Charte « Utilisateurs » des ressources informatiques, numériques et de communication électronique

UES EVEL & QUADRAL

Mise à jour – Septembre 2024

PREAMBULE

L'Unité Economique et Sociale *(UES)* EVEL & QUADRAL met en œuvre un système d'information et de communication nécessaire à l'exercice de son activité. Sont ainsi mis à disposition des collaborateurs : des équipements et applications informatiques, numériques et de communication électronique dans le cadre de leur activité professionnelle.

La présente charte définit les règles et les bonnes pratiques que tout utilisateur doit respecter lors de l'utilisation des ressources informatiques mises à disposition du personnel de l'UES. Elle vise à garantir un usage sécurisé, éthique et conforme à la législation en vigueur.

Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de règles de sécurité et de bonne conduite. En effet, l'imprudence, la négligence ou la malveillance d'un utilisateur peuvent avoir des conséquences graves, de nature à engager sa responsabilité civile et / ou pénale ainsi que celle des structures composant l'UES.

1. QUELQUES DEFINITIONS

On désignera sous le terme *« Utilisateurs »* toute personne autorisée à accéder aux outils informatiques, numériques et de communication électronique des structures de l'UES et à les utiliser : employés, alternants, stagiaires, intérimaires, prestataires, visiteurs occasionnels ...

Les termes *"outils informatiques, numériques et de communication électronique"* regroupés sous la dénomination *« ressources informatiques »* recouvrent tous les équipements informatiques, de télécommunications et de reprographie des structures de l'UES.

- ***« Administrateur SI »*** : personne spécialement compétente en matière informatique ou ayant une délégation pour gérer tout ou partie des systèmes d'information et/ou de communications électroniques. Dans le cadre de son activité, il possède des droits étendus quant à l'utilisation et la gestion des ressources informatiques ainsi que des possibilités techniques d'accès aux informations des autres utilisateurs. A ce titre, il est assujetti au devoir de réserve et tenu de préserver la confidentialité des données.

- ***« Donnée à caractère personnel »*** : toute information relative à une personne physique identifiée ou identifiable *(personne concernée),* directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

- ***« Equipement nomade »*** *:* moyens techniques *(ordinateur portable, téléphone mobile, tablettes et éléments accessoires : supports de stockage amovibles, clé USB, équipement réseaux, équipement sans fil)* qui permettent l'accès, le transport ou le stockage de données et qui peuvent être utilisées à l'extérieur de l'entité.

- ***« Ressources informatiques »*** *:* équipements informatiques *(ordinateurs fixes ou portables, serveurs, équipements amovibles, équipements nomades, imprimantes, photocopieurs …),* applications, systèmes d'exploitation, ressources de télécommunication, ainsi que locaux informatiques pouvant être accessibles localement ou à distance, directement ou à partir du réseau administré par la DSI ou un prestataire de services pour le compte d'une structure de l'UES et/ou de la DSI.

- ***« Ressources de télécommunication »*** *:* tout ou partie du système de télécommunication des structures de l'UES et notamment les terminaux de télécommunication tels que les téléphones fixes et mobiles, réseaux informatiques et services comme intranet, internet, messagerie, forum (*ex : Teams, Zoom).*

- ***« Traitement »*** *:* toute opération ou ensemble d'opérations quel que soit le procédé utilisé *(collecte, enregistrement, organisation, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction).*

- ***« Data »*** *:* Données pouvant circuler grâce à internet par un réseau téléphonique ou informatique, hormis les données vocales.

- ***« Délégué à la Protection des Données »*** ou *« Data Protection Officer (DPO) »* : personne chargée de mettre en conformité l'ensemble des traitements de sa structure avec le RGPD.

2. DOMAINES D'APPLICATION DE LA CHARTE

2.1 Personnes concernées

Les obligations décrites s'appliquent à tout utilisateur des ressources informatiques de l'UES pour l'exercice de ses activités professionnelles. Toute personne, qu'il s'agisse d'employés, de sous-traitants ou de visiteurs, est tenue de respecter les dispositions de la présente charte.

2.2 Moyens concernés

Sont visés par la présente l'ensemble des ressources informatiques, qui sont :

- la propriété des structures de l'UES, mis à disposition des utilisateurs à des fins professionnelles ;

- la propriété personnelle de l'utilisateur dont il a obtenu une autorisation d'utilisation dans le cadre professionnel. **L'utilisateur ne peut utiliser à des fins professionnelles des ressources informatiques qui sont sa propriété personnelle, qu'avec l'autorisation de la DSI et de sa hiérarchie**, sous réserve du respect des prescriptions techniques exigées.

2.3 Usages concernés

La présente charte s'applique à tous les types d'usage qu'ils aient lieu :

- Dans les locaux des structures de l'UES ;

- Dans le cadre d'un usage dit *« nomade »,* quel que soit le lieu ;

- Dans le cadre d'un accès à distance *(ex : télétravail),* quel que soit le lieu.

3. LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION DE L'UES

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par l'UES.

3.1 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation de comptes sécurisés *("login" ou identifiant)* fournis à l'utilisateur lors de son arrivée.

Les moyens d'authentification sont strictement personnels et confidentiels. En aucun cas ils ne doivent être partagés, l'utilisateur étant responsable de toute action réalisée avec son identifiant. Ils varient en fonction des équipements et applications utilisées. Dans certains cas, une authentification renforcée est mise en œuvre pour réaliser des opérations sensibles.

3.2 Les règles de sécurité

Les utilisateurs doivent impérativement respecter les règles de bonne conduite définies ci-dessous en ne traitant pas de données à caractère personnel sans s'être assuré du respect des dispositions légales et règlementaires relatives à la protection des données auprès du DPO de l'UES.

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- **Signaler par tous moyens à votre convenance à la DSI toute violation ou tentative de violation suspectée de son compte utilisateur** et de manière générale tout dysfonctionnement / comportements suspects liées à la sécurité informatique ;

- **Ne jamais divulguer ses mots de passe** *(y compris aux équipes informatiques)* ;

- Ne jamais demander son mot de passe à une autre personne ;

- Ne pas utiliser son mot de passe professionnel sur un service privé ;

- Ne pas utiliser un identifiant ou un mot de passe d'un autre collaborateur ;

- **N'utiliser que les applications préinstallées par la DSI** sur les équipements ainsi que les outils qui sont d'usage dans l'entreprise. Le collaborateur est pleinement responsable des conséquences qu'auraient l'installation, par lui, d'applications tierces ou d'outils qui ne sont pas en rapport avec les usages de l'entreprise et/ou avec les instructions de la DSI. En cas de doute, la DSI doit nécessairement être interrogée.

- Ne pas copier, modifier, détruire les applications propriétés des structures de l'UES ;

- Veiller à ce que l'ordinateur et/ou smartphone soient verrouillés dès lors qu'ils ne sont pas utilisés ;

- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations sur lesquelles les utilisateurs ne sont pas habilités ;

- Ne pas envoyer de messages à caractère injurieux, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de porter atteinte à la vie privée des personnes ou à leur dignité, relatifs à la race, l'origine nationale, les mœurs, la religion, les opinions politiques, les origines sociales, l'âge ou le handicap. L'envoi de tels messages pourra entraîner des sanctions disciplinaires ;

- Ne pas consulter, copier ou télécharger le contenu de fichiers ou de sites à caractère pornographique, pédophile, négationniste, raciste ou xénophobe ou contraire aux bonnes mœurs ou à l'ordre public. Les actes passibles de sanctions pénales seront dénoncés, à qui de droit, par la Direction Générale de la structure concernée, sans préjudice des sanctions de nature disciplinaire telles que prévues au règlement intérieur de l'UES ;

- Ne pas utiliser les ressources de l'UES à des fins de harcèlement, menace, chantage et, de manière générale, à la violation des droits en vigueur ;

- Ne pas falsifier le contenu et les propriétés d'un fichier ;

- Ne pas télécharger ou utiliser tout fichier et/ ou document illégal ou portant atteinte aux droits d'auteurs *(fichiers de musique, vidéos, logiciels, …)* dans les systèmes d'information de l'UES ;

- **Ne pas utiliser de services en ligne non validés par la DSI**, notamment les services de stockage/d'échange de données pour stocker, partager, communiquer ou échanger des informations professionnelles ;

- Ne pas diffuser ou utiliser l'adresse mail professionnelle sur des sites Internet/applications sans rapport avec l'activité professionnelle ;

- Ne pas porter atteinte aux dispositifs de sécurité interdisant les reproductions ou communications des données professionnelles, porter atteinte à la réputation de l'entreprise ou constituer pour elle une gêne quelconque ;

- Ne pas connecter de clé USB ou tout autre équipement de stockage externe à un équipement de l'entreprise. L'utilisation d'outils de partage de fichiers sécurisés et validés par l'entreprise est à privilégier ;

- Ne pas désactiver ou contourner les procédures de sécurité mises en place par la DSI telles que les antivirus, les pare feux, le paramétrage des équipements interdisant certaines actions ou plus généralement tout autres mécanismes de sécurisation existant ;

- Respecter les consignes de sécurité définies par la DSI *;*

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès aux systèmes d'information sans l'accord préalable du service informatique. Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre les sociétés de l'UES et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation conformément aux dispositions du RGPD notamment.

4. LES MOYENS INFORMATIQUES

4.1 Configuration du poste de travail

Les structures de l'UES mettent à disposition de chaque utilisateur un poste de travail doté des applications nécessaires à l'accomplissement de ses missions ou sa fonction *(ex : ordinateur fixe et/ou nomade, smartphone)*.

L'utilisateur ne doit pas :

• Modifier ces équipements et leur fonctionnement, leur paramétrage, leur branchement ainsi que leur configuration physique ou logicielle ;

• Déplacer l'équipement informatique, sauf autorisation ou s'il s'agit d'un équipement nomade ;

• Nuire au fonctionnement de ces outils et applications.

4.2 Equipements nomades

Les équipements nomades professionnels mis à disposition des utilisateurs font l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Préconisations : l'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent être verrouillés de manière à prévenir tout accès non autorisé aux données qu'ils contiennent. Remplacer le code PIN par défaut *(ex : cartes SIM "0000")* par un code à 4 chiffres plus sécurisé *(pas de chiffres identiques …).* Idem code de déverrouillage de l'écran du smartphone.

L'usage de terminaux personnels est toléré sous certaines conditions :

− L'utilisateur concerné doit obligatoirement en informer préalablement la DSI de sa structure, la DSI se réserve le droit de refuser l'usage d'un terminal personnel selon le niveau de responsabilité du collaborateur et donc de la confidentialité des données qu'il peut être amené à traiter ;

− **Il doit maintenir sur son terminal un niveau de sécurité au moins égal à celui des terminaux professionnels** qui lui serait attribués, cela peut aller jusqu'à l'obligation d'installer un antivirus ou un outil de gestion de terminaux mobiles permettant à la DSI de limiter les usages professionnels sur ce terminal. Il doit notamment chiffrer les supports de son terminal, avoir un système de verrouillage automatique en cas de non-utilisation ;

- **L'utilisateur ne peut en aucun cas se prévaloir d'un droit à utiliser un terminal personnel imposant à la DSI ou plus généralement à l'entreprise d'adapter ses process ou règles afin de permettre l'usage de ces terminaux**. La DSI se réserve le droit de ne pas intervenir ou rechercher les causes de dysfonctionnement sur ces terminaux.

L'utilisateur assure la garde et la responsabilité du matériel confié et doit informer les services dédiés en cas d'incident *(perte, vol, dégradation)* afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

4.3 Internet

Les utilisateurs peuvent accéder aux sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient. Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

4.4 Guide de bonnes pratiques des réseaux sociaux

Les réseaux sociaux *(tels que LinkedIn, Facebook, Instagram…)* sont devenus un support marketing et promotionnel importants pour les entreprises, un outil de visibilité vers l'extérieur fondé sur les échanges libres et le partage d'informations. Ils apparaissent comme un vecteur de communication indispensable.

Cependant, n'offrant que des garanties très limitées en termes de confidentialité et protection des données qui y sont déposées et d'authentification des utilisateurs qui y sont connectés, l'utilisation non conforme de ces services est susceptible d'engager la responsabilité de l'utilisateur. Une vigilance renforcée est donc indispensable.

Il est recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle. Ces services ne doivent donc pas être utilisés pour la diffusion ou le partage d'informations confidentielles de l'entreprise même entre collaborateurs de l'UES.

De manière générale, toute publication d'information interne, financière, stratégique de l'entreprise est interdite.

L'utilisateur doit veiller au respect des lois et règlements et par conséquent il ne doit pas faire de commentaires injurieux, diffamatoires envers son employeur. Il est personnellement responsable des contenus ou commentaires publiés sur ces services.

L'entreprise se réserve le droit de limiter l'accès à tout ou partie de ces services qui pourraient représenter une menace pour son système d'information.

4.5 Messagerie électronique

Conditions d'utilisation

Les outils de messagerie électroniques *(ex : e-mail, outil collaboratif, sms, messagerie instantanée, etc.)* mis à disposition des utilisateurs sont destinés à un usage professionnel. L'utilisation de ces outils à des fins personnelles est tolérée si elle n'affecte pas le travail du salarié ni la sécurité du réseau informatique de l'UES.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message sera présumé professionnel.

Les structures de l'UES s'interdisent d'accéder aux dossiers et aux messages identifiés comme privé notamment *« personnel »* ou *« syndical »,* etc … dans l'objet de la messagerie du salarié d'une des structures de l'UES.

Le transfert de messages professionnels, ainsi que leurs pièces jointes, sur des messageries personnelles est strictement interdit.

Les salariés peuvent consulter leur messagerie à distance sur tous les équipements informatiques à leur disposition *(professionnels et/ou personnels).* Les informations qui seraient copiées sur l'équipement utilisé par le salarié dans ce cadre doivent être effacées dès que possible de l'ordinateur utilisé.

Droits de consultation de la messagerie e-mails

En cas d'absence d'un salarié en activité et afin de ne pas interrompre le fonctionnement du service, les services informatiques peuvent, via une demande formalisée par mail, émise par le responsable et validée par la Direction Générale de la structure :

▪ Activer une notification d'absence générique sur la messagerie du salarié comportant les coordonnées à utiliser afin de réorienter les correspondances et d'informer les correspondants internes et externes du salarié.

▪ Donner accès à une personne à la messagerie e-mail du salarié concerné pour consultation ponctuelle de messages électroniques à caractère professionnels. Tout e-mail est considéré comme relevant du domaine professionnel dès lors qu'il n'est pas indiqué comme *« Privé »* ou *« Personnel ».* Pour ce faire, le *« demandeur »* transmet à son *« Responsable »* la justification de sa demande par mail. Une fois validée, celle-ci parvient

au Directeur Général de la société concernée qui décide en dernier ressort de l'acceptation ou pas de la demande. En cas de réponse positive, il informe la DSI de son acceptation d'ouvrir pour une durée déterminée au *« demandeur »* la messagerie de la personne absente pour traiter / récupérer les données nécessaires à la continuité des missions du service. Un message automatique de la DSI est transmis à l'utilisateur concerné afin d'indiquer l'activation et la désactivation du dispositif de consultation.

Courriel non sollicité

La DSI dispose d'un outil permettant de lutter contre la propagation des messages non désirés *(spam).* Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel. Il est en outre rappelé que chaque utilisateur doit signaler les messages indésirables qu'il peut toutefois recevoir.

4.6 Téléphone et usages en mobilités *(data)*

Les structures de l'UES mettent à disposition de certains utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Les usages donnant lieu à des facturations surtaxées *(ex : sms ou services payants)* sont interdits sauf cas de nécessité justifiée *(ex : services médicaux d'urgence, astreintes techniques, etc …).*

Les usages internationaux des téléphones mobiles *(voix et data)* peuvent être activés sur demande justifiée auprès des gestionnaires en charge de la gestion de la téléphonie de chaque structure de l'UES.

En cas de dépassement des limites des contrats établis avec les opérateurs, ou en cas d'utilisation manifestement anormale détectée, les structures de l'UES se réservent le droit de réaliser une analyse détaillée des usages.

4.7 Protection de la vie privée

Etant donné que tous les fichiers présents sur un ordinateur de travail sont supposés être professionnels, l'entreprise peut accéder à l'ensemble des données, fichiers et messages électroniques stockés sur le matériel mis à disposition.

Cependant, à l'exception de situations particulières, présentant un risque pour la sécurité du SI, l'entreprise ne pourra accéder aux données, fichiers et messages électroniques expressément désignés comme « personnels » ou « privés » par son utilisateur (exemple : fichiers rangés dans un répertoire nommé « personnel ou confidentiel » ou mails avec l'indication « personnel » en début du champ « objet »).

En cas de départ d'un collaborateur, l'ensemble des données privées qu'il laisserait dans les systèmes d'information seront détruites dans un délai maximum de 6 mois après son départ.

5. L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information, différents dispositifs sont mis en place :

5.1 Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mis en œuvre *(filtrage des sites Internet, élimination des courriels non sollicités, blocage de certains protocoles…).*

5.2 Les systèmes automatiques de traçabilité

La DSI opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité. Elle s'appuie pour ce faire, sur des fichiers de journalisation *(fichiers « logs »)* qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement. La DSI est la seule utilisatrice de ces informations.

5.3 Gestion du poste de travail

A des fins de maintenance informatique, les services informatiques peuvent accéder à distance à l'ensemble des postes de travail, avec l'autorisation expresse de l'utilisateur.

6. TRAVAIL A DISTANCE

Il est possible d'accéder au système d'information en dehors des locaux dédiés dans le cadre du travail à distance *(missions professionnelles, télétravail)*.

Tout utilisateur à distance du Système d'information s'engage à respecter les règles de sécurité informatiques intégrées dans cette Charte et à mettre en œuvre tous les protocoles visant à assurer la protection des données de l'entreprise et leur confidentialité. Il est rigoureusement interdit de stocker de manière pérenne des données professionnelles sur un équipement n'appartenant pas à ces structures.

Il est nécessaire de verrouiller la session lors d'une d'absence prolongée pour éviter toute intrusion du SI par des tiers, des membres de la famille... Il faut également protéger autant que possible les écrans des regards indiscrets notamment en cas de travail sur des données sensibles *(clients, financières...)* et stocker l'équipement informatique si nécessaire dans un lieu sécurisé.

7. PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer aux services informatiques tous les équipements professionnels mis à sa disposition *(ordinateur, téléphone mobile, etc.)*.

A la date de son départ effectif *(fin de contrat de travail),* l'ensemble des accès aux applications et aux fichiers ou données sont supprimés.

Concernant les données personnelles :

− L'utilisateur doit préalablement organiser avant son départ effectif, la récupération éventuelle de ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le responsable.

− Les comptes et les données personnelles *(hors ressources humaines)* de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum de 6 mois après son départ.

Concernant la messagerie :

− Le départ effectif *(fin de contrat de travail)* d'un utilisateur entraînant immédiatement la fin d'accès à sa boîte aux lettres, il doit donc préalablement à son départ, prévenir ses contacts par une réponse automatique les informant :

1) Qu'il ne fait plus partie des effectifs ;

2) Qu'une autre personne est désignée pour, prendre en charge leur besoin et/ou desiderata éventuellement.

− Il est de la responsabilité de l'utilisateur de :

1) Supprimer ses messages à caractère privé de sa boîte aux lettres électronique professionnelle ;

2) Prévenir ses interlocuteurs « privés » de son départ, et de communiquer le cas échéant une nouvelle adresse mail.

- Concernant la gestion des accès relatifs à des situations spécifiques *(maternité, longue maladie, licenciement pour faute, mise à pied à titre conservatoire),* les accès à la messagerie pourront être suspendus sur demande de la Direction Générale ou de la Direction des Ressources Humaines.

8. RESPONSABILITES - SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre conformément aux dispositions du Règlement Intérieur de l'UES.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est susceptible de sanctions pénales prévues par la loi.

9. EVOLUTION DE LA CHARTE

Cette charte peut être modifiée à tout moment pour s'adapter aux évolutions technologiques, réglementaires ou législatives. Toute modification sera communiquée préalablement aux utilisateurs.