

Charte d'utilisation des ressources informatiques de Lannion-Trégor Communauté

Préambule

En plein essor, les technologies numériques jouent un rôle fondamental au cœur des pratiques professionnelles. C'est pourquoi Lannion-Trégor Communauté s'est engagée dans une démarche proactive en faveur de la sécurité de ses ressources informatiques, afin de préserver la confidentialité et l'intégrité des données de ses administrés, de ses employés, de ses élus et de ses partenaires.

Pour se faire, la présente charte fixe de manière transparente les modalités d'utilisation des ressources informatiques de Lannion-Trégor Communauté afin d'en favoriser un usage optimal en termes de **confidentialité**, de **respect de la réglementation et des personnes**, mais également en termes de **sécurité et de performance informatiques**.

**La charte revêt un caractère opposable à l'égard de l'ensemble
des utilisateurs des ressources informatiques
(employés, élus, stagiaires, prestataires extérieurs, ...)**

car chaque personne est un maillon à part entière de la sécurité informatique

L'objectif est de fixer et faire connaître des « règles du jeu » qui soient suffisamment protectrices pour le bon fonctionnement de la collectivité, tout en s'assurant que chacune de ces règles est respectueuse des droits de chaque utilisateur, notamment en matière de droit du travail ainsi qu'en matière de protection de la vie privée et des données à caractère personnel.

La charte a été présentée au Comité Technique de Lannion-Trégor Communauté le 7 novembre 2019. Elle remplace la charte informatique précédemment adoptée. Elle sera susceptible d'être modifiée, notamment en fonction des évolutions réglementaires, organisationnelles et technologiques qui adviendraient.

Sommaire :

ARTICLE 1 :	LES PERSONNES CONCERNEES	2
ARTICLE 2 :	LES RESSOURCES INFORMATIQUES CONCERNEES	2
ARTICLE 3 :	CONDITIONS D'ACCES AUX RESSOURCES INFORMATIQUES	2
ARTICLE 4 :	REGLES GENERALES D'UTILISATION ET DE SECURITE DES RESSOURCES INFORMATIQUES.....	4
ARTICLE 5 :	CONDITIONS DE CONFIDENTIALITE	5
ARTICLE 6 :	RESPECT DE LA LEGISLATION RELATIVE AUX LOGICIELS	5
ARTICLE 7 :	PRESERVATION DE L'INTEGRITE DES SYSTEMES INFORMATIQUES	6
ARTICLE 8 :	MESURES D'HISTORISATION ET DE SECURITE DES USAGES	6
ARTICLE 9 :	FINALITES DU CONTROLE DE L'UTILISATION DES RESSOURCES INFORMATIQUES	6
ARTICLE 10 :	SANCTIONS	7
ARTICLE 11 :	LA DIRECTION DES SYSTEMES D'INFORMATION.....	7

Article 1 : Les personnes concernées

La présente charte s'applique à l'ensemble du personnel et des élus de Lannion-Trégor Communauté, mais également aux personnes au sein d'organismes partenaires utilisant les ressources informatiques de Lannion-Trégor Communauté (par exemple : Centre Intercommunal d'Action Sociale, Lannion-Trégor Solidarités, Office de Tourisme Communautaire, SEM Lannion-Trégor, ...).

Elle est également applicable à **tout intervenant extérieur ayant accès aux ressources informatiques** de Lannion-Trégor Communauté (prestataires de service, stagiaires, visiteurs occasionnels, ...). Toute intervention extérieure doit faire l'objet d'une information à l'administrateur réseau.

→ **L'ensemble de ces personnes est indistinctement désigné, ci-après, par le terme « utilisateurs ».**

Les agents de la Direction des Systèmes d'Information de Lannion-Trégor Communauté chargés de la gestion des accès aux ressources informatiques de Lannion-Trégor Communauté sont désignés, ci-après, par le terme « **administrateur réseau** » (dont le cadre d'intervention est détaillé à l'article 11 de la présente charte).

Article 2 : Les ressources informatiques concernées

Les « ressources informatiques » sont constituées de l'ensemble :

- ☑ **des équipements mis à disposition par LTC** (ordinateurs, téléphones, tablettes, clés USB, disque durs, matériels d'impression, serveurs, badges d'accès, appareils de connexion et de réseaux, ...);
- ☑ **des services numériques mis à disposition par LTC** (messagerie, logiciels, applications, ...);
- ☑ **ainsi que des données accessibles via ces équipements et ces services numériques.**

Article 3 : Conditions d'accès aux ressources informatiques

L'accès aux ressources informatiques est limité en fonction des besoins réels et des contraintes imposées par le partage des ressources entre l'ensemble des utilisateurs :

- ☑ L'accès n'est autorisé que dans le cadre de l'activité professionnelle ou d'un mandat électif ;
- ☑ L'accès disparaît dès que son utilisateur ne remplit plus les conditions qui l'ont autorisé ;
- ☑ Les droits de chacun sont précisés au moment de l'ouverture du compte d'accès et peuvent être réévalués selon les besoins de son activité ;
- ☑ **Conformément à la réglementation et à la jurisprudence, il est rappelé que les données d'un employé (fichiers, dossiers, logiciels, messagerie électronique, etc ...) détenues dans les outils informatiques mis à sa disposition pour les besoins de son travail sont présumées avoir un caractère « professionnel ». Ces données peuvent donc être consultées par l'employeur, y compris hors la présence de l'employé, sauf si ce dernier les a identifiées comme étant privées**, par exemple, en nommant expressément un fichier, un répertoire informatique ou encore l'objet d'un courriel avec des mots tels que « privé » ou « personnel ». Attention : un répertoire intitulé « mes documents » ou bien désigné par le prénom, le nom ou les initiales de l'employé ne sont pas considérés comme présentant un caractère privé.

Conformément à la réglementation et à la jurisprudence en vigueur, l'employeur ne peut procéder à l'ouverture des données identifiées comme privées qu'en présence de l'employé ou celui-ci dûment appelé ou en cas de risque ou évènement particulier. En outre, il est également rappelé que l'accès aux messages d'un utilisateur doit se faire dans le respect du principe du « secret des correspondances ».

Ces données à caractère privé ne doivent pas être stockées sur le réseau informatique, ce dernier étant dédié à un usage professionnel.

- ☑ Conformément à la réglementation, en cas de nécessité de service et si l'employeur ne peut accéder à ces informations par d'autres moyens, lors de l'absence de l'utilisateur (déplacement, congés, maladie, etc...), l'accès aux ressources dont il détient les codes d'accès peut être sollicité. Sauf situation exceptionnelle, les codes d'accès ne seront pas demandés à l'utilisateur.

Dans tous les cas, toute demande d'accès à des ressources informatiques adressée à un administrateur réseau doit parvenir par écrit, de la part d'un supérieur hiérarchique de niveau équivalent à « direction de pôle ». Cette demande est communiquée, pour information, à l'utilisateur concerné.

- ☑ **Lorsque l'utilisateur est amené à cesser l'activité qui justifiait jusqu'alors son accès aux ressources informatiques** (exemples : fin de contrat de travail d'un employé, fin de mandat d'un élu, fin de contrat d'un prestataire, ...), **il doit s'assurer, avant son départ, que l'ensemble de ses données professionnelles (fichiers informatiques, courriels, liste de contacts, ...) restent accessibles après sa cessation d'activité** (par exemple : en transférant toutes ses données sur le réseau informatique).

Il revient également au service ou à la direction concernée d'anticiper cette situation afin d'assurer l'accès aux ressources après le départ de la personne.

L'utilisateur peut également supprimer ou récupérer les éventuelles données dont il disposait pour son usage privé.

Après la cessation d'activité de l'utilisateur :

- les différents accès de l'utilisateur (ordinateur, messagerie, etc...) seront désactivés par l'administrateur réseau.
- l'ensemble des données présentes sur les différents équipements qui étaient mis à disposition de l'utilisateur seront intégralement et définitivement supprimées (disque dur de l'ordinateur, mémoire du téléphone, clé USB, etc ...) afin d'éviter toute violation de données, notamment dans le cas où ces équipements seraient réutilisés ultérieurement.

Par ailleurs, l'identité d'une personne ayant cessé son activité ne pourra plus être utilisée après son départ (par exemple : l'adresse courriel nominative d'un ancien employé ne pourra plus être utilisée pour envoyer des messages).

- ☑ **Aucun matériel ne doit être réattribué à une nouvelle personne sans avoir préalablement été confié au Service Informatique (qui assurera une réinitialisation et un reparamétrage du matériel si nécessaire).**

Article 4 : Règles générales d'utilisation et de sécurité des ressources informatiques

La mise en place de règles encadrant l'utilisation des ressources informatiques et favorisant leur sécurité est une nécessité afin d'éviter les intrusions et accès illicites.

Lannion-Trégor Communauté ne saurait être tenu pour responsable de la nature des données et informations qui transitent par son intermédiaire. **Tout utilisateur est responsable de l'usage des ressources informatiques qui en est fait à partir des équipements mis à sa disposition ou à grâce à ses moyens d'accès (mots de passe, codes, badges, ...).**

Utilisation :

- ☑ **Seuls ont vocation à être consultés, les ressources informatiques qui présentent un lien direct et nécessaire avec l'activité professionnelle ou le mandat électif de l'utilisateur ;**

Une utilisation des ressources informatiques pour un motif personnel est tolérée, à condition que cette utilisation soit occasionnelle, ne perturbe pas l'activité professionnelle, ne soit pas contraire à la loi et aux bonnes mœurs et qu'elle ne mette pas en cause l'intérêt légitime, la sécurité ou la réputation de Lannion-Trégor Communauté. Est notamment interdite la consultation, diffusion ou réception d'informations en opposition avec les valeurs sociales et morales ou nuisant au respect de la personne humaine et aux libertés individuelles ou aux droits d'un tiers ;

- ☑ Les utilisateurs ne doivent changer aucun paramètre de sécurité ou de connexion du matériel et logiciels mis à leur disposition sans l'accord explicite de l'administrateur réseau de Lannion-Trégor Communauté ;
- ☑ L'installation de logiciels non agréés par Lannion-Trégor Communauté et le contournement de leurs restrictions d'utilisation sont interdits ;
- ☑ Les données circulant sur les réseaux (Internet ou local) peuvent être réglementées ou protégées. L'utilisateur doit donc disposer de toutes les autorisations nécessaires (licence d'utilisation de logiciels, droit de reproduction des images, textes et sons). L'utilisateur peut se rapprocher du service juridique ou de la Direction des Systèmes d'Information de Lannion-Trégor Communauté en cas de doute ;
- ☑ L'utilisateur s'engage à ne pas utiliser le nom et l'adresse de Lannion-Trégor Communauté à des fins non professionnelles, illicites ou illégales.

Sécurité :

L'utilisateur doit à son niveau participer à la sécurité générale. Il constitue l'un des maillons fondamentaux de la sécurité informatique. Il est responsable de l'utilisation des ressources informatiques faite à partir de son compte. C'est pourquoi il doit prendre, en termes de sécurité, des précautions simples mais efficaces :

- ☑ Appliquer les consignes de sécurité du service auquel il appartient ;
- ☑ Laisser les ressources informatiques inaccessibles lorsqu'il s'absente (exemple : verrouiller l'accès à l'ordinateur) et ne pas laisser en évidence des équipements informatiques (téléphone mobile, cd-rom, clé USB, ...) ;
- ☑ Signaler toute anomalie ou dysfonctionnement à l'administrateur réseau dans les plus brefs délais ;
- ☑ Signaler toute perte ou vol de données ou de matériel informatique (même s'il ne contient aucune donnée) à l'administrateur réseau dans les plus brefs délais ;
- ☑ Informer l'administrateur réseau en cas de perte ou de vol de ses moyens d'accès (clé, badge, carte magnétique, ...) ;

- ☑ **Veiller à choisir des mots de passe sûrs, gardés secrets, à ne les communiquer en aucun cas** (sauf dans les cas prévus à l'article 3) **et à les changer périodiquement**. Le mot de passe est une forme d'identification qui engage la responsabilité de l'utilisateur. Il est recommandé de se référer aux prescriptions de la CNIL (voir le site Internet « www.cnil.fr ») ;
- ☑ Ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers des matériels dont il a l'usage ;
- ☑ Être vigilant aux risques de détournements de données ;
- ☑ Supprimer tout courriel inutile ou non sollicité ;
- ☑ Sauvegarder les courriels ainsi que tout fichier contenant des données professionnelles sur les serveurs appropriés (réseau interne). **La messagerie électronique ainsi que le stockage interne de l'ordinateur ou du téléphone ne sont pas des espaces de sauvegarde appropriés ;**
- ☑ Ne pas accéder à une messagerie électronique personnelle (compte tenu des risques liés à des logiciels malveillants ou d'intrusion informatique).

Article 5 : Conditions de confidentialité

Tout utilisateur doit respecter la confidentialité des données auxquelles il a accès, notamment en vertu de la loi « informatique et libertés » du 6 janvier 1978 dans sa version en vigueur et des dispositions du Règlement Général sur la Protection des Données. Ainsi, :

- ☑ Il ne doit pas accéder à des données en faisant usage des codes d'accès d'un autre utilisateur (accès à des courriers électroniques, fichiers informatiques, logiciels, ...) ni pour les lire, les copier, les transmettre, les modifier ou les effacer ;
- ☑ Il ne doit pas masquer sa véritable identité ;
- ☑ Il s'engage à ne pas divulguer, sans autorisation, des informations ou des documents dont il a connaissance à l'occasion de ses fonctions ;
- ☑ Il ne peut mettre en place, conserver et divulguer des données personnelles relatives à des tiers sans autorisation adéquate.

Article 6 : Respect de la législation relative aux logiciels

Il est strictement interdit d'utiliser le courrier électronique, l'accès à internet et plus généralement l'infrastructure informatique de Lannion-Trégor Communauté en vue :

- ☑ de copier des logiciels commerciaux protégés par le droit d'auteur ;
- ☑ de copier, stocker, diffuser ou télécharger des données protégées par le droit d'auteur sans y être autorisé ou sans s'être acquitté des droits nécessaires ;
- ☑ d'utiliser des logiciels couverts par des droits de licence sans autorisation.

De manière générale, l'utilisateur s'engage à respecter la réglementation applicable, notamment celle relative à la propriété intellectuelle et commerciale, le droit de la concurrence, etc.

Article 7 : Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement de perturbations au système informatique et au réseau, soit par des manipulations anormales, soit par l'importation de logiciels malveillants (virus, vers, chevaux de Troie, etc...) ou de tout procédé susceptible de porter atteinte au fonctionnement normal des ressources informatiques ou à la sécurité. Sont notamment interdits :

- ✎ La transmission, l'installation ou l'exécution de logiciels pouvant mettre en péril la sécurité des ressources informatiques ;
- ✎ L'envoi et la réception de messages ou fichiers susceptibles d'être porteurs de logiciel malveillant ;
- ✎ De modifier le fonctionnement normal d'un matériel ou logiciel informatique ;
- ✎ De connecter une machine ou un équipement qui ne fait pas partie du parc informatique géré par Lannion-Trégor Communauté (ordinateur personnel, clé USB personnelle, disque dur personnel, téléphone mobile personnel, ...), à un ordinateur ou au réseau informatique de Lannion-Trégor Communauté, sans l'accord explicite de l'administrateur réseau.

Article 8 : Mesures d'historisation et de sécurité des usages

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources informatiques ainsi que les échanges via le réseau peuvent être historisés, analysés et contrôlés par l'administrateur réseau, dans le respect de la législation applicable. Dans ce cas,

1 - Sont concernés par l'enregistrement en vue de contrôle :

- La traçabilité des accès et des utilisations des ressources informatiques ;
- La traçabilité des fichiers stockés, téléchargés ou envoyés.

2 - Ces mesures peuvent être opérées via :

- La mise en place de dispositifs d'historisation de l'utilisation des identifiants personnels des utilisateurs ;
- Un contrôle des adresses IP de connexion, source et destination ;
- Un recensement et une analyse des sites internet les plus visités et des durées correspondantes.

L'historique de cette traçabilité est conservé sur une période glissante ne pouvant excéder six mois.

Article 9 : Finalités du contrôle de l'utilisation des ressources informatiques

Lannion-Trégor Communauté peut être amenée à exercer un contrôle de l'usage des ressources informatiques. Les finalités de ce contrôle sont notamment les suivantes :

- La prévention et la répression des faits illicites ou diffamatoires, des faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits ;
- La protection des intérêts de Lannion-Trégor Communauté, auxquels sont attachés un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;
- La sécurité, le bon fonctionnement technique et l'intégrité du système d'information de Lannion-Trégor Communauté ;

- ☑ Le respect des principes et règles d'utilisation des ressources informatiques, tels que définis par la présente charte.

Lannion-Trégor Communauté respecte le principe de proportionnalité dans la poursuite de ces divers objectifs, conformément aux règles relatives au respect de la vie privée des utilisateurs.

Article 10 : Sanctions

Chaque utilisateur est responsable de l'usage du système mis à sa disposition conformément à la présente charte.

Toute utilisation abusive, détournée ou non conforme de l'outil informatique pourrait être de nature à justifier une sanction (par exemple : sanction disciplinaire ou limitation d'usage des ressources informatiques) ou une éventuelle demande de dommages et intérêts. Elle est également susceptible d'entraîner la responsabilité personnelle de l'utilisateur tant sur le plan civil que pénal.

Dans l'hypothèse où la responsabilité de Lannion-Trégor Communauté serait engagée du fait de l'utilisateur, celle-ci se réserve la possibilité de se retourner contre ce dernier.

Article 11 : La Direction des Systèmes d'Information

Au sein de la Direction des Systèmes d'Information, l'administrateur réseau assure la gestion et la sécurité des accès aux ressources informatiques. Pour se faire, il est autorisé à :

- ☑ Accéder aux informations contenues dans les systèmes qu'il administre à des fins de diagnostic et d'administration du système ;
- ☑ Établir des procédures de surveillance de toutes les tâches exécutées sur les postes afin de déceler les violations ou tentatives de violation de la présente charte, tel que prévu par l'article 9 de la présente Charte ;
- ☑ Prendre des mesures conservatoires en cas d'urgence ou des mesures d'investigation en vue de réaliser les contrôles précités ;
- ☑ Limiter l'accès à certaines ressources, notamment des sites Internet, dont le contenu est contraire aux dispositions de la présente charte ;
- ☑ En cas d'urgence, isoler voire neutraliser toute donnée, fichier ou matériel qui mettrait en péril la sécurité des ressources informatiques.

Si l'administrateur réseau obtient communication volontaire des mots de passe et identifiants de la part de l'utilisateur, il sera soumis à un engagement de confidentialité à l'égard de tout tiers et ne pourra en faire usage que dans les conditions visées à l'article 3.

L'administrateur réseau s'engage à ne pas divulguer les informations auxquelles il accède dans le cadre de ses fonctions lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de Lannion-Trégor Communauté.



La Direction des Systèmes d'Information de Lannion-Trégor Communauté est à disposition pour renseigner tout utilisateur concernant l'application de la présente Charte.