Retour au Dossier Organisationnel
Retour à la liste des procédures

Sujets connexes	Proc#138 - Arrivée d'un collaborateur ou d'un stagiaire Proc#139 - Départ d'un collaborateur ou d'un stagiaire Proc#136 - Poste de travail collaborateur Proc#15 - Droits des personnes (RGPD) Carte d'organisation fonctionnelle Titulaires des fonctions et correspondants

Proc#134 - Charte d'utilisation des ressources informatiques

Informations qualité

Suivi des modifications majeures		
Date	**Auteur**	**Modifications**
12 décembre 2017	Nicolas MARCHAND	Création
1er octobre 2026	Nicolas MARCHAND\ Alexia LABARTHE	Refonte : rôles renvoyés aux fonctions de l'organisation ; règles de mots de passe, de chiffrement et de stockage alignées sur Proc#136 ; ajout du télétravail et de l'usage des téléphones personnels ; départ renvoyé à Proc#139 ; mise à jour des textes légaux et des droits RGPD ; mise au format de la maîtrise documentaire

Suivi des approbations	Cartographie fonctionnelle – fiche de la procédure
Objet	Définir les règles d'accès et d'utilisation des moyens informatiques et de communication de Logeas Informatique, dans les locaux, en mobilité et en télétravail.
Destinataires	**- Validation des modifications :** Gérant **- Approbation du document :** Tous
Origine	Ce document remplace la charte du 12 décembre 2017 (PROC-NFlog-46).

1. Objet et valeur de la charte

Logeas Informatique met à disposition de ses collaborateurs les outils informatiques et de communication nécessaires à son activité. La présente charte fixe les règles d'accès et d'utilisation de ces outils, y compris hors des locaux (télétravail, mobilité). Elle sensibilise aussi chacun aux risques pour la confidentialité et l'intégrité des informations : l'imprudence, la négligence ou la malveillance d'un utilisateur peuvent engager sa responsabilité civile ou pénale, ainsi que celle de l'entreprise.

La charte est diffusée par **note de service** et consultable à tout moment sur cette page. Chaque membre de l'équipe l'approuve dans la cartographie fonctionnelle (article 15) ; chaque nouvel arrivant la reçoit et l'approuve à son arrivée (Proc#138).

2. Définitions

Terme	Sens dans la charte
Utilisateur	Toute personne autorisée à utiliser les outils de Logeas Informatique : salariés, stagiaires, intérimaires, personnels de prestataires, visiteurs.
Outils	Équipements informatiques, de téléphonie et d'impression de l'entreprise, et services en ligne fournis par l'entreprise (messagerie et kSuite d'Infomaniak, dont kDrive et kChat ; gestionnaire de mots de passe Proton ; GitLab ; serveurs et applications LoGeAs).
Données de l'entreprise	Toute information appartenant à Logeas Informatique ou confiée par ses clients.
Données sensibles	Parmi les données de l'entreprise : les bases et sauvegardes des clients, les données personnelles (clients, salariés), les données financières et comptables, les codes sources, les mots de passe et accès. À ne pas confondre avec les « catégories particulières » de données du RGPD (santé, opinions…).
Terminal personnel	Téléphone, tablette ou ordinateur appartenant à l'utilisateur.

3. Rôles

Les rôles sont des fonctions de la carte d'organisation fonctionnelle ; les personnes qui les tiennent sont indiquées dans Titulaires des fonctions et correspondants.

Rôle	Ce que la charte lui confie
Gérant	Autorisations : logiciels hors liste, copie de données sur un support externe, usage d'un terminal personnel ; réception des signalements d'incident ; sanctions.
Correspondant infogérance	Installation et maintenance des postes et du réseau, ouverture et fermeture des accès, accès des visiteurs, journaux techniques.
Correspondant RGPD	Registre des traitements et respect des droits des personnes (Proc#15). Il s'agit d'un référent interne, et non d'un délégué à la protection des données (DPO) désigné auprès de la CNIL.

4. Protection des données personnelles

Le règlement (UE) 2016/679 (RGPD) et la loi n°78-17 du 6 janvier 1978 modifiée encadrent les traitements de données personnelles.

Le Correspondant RGPD tient le registre des traitements de Logeas Informatique ; ce registre est communiqué à toute personne qui en fait la demande. Il veille au respect des droits des personnes : accès, rectification, effacement, limitation, opposition et portabilité, selon Proc#15. Toute personne peut également adresser une réclamation à la CNIL.

Les utilisateurs amenés à accéder à des données personnelles signent en outre l'engagement de confidentialité.

5. Accès et authentification

1. **5.1** Chaque utilisateur reçoit des accès personnels à son arrivée. Ses droits sont limités à ce que demande sa fonction : il n'accède pas aux données dont il n'a pas besoin.
2. **5.2** Les identifiants et mots de passe sont personnels et confidentiels. On ne confie jamais son mot de passe et on ne demande jamais celui d'un collègue. Les comptes partagés sont gérés dans Proton.
3. **5.3** Les mots de passe professionnels sont **conservés exclusivement dans le gestionnaire Proton** fourni par l'entreprise. Ils sont uniques pour chaque service, et longs : au moins 12 caractères, de préférence générés par Proton ou formés d'une phrase. Ils ne contiennent ni nom ni prénom.
4. **5.4** Un mot de passe est changé immédiatement en cas de doute sur sa confidentialité. Il n'y a pas de renouvellement périodique imposé.
5. **5.5** La double authentification est activée sur la messagerie et la kSuite, sur Proton, sur GitLab et sur les applications LoGeAs qui la proposent.

6. Règles de sécurité

Tout utilisateur s'engage à :

1. **6.1** signaler sans délai au gérant toute compromission, réelle ou suspectée, d'un compte ou d'un équipement, ainsi que tout dysfonctionnement ;
2. **6.2** ne pas masquer son identité ni usurper celle d'autrui ;
3. **6.3** ne pas accéder ou tenter d'accéder à des informations qui ne lui sont pas destinées, ni les modifier ou les supprimer ;
4. **6.4** ne pas copier, modifier ou détruire les logiciels de l'entreprise en dehors de son travail ;
5. **6.5** verrouiller sa session dès qu'il quitte son poste ;
6. **6.6** ne copier des données de l'entreprise sur un support externe (clé USB, disque) qu'avec l'accord du gérant, et uniquement sur un support chiffré (article 9.3) ;
7. **6.7** ne pas transférer de messages ou de documents professionnels vers une messagerie ou un stockage personnels.

Les visiteurs n'accèdent au réseau qu'avec l'accord du Correspondant infogérance. Les prestataires qui accèdent aux outils signent la présente charte avant tout accès ; les contrats passés avec eux prévoient une clause de confidentialité.

7. Poste de travail

Le poste est installé selon Proc#136. L'utilisateur :

1. **7.1** ne modifie pas les **réglages de sécurité** du poste : session Windows locale (pas de compte Microsoft), OneDrive désactivé, chiffrement BitLocker, verrouillage automatique de l'écran ;
2. **7.2** peut installer les **outils de travail** prévus par Proc#136 et ses documents techniques (par exemple les outils de développement) ; tout autre logiciel est soumis à l'accord du gérant ;
3. **7.3** ne connecte pas au réseau de l'entreprise un équipement non fourni par elle sans l'accord du Correspondant infogérance ;

4. **7.4** ne déplace pas le matériel fixe ; il garde sous sa responsabilité le matériel nomade qui lui est confié (portable, téléphone, clé) et signale au gérant toute perte, tout vol ou toute dégradation ;
5. **7.5** restitue le matériel de l'entreprise à son départ (Proc#139).

Le Correspondant infogérance peut intervenir à distance sur un poste pour la maintenance. Il prévient l'utilisateur avant toute prise de main sur une session ouverte, et n'accède pas aux contenus personnels.

8. Internet, messagerie, téléphone

8.1 Internet

L'usage d'Internet est professionnel. Un usage personnel ponctuel et raisonnable est toléré, pour des sites dont le contenu n'est pas contraire à la loi et ne nuit pas à la réputation de l'entreprise.

8.2 Messagerie

- La messagerie est professionnelle ; un usage personnel raisonnable est toléré.
- Un message ou un dossier est **personnel** s'il est identifié comme tel, par exemple par un objet ou un nom de dossier commençant par « PERSO ». L'entreprise n'ouvre pas les messages et dossiers personnels. Tout autre message est présumé professionnel.
- En cas d'absence de plus de 3 jours, l'utilisateur active une réponse automatique indiquant un contact de remplacement.
- En cas d'absence imprévue, le gérant peut faire suivre ponctuellement un message professionnel, identifié par son objet ou son expéditeur ; l'utilisateur est informé de la liste des messages transmis.
- **Au départ**, la boîte est redirigée vers contact@logeas.fr avec une réponse automatique (Proc#139). L'utilisateur est prévenu de cette redirection et retire ses messages personnels avant son départ.
- La messagerie instantanée de l'entreprise est kChat ; les autres messageries instantanées ne sont pas utilisées pour le travail.

8.3 Téléphone

L'usage personnel du téléphone de l'entreprise est admis s'il reste raisonnable. L'entreprise ne fait pas de suivi individuel des appels ; elle suit globalement les consommations par rapport aux contrats des opérateurs. En cas de dépassement anormal, le gérant consulte le relevé détaillé de la ligne concernée après en avoir informé l'utilisateur.

9. Données de l'entreprise

1. **9.1** Les données de l'entreprise sont stockées sur ses outils : kDrive, GitLab, serveurs et applications LoGeAs.

2. **9.2** Une copie locale n'est admise que sur le disque de données chiffré d'un poste fourni par l'entreprise (Proc#136) : image synchronisée de kDrive, dépôts de code, bases de travail. Aucune donnée de l'entreprise n'est conservée sur un équipement ou un stockage personnel (y compris un service de sauvegarde en ligne personnel).
3. **9.3** Tout support contenant des données sensibles est chiffré. La solution de l'entreprise est **BitLocker** ; les clés de récupération sont conservées dans Proton (Proc#136).
4. **9.4** Une base client n'est copiée sur un poste que pour une assistance ou un test, et effacée dès qu'elle n'est plus utile. Lorsque le test ne nécessite pas de données réelles, la base est anonymisée.
5. **9.5** Hors des locaux, l'utilisateur veille à ce que son écran ne soit pas visible par des tiers lorsqu'il affiche des données sensibles.
6. **9.6** Les documents imprimés contenant des données sensibles sont détruits après usage.

10. Télétravail et mobilité

Ces règles s'appliquent en complément de toutes les autres, dans les conditions prévues par l'avenant de télétravail de chaque salarié.

1. **10.1** Le télétravail se fait avec le matériel fourni par l'entreprise. L'usage d'un terminal personnel n'est possible que dans les conditions de l'article 11.
2. **10.2** L'accès aux **serveurs** de l'entreprise se fait uniquement par le **VPN** fourni. Les **outils en ligne** (messagerie, kSuite, Proton, GitLab, applications LoGeAs) sont accessibles directement, avec double authentification.
3. **10.3** Sur un Wi-Fi public (gare, hôtel), l'utilisateur se limite aux outils en ligne, ou passe par le partage de connexion de son téléphone ou par le VPN.
4. **10.4** L'utilisateur assure la garde du matériel à son domicile et verrouille sa session à chaque absence.
5. **10.5** Les jours et horaires de télétravail sont ceux de l'avenant. Pendant ces plages, l'utilisateur est joignable par téléphone, messagerie et kChat. En dehors, il n'est pas tenu de répondre.

11. Téléphones professionnels et terminaux personnels

11.1 Téléphone fourni par l'entreprise

Il est protégé en permanence par un code ou un moyen biométrique ; ses mises à jour de sécurité sont appliquées dès leur disponibilité ; seules des applications utiles au travail y sont installées.

11.2 Terminal personnel : principe

L'utilisation d'un terminal personnel pour le travail (par exemple les applications de messagerie, kDrive ou kChat sur son téléphone) est une **faculté** : elle n'est jamais imposée, et l'entreprise fournit le matériel nécessaire à qui le souhaite.

Elle est soumise à l'**accord écrit du gérant** (un courriel suffit), qui tient la liste des utilisateurs concernés et des applications autorisées.

Cet usage ne donne lieu à aucune indemnité.

 À confirmer par la gérance.

11.3 Vie privée

L'entreprise n'installe aucun outil de gestion à distance (MDM, MAM) sur un terminal personnel. Elle n'accède jamais à son contenu, ne le localise pas et ne peut pas l'effacer à distance. La sécurité des données professionnelles sur ce terminal repose donc sur l'utilisateur.

11.4 Engagements de l'utilisateur

- Maintenir le système et les applications à jour ; protéger l'appareil par un code ou un moyen biométrique ; activer le chiffrement s'il est disponible.
- N'installer que les applications professionnelles autorisées.
- Signaler sans délai au gérant la perte, le vol ou la compromission de l'appareil, pour que ses accès soient suspendus.
- Ne pas enregistrer de données sensibles sur l'appareil en dehors des applications professionnelles.

11.5 Fin de l'usage ou départ

Au plus tard à son **dernier jour de travail**, l'utilisateur désinstalle les applications professionnelles de son terminal personnel et supprime les données de l'entreprise qui y sont enregistrées. Il est invité à signer l'attestation figurant en annexe 2. Le solde de tout compte ne dépend pas de cette attestation.

De son côté, l'entreprise ferme les accès de l'utilisateur au plus tard le même jour (Proc#139).

12. Administration du système d'information

1. **12.1 Filtrage** : des filtres limitent les courriels non sollicités, les sites dangereux et certains protocoles (pair à pair, messageries instantanées non fournies par l'entreprise).
2. **12.2 Journaux** : les connexions et tentatives de connexion aux outils sont enregistrées (date, poste ou adresse, nature de l'événement). Seul le Correspondant infogérance les consulte, pour résoudre un incident ou assurer la sécurité. Ils sont conservés six mois.

    À confirmer : l'ancienne charte prévoyait trois mois.

3. **12.3 Interventions** : le Correspondant infogérance mène sans avertissement les investigations nécessaires à la résolution d'un incident. Aucun contrôle individuel de l'activité

d'un utilisateur n'est fait sans qu'il en soit informé au préalable.

13. Départ de l'utilisateur

Le départ suit Proc#139. Pour l'utilisateur, cela implique :

- restituer le matériel de l'entreprise ;
- avant de rendre son matériel, retirer ses fichiers et messages personnels, qui seront sinon effacés par l'entreprise ;
- ne conserver aucune copie des données de l'entreprise ; toute exception est autorisée par écrit par le gérant ;
- pour un terminal personnel, appliquer l'article 11.5.

L'entreprise ferme les accès au plus tard le dernier jour de travail, ou dès la date de dispense d'activité. Les comptes et les données personnelles de l'utilisateur sont supprimés dans le mois qui suit son départ.

L'engagement de confidentialité reste valable après le départ.

14. Responsabilités et sanctions

Le non-respect de la charte peut engager la responsabilité de l'utilisateur. Selon la gravité du manquement, il peut donner lieu à un rappel à l'ordre du gérant ou à une sanction disciplinaire, dans le respect du Code du travail.

Le non-respect des textes de l'annexe 1 peut en outre entraîner des sanctions pénales.

Après la fin du contrat, seules les actions prévues par la loi restent possibles, notamment au titre de l'engagement de confidentialité.

15. Entrée en vigueur et mises à jour

La charte est un document permanent : elle s'applique sans limitation de durée, jusqu'à son remplacement par une nouvelle version.

Chaque version suit la maîtrise documentaire (Proc#163) : elle est validée par le gérant, puis approuvée par chaque membre de l'équipe dans la cartographie fonctionnelle. Cette approbation vaut prise de connaissance et acceptation de la charte.

Une version entre en vigueur à la date de sa validation par le gérant. Elle s'applique à chaque membre de l'équipe à compter de son approbation, et à chaque nouvel arrivant à compter de son arrivée (Proc#138).

Une modification de forme ne donne pas lieu à une nouvelle approbation. Une modification des règles fait l'objet d'une nouvelle version, présentée à l'équipe avant sa validation.

Annexe 1 - Textes applicables

- Règlement (UE) 2016/679 du 27 avril 2016, règlement général sur la protection des données (RGPD).
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version issue de l'ordonnance n°2018-1125 du 12 décembre 2018.
- Code pénal, articles 226-16 à 226-24 (atteintes aux droits de la personne résultant des traitements informatiques).
- Code pénal, articles 323-1 à 323-8 (atteintes aux systèmes de traitement automatisé de données, issus de la loi n°88-19 du 5 janvier 1988 dite loi Godfrain).
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).
- Code de la propriété intellectuelle, articles L.335-2 et suivants (contrefaçon, y compris des logiciels).
- Code du travail, article L.1121-1, et Code civil, article 9 (respect de la vie privée).

Annexe 2 - Attestation de fin d'usage d'un terminal personnel

Je soussigné(e) ....., ayant exercé la fonction de ..... au sein de Logeas Informatique, atteste sur l'honneur :

- avoir désinstallé de mon terminal personnel les applications professionnelles qui y étaient installées (messagerie, kDrive, kChat, ou autre outil de l'entreprise) ;
- avoir supprimé les fichiers, courriels, contacts et autres données de Logeas Informatique ou de ses clients enregistrés sur ce terminal ou dans ses sauvegardes ;
- ne conserver aucune copie de ces données.

J'ai été informé(e) que Logeas Informatique ne dispose d'aucun moyen d'intervenir sur mon terminal personnel.

Fait à ....., le ...../...../.....

Signature, précédée de la mention « Lu et approuvé » :

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
https://wiki-logeas.fr/certif/doku.php?id=certif:charteinformatique&rev=1790859470

Last update: **2026/10/01 14:57**