de diagnostic et d'administration, en respectant scrupuleusement la confidentialité de ces informations,
- d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte, après autorisation de son responsable fonctionnel et en relation avec le correspondant sécurité du réseau.

Tout administrateur système a le devoir :

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction,
- d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le correspondant sécurité du réseau,
- de respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au strict nécessaire et en respectant un "secret professionnel" sur ce point,
- de respecter, s'il est lui-même utilisateur du système, les règles qu'il est amené à imposer aux autres utilisateurs,
- de solliciter auprès du correspondant sécurité réseau des modifications du système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- d'informer immédiatement son responsable fonctionnel de toute tentative (fructueuse ou non) d'intrusion sur son système, ou de tout comportement dangereux d'un utilisateur,

10. Informations vous concernant

Magali Héraud, membre de ETIC SAS est responsable du traitement des données.

Celles-ci seront conservées pendant 99 ans. Toutefois l'administrateur/membre qui l'a publié pourra supprimer les données publiées quand il le souhaite.

Si le site utilise des cookies, vous pourrez les supprimer en vous rendant dans les préférences de votre navigateur web.

« Les informations recueillies font l'objet d'un traitement informatique destiné à mettre en réseau les membres de la Social Change Plateform. Les destinataires des données sont ses membres, sauf publication publique choisit par l'émetteur.
Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à contact@etic.co.
Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.

Le(s) service(s) d'ETIC dispose(nt) de moyens informatiques destinés à gérer plus facilement les informations.
Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : les membres de la SCP.
Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service contact@etic.co.

Attention !
En l'absence de réponse de votre part dans un délai d'un mois à compter de la réception de ce courrier, votre accord sera réputé acquis. Vous pourrez toutefois nous faire part ultérieurement, à tout moment, de votre souhait que la diffusion de vos données sur Internet cesse. Nous vous rappelons que vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent.
Pour exercer ce droit, adressez-vous à : contact@etic.co

11. Cadre juridique

Les lois énoncées dans ce document sont données à titre purement indicatif et de manière non exhaustive.

1.1 Délits informatiques

La loi française reconnaît certaines actions sur les systèmes informatiques comme étant des délits et prévoit de les sanctionner. A titre d'exemple (la liste est loin d'être exhaustive) :

- l'intrusion sur un ordinateur à travers un réseau, cf. loi du 5 janvier 1988, article 462 (peines d'amende et de prison en cas d'introduction dans un système informatique, avec ou sans intervention sur le système).
- la copie illicite de logiciels, cf. loi du 3 juillet 1985, article 47 (toute reproduction autre qu'une copie de sauvegarde est une contrefaçon, la copie privée n'est pas autorisée)
- l'emprunt de l'identité d'un tiers, (comprenant l'envoi d'un courrier électronique sous une fausse identité)
- le vandalisme informatique (destruction de fichiers sans en avoir l'autorisation par exemple)

1.2 Sanctions pénales

L'Entreprise est tenue par la loi de signaler toute violation constatée des lois. Les sanctions pénales peuvent aller de 1 mois à plusieurs années de prison et de 300 euros à plusieurs centaines de milliers d'euros d'amende. Les principales lois françaises et européennes sont :

- le code de propriété intellectuelle,

- la loi du 6/01/1978 sur l'informatique, la sécurité et les libertés,
- la loi du 3/07/1985 sur la protection des logiciels,
- la loi du 5/01/1988 (Godefrain) sur la fraude informatique,
- les articles 462-2 à 462-9 du code pénal,
- la convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel,
- la directive de la CEE du 21/12/1988 sur l'harmonisation juridique de la protection des logiciels.

1.2.1 Extraits du code de propriété intellectuelle

Art. L335-2 - Toute édition d'écrits, de composition musicale, de dessin, de peinture, ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit. La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de deux ans d'emprisonnement et de 150 000 euros d'amende. Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaits.

Art. L335-3 - Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.

Art. L335-9 - En cas de récidive des infractions définies aux articles L 335 -2 à L.335 -4 ou si le délinquant est ou a été lié par convention avec la partie lés, les peines encourues sont portées au double.

1.2.2 Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique

Article unique. - Dans le titre II du livre II du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

Chapitre III De certaines infractions en matière informatique :

- Article 462-2. Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement d'un mois à un an et d'une amende de 300 euros à 7500 euros ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 1500 euros à 15 000 euros.
- Article 462-3. Quiconque aura intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un

emprisonnement de trois mois à trois ans et d'une amende de 1500 euros à 15 000 euros ou de l'une de ces deux peines.

- Article 462-4. Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 300 euros à 75 000 euros ou de l'une de ces deux peines.

- Article 462-5. Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3000 euros à 300 000 euros.

- Article 462-6. Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3000 euros à 300 000 euros ou de l'une de ces deux peines.

- Article 462-7. La tentative des délits prévus par les articles 462-2 à 642-6 est punie des mêmes peines que le délit lui-même.

- Article 462-8. Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462 -2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- Article 462-9. Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.

1.3 Rappel de la CNIL

1.3.1 La sécurité des fichiers

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000€d'amende. art. 226-17 du code pénal

1.3.2 La confidentialité des données

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).
La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende.

La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende. art. 226-22 du code pénal

1.3.3 La durée de conservation des informations

Les données personnelles ont une date de péremption.
Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier.
Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 € d'amende.

art. 226-20 du code pénal

1.3.4 L'information des personnes

Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées.
Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 € par infraction constatée et 3 000 € en cas de récidive. art. 131-13 du code pénal Décret n° 2005-1309 du 20 octobre 2005

1.3.5 L'autorisation de la CNIL

Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL.
Le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000€ d'amende. art. 226-16 du code pénal

1.3.6 La finalité des traitements

Un fichier doit avoir un objectif précis.
Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif.
Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.
Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 € d'amende. art. 226.21 du code pénal

12. Modification de la charte

Le signataire est informé que cette charte peut être modifiée à tout moment. Les modifications apportées lui seront notifiées périodiquement.

Date :

Nom :

Prénom :

Qualité :

Utilisateur des moyens informatique de la ***Social Change Plateform***, je déclare avoir pris connaissance de la présente charte de bon usage de l'informatique et des réseaux et m'engage à la respecter.

Signature :