Charte d'utilisation des moyens informatiques et des outils numériques

Rhenus Logistics Alsace
5 rue du Havre
67000 Strasbourg, France

Table des matières

1 Domaine de validité

Rhenus Logistics Alsace : tous les sites et activités

2 Objectif et but

Ce document est la charte d'utilisation des moyens informatiques et des outils numériques, entre le collaborateur de Rhenus Logistics ci-après dénommé « l'utilisateur » et Rhenus Logistics ci-après dénommé l'«entreprise ».

Cette charte a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'entreprise et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif.

Il incombe à l'utilisateur une utilisation raisonnée et responsable des ressources informatiques et technologiques de l'entreprise mises à sa disposition.

Cette charte clarifie les droits et les devoirs relatifs à l'usage des systèmes d'information conformément au cadre légal et la politique en vigueur dans le groupe Rhenus.

L'utilisateur bénéficiera de formations à caractères obligatoires pour tester ses acquis sur la présente charte.

3 Moyens mis à disposition

Tout l'environnement mis à disposition des utilisateurs est destiné à un usage exclusivement professionnel. Les règles s'appliquant sont définies dans le cadre du périmètre couvert par les sections suivantes.

L'utilisateur est tenu d'utiliser uniquement les moyens mis à disposition par l'entreprise. L'usage de tout autre moyen que ceux mis à disposition par l'entreprise est interdit. Si l'utilisateur devait avoir un besoin supplémentaire il devra en référer au Service Informatique pour analyse et le cas échéant, définition des moyens complémentaires.

3.1 Authentification

Tout utilisateur se verra attribuer les privilèges nécessaires et suffisants pour assurer les missions qui lui sont confiées dans le cadre de l'utilisation des systèmes d'information de l'entreprise :

- un compte d'accès aux services de l'entreprise (ouvrant les accès aux ressources réseaux et systèmes), par exemple :

Le compte de l'utilisateur dans l'Active directory RHS.ZZ respecte la convention *prénom.nom.*

- des accès complémentaires :

- logiciels
- email
- ressources pour le stockage des données

Les privilèges de l'utilisateur sont automatiquement suspendus lors de la cessation même provisoire de l'activité professionnelle ou pourront l'être dès lors qu'un usage illicite ou abusif du compte est suspecté ou démontré.

3.2 Matériels informatiques

Les matériels doivent être maintenus en état de propreté par l'utilisateur auquel ils ont été confiés. Le nettoyage est à faire tout matériel éteint. L'utilisateur s'engage à éteindre le matériel tous les soirs à la fin de l'activité.

Tout matériel en possession de l'utilisateur doit être remis au Service Informatique avant de quitter l'entreprise.

Dans le cadre de l'exécution de ses tâches à son poste de travail, si un utilisateur fait preuve à l'entreprise d'un besoin avéré de dispositifs adaptés, le Service Informatique mettra en œuvre les moyens nécessaires.

Tout vol ou détérioration volontaire ou non du matériel doit immédiatement être signalé au Service Informatique.

3.3 Stockage des données

Chaque utilisateur se voit attribuer les accès suivants:

- un espace d'entreprise individuel accessible uniquement par lui-même
- un ou plusieurs répertoires partagés, en fonction de son appartenance à un ou plusieurs groupes définis d'utilisateurs travaillant en commun
- l'accès au disque local de son poste de travail sur lequel aucune information nominative ou confidentielle ne doit être conservée.
- un répertoire personnel servant à stocker uniquement ses informations privées

L'outil de messagerie ou e-mail n'est pas un système de stockage de documents. Il est conseillé de sauvegarder les emails critiques dans un des répertoires listés ci-dessus (impression PDF ou fichier email) ainsi que leurs pièces jointes également.

Pour les échanges des fichiers volumineux avec des tiers, il est obligatoire d'utiliser de la plateforme sécurisée Rhenus Sharebox (accessible via My Rhenus).

3.4 Principe de délégation

Pour assurer la continuité des activités de l'entreprise, un principe de délégation est mis en place.

Avec le support de son responsable hiérarchique un utilisateur désigne une personne de confiance.

En cas d'absence et/ou du départ de l'utilisateur, la personne désignée par l'utilisateur aura accès au contenu professionnel de la boite aux lettres, au calendrier et à l'espace d'entreprise individuel.

Pour la mise en place de cette délégation, l'utilisateur doit ratifier une déclaration spécifique disponible auprès du Service Informatique.

3.5 Appareils mobiles et télétravail

3.5.1 Politique en matière d'appareils mobiles

Il faut distinguer deux types d'appareils mobiles, les terminaux mobiles et les supports de stockage de données amovibles. Les terminaux mobiles sont équipés d'un système d'exploitation qui permet de stocker des fichiers localement. *Par exemple : Ordinateurs portables / tablettes, Smartphones / téléphones portables.* Les supports de stockage de données amovibles mettent à disposition de l'espace de stockage pour que les informations puissent être lues et écrites à l'aide de terminaux mobiles ou fixes. *Par exemple : disques durs externes, clés USB, Cartes SD et toutes les autres cartes mémoire, disques / CD / DVD / DVD / Blu-ray.*

Les terminaux mobiles et les supports de stockage de données amovibles ne doivent pas être stockés dans un endroit visible afin d'éviter de donner aux voleurs l'occasion d'opérer. Par exemple :

- Voitures: dans la mesure du possible ne laissez pas vos matériels dans la voiture. Si cela n'est pas possible, rangez-les impérativement dans le coffre, car ils sont alors invisibles pour les gens.
- Chambres d'hôtel: dans la mesure du possible ne laissez pas vos matériels dans votre chambre d'hôtel. Si cela n'est pas possible, rangez les matériels dans un coffre-fort, car ils ne sont pas directement visibles si la porte de la chambre est laissée ouverte (par exemple lorsque la chambre est nettoyée et que vous êtes absent).
- Rendez-vous chez le client: les terminaux mobiles, par exemple les ordinateurs portables, doivent toujours être verrouillés, les supports de stockage de données amovibles ne doivent pas être laissés sans surveillance, et assurez-vous que la pièce est verrouillée, par exemple lorsque vous prenez une pause.
- Voyages d'affaires: vous devez transporter des terminaux mobiles et des supports de stockage de données amovibles comme bagage à main.

Vous ne pouvez pas utiliser des supports de stockage de données amovibles privés pour stocker des données professionnelles. Il en va de même pour les supports de données des clients ou partenaires commerciaux.

3.5.2 Télétravail

En déplacement, l'utilisateur doit utiliser une connexion chiffrée fournit par le Service Informatique pour accéder au système d'information de l'entreprise (VPN ou équivalent).

En déplacement à l'étranger, l'utilisateur doit se conformer au cadre juridique local cf. annexe 3. Lorsque vous voyagez à l'étranger, n'enregistrez pas les données confidentielles localement (même si elles sont stockées sous forme chiffrée), mais téléchargez-les via une connexion chiffrée. Avant de commencer votre voyage, renseignez-vous auprès de votre Service Informatique pour savoir s'il existe des règles particulières à appliquer.

Si vous travaillez dans des espaces publics à l'extérieur de l'entreprise (cafés, restaurants, trains, expositions, etc.), utilisez un film de confidentialité sur votre écran (disponible sur demande au Service Informatique) pour éviter que quelqu'un ne regarde discrètement derrière vous pour lire votre écran. Le film de confidentialité ne fournit pas une protection absolue, de ce fait soyez vigilant à votre environnement.

Le chiffrement de vos données n'assure pas une sécurité infaillible, il convient de respecter les règles précitées.

3.6 Logiciels et applications métiers

Les logiciels sont mis à disposition des utilisateurs pour un usage exclusivement professionnel. Les logiciels sont la propriété de l'entreprise et son installés sur le matériel de l'entreprise. Ils ne peuvent être transférés sur un autre poste ou transmis à un tiers sous aucun prétexte.

Il est strictement interdit d'installer d'autres logiciels que ceux fournis par l'entreprise.

Il est impératif d'utiliser la banque de logiciels mise à disposition de l'utilisateur. Toute autre demande doit être adressée au Service Informatique.

Pour toute installation de logiciels soumis à licence ou non, récupérable par téléchargement ou autre moyen, l'accord du Service Informatique est indispensable. Par extension, il est interdit de stocker des données soumises à des droits ou licences que l'entreprise ne possède pas, quel que soit l'emplacement de stockage (partage réseau, poste de travail, support de stockage de données amovible).

A titre d'exception, les droits d'administrateur local peuvent être donnés à l'utilisateur afin qu'il effectue des tâches spécifiques, dans le cadre de ses fonctions. Pour ce faire, celui-ci doit ratifier une déclaration spécifique disponible auprès du Service Informatique.

L'entreprise se réserve le droit de mettre en place un processus automatique de verrouillage et de déconnexion des comptes d'accès en cas d'inactivité prolongée et pour des raisons de sécurité de l'information.

3.7 E-mails et outils collaboratifs

Les e-mails et outils collaboratifs fournis par l'entreprise sont destinés à un usage exclusivement professionnel.

Il est strictement interdit d'installer une adresse email personnelle sur le matériel de l'entreprise

Les e-mails et outils collaboratifs ne doivent pas être utilisés comme vecteur de diffusion de « masse » (tant en termes de volume que de destinataires) ou de chaînes de message nuisibles au bon fonctionnement du réseau.

N'envoyez aucune information confidentielle par email, puisque ceux-ci ne sont pas considérés comme sécurisés, utilisez Rhenus Sharebox ou équivalence communiquée par le Service Informatique.

L'archivage des emails est géré par un serveur :

- Tous les emails de plus de 60 jours qui n'ont pas été stockés dans un dossier "Privé*", "Confidentiel*", "Application*" ou "ImportMigration" seront archivés.

- Tous les emails qui n'ont pas été stockés dans un dossier seront également archivés. Comme le dossier "Envoyé" est également archivé, tous vos messages privés qui ont été envoyés doivent être déplacés dans le dossier "Privé*" afin d'être exclus du processus d'archivage.

3.8 Internet

L'accès Internet est prévu pour une utilisation exclusivement professionnelle dans le cadre des activités de l'entreprise. L'entreprise vérifiera de manière régulière l'utilisation d'Internet.

L'accès Internet est fourni via les fournisseurs d'accès Internet choisis pour le réseau de l'entreprise. Les connexions sont gérées par un serveur mandataire déclaré aux autorités compétentes (Proxy). Pour des raisons de sécurité, il est interdit de mettre en place et d'utiliser des Fournisseur d'Accès Internet et/ou proxy tierces.

Sont aussi proscrites toutes activités qui pourraient entrainer une perte de confidentialité, d'intégrité ou de disponibilité des réseaux ou des systèmes d'information.

Il faut utiliser la version sécurisée (HTTPS) des pages web à chaque fois que cela est possible.

Note : avec les navigateurs Internet il est possible de vérifier l'utilisation de sites sécurisés en s'assurant de la présence du « cadenas » dans la barre d'adresse. Si le cadenas n'est pas visible dans la barre d'adresse, alors le site avec lequel vous communiquez et échangez des données, n'est pas sécurisé. L'utilisateur peut aussi vérifier la validité du certificat et son émetteur par ce biais.

Un accès Wifi public vers Internet est fourni par l'entreprise selon le cadre légal en vigueur (cf. annexe 2).

3.9 Téléphonie

La téléphonie est prévue pour une utilisation exclusivement professionnelle dans le cadre des activités de l'entreprise, sauf en cas d'urgence. Sur demande de son responsable un téléphone fixe et/ou mobile peut être fourni à l'utilisateur.

Trois services de téléphonie mobile sont disponibles *Téléphone sans data*, *Corporate Device* et *BYOD*.

Services de téléphonie mobile	Appels téléphoniques	Accès à E-mail de l'entreprise et à Internet	*Responsable et propriétaire du matériel et de l'abonnement*
Téléphone sans data	**OUI**	NON	L'entreprise
Corporate Device	**OUI**	**OUI**	L'entreprise
BYOD	**OUI**	**OUI**	**L'utilisateur**

En règle générale, l'utilisateur s'engage à :

- Privilégier l'utilisation des numéros abrégés pour effectuer les communications internes à l'entreprise. Les numéros abrégés sont disponible dans l'annuaire en ligne de l'entreprise
- Privilégier l'utilisation des outils collaboratifs reposant sur le réseau Internet (exemple: SKYPE)
- Ne pas utiliser la carte SIM fournie par l'entreprise dans un autre téléphone que celui fourni par l'entreprise, dans le cas contraire l'utilisateur s'engage à rembourser tous les frais qui en découleront
- Protéger et prendre soin de son matériel

Le principe du BYOD est que l'utilisateur amène son matériel et son abonnement propre, et que l'entreprise y installe une application permettant l''accès à la boite aux lettres et au calendrier de l'entreprise. Pour utiliser le service BYOD l'utilisateur doit ratifier une déclaration spécifique disponible auprès du Service Informatique.

3.10 Antivirus

Les systèmes d'information sont équipés d'un antivirus dont la gestion est centralisée. Le Service Informatique a obligation de monitorer l'état et de faire procéder aux mises à jour du logiciel d'antivirus régulièrement.

A charge de l'utilisateur de vérifier que l'antivirus est bien actif, synchronisé, et de valider les pop-up de mise à jour.

En cas d'avertissement du système, de doute ou si l'utilisateur pense que son matériel est victime d'une infection virale, il doit immédiatement éteindre celui-ci et débrancher le câble réseau ou désactiver l'interface wifi (ordinateur portable, téléphone mobile) et avertir le Service Informatique.

Le Service Informatique se réserve le droit de procéder à toute action jugée nécessaire pour contenir une propagation éventuelle d'une infection virale.

3.11 Impressions

Les solutions d'impression sont prévues pour une utilisation exclusivement professionnelle dans le cadre des activités de l'entreprise. L'entreprise vérifiera de manière régulière l'utilisation des solutions d'impressions.

L'entreprise se réserve le droit de mettre en place un processus automatique de limitation ou de blocage des comptes d'accès aux solutions d'impressions en cas de besoin ou d'abus.

3.12 Propriété

L'entreprise étant le seul propriétaire des moyens mis à disposition, elle se réserve le droit à tout moment de les récupérer, sans préavis.

Il est rappelé que l'octroi des moyens quels qu'ils soient par l'entreprise ne crée aucun droit contractuel ou d'usage à en bénéficier pour l'utilisateur.

4 Règles de Sécurité

Les règles de sécurité listées ci-après s'appliquent à l'ensemble des moyens mis à disposition de l'utilisateur par l'entreprise.

Chaque salarié a obligation, à l'expiration de son contrat de travail, quel qu'en soit le motif, de restituer, sans qu'il soit besoin de lui formuler une demande expresse ou une mise en demeure préalable, tous les documents et matériels qui auraient pu lui être confiés ainsi que toutes les copies et reproductions en sa possession à titre professionnel ou autorisées pour son usage personnel.

4.1 Gestion de l'incident de Sécurité

Immédiatement après l'observation ou l'avis d'un événement de sécurité présumé, l'utilisateur doit utiliser les moyens à sa disposition pour signaler sans délai cette connaissance et/ou cette suspicion au Service Informatique.

4.2 Catégorisation de l'information

Il faut distinguer quatre niveaux de confidentialité : Public, Usage Interne, Confidentiel, Personnel

- Public : Information pouvant être publiée vers une audience publique sans risque de dommage à l'entreprise ou à ses partenaires ni aux employés
- Usage Interne : Distribution libre au sein de l'entreprise et au sein des sociétés dans lesquelles nous détenons une participation majoritaire.
- Confidentiel : Seulement à un certain groupe d'employés déterminé par le propriétaire de l'information (principe du besoin de savoir).
- Personnel : Information à caractère personnel

Une mention écrite sur la nature interne du document de l'entreprise et les exigences en matière de protection doit être apposée avant le transfert aux partenaires commerciaux.

L'utilisateur s'engage à respecter une confidentialité stricte des informations auxquelles il a accès et a pu avoir accès dans l'exercice de ses fonctions, et cela dans tous ses domaines d'activité.

Sans approbation préalable du propriétaire d'une information ou d'un fichier à caractère Confidentiel, l'utilisateur destinataire ne doit pas les divulguer à des tiers non autorisés, même au sein de Rhenus, ni durant son emploi chez Rhenus, ni ultérieurement. Cette disposition s'applique à toute information détenue pour les besoins du service ou obtenue fortuitement.

L'utilisateur devra prendre toutes précautions à sa portée pour assurer la confidentialité, la disponibilité et l'intégrité des données, en sa possession ou auxquelles il accède.

Aucune action ne sera réalisée dans le but d'obtenir de façon illicite ou frauduleuse des droits supplémentaires ou des données confidentielles autres que ceux fournis par l'établissement pour les besoins professionnels.

Dans les mêmes conditions, il est interdit d'accéder ou de se faire transmettre sciemment des informations illicites.

4.3 Ethique de l'information

Les informations diffusées ou stockées ne doivent pas contenir d'éléments qui pourraient être considérés comme offensants, diffamatoires, discriminatoires ou méprisants.

Un tel contenu inapproprié inclurait, mais ne s'y limiterait pas, des propos ou images pornographiques, la promotion de causes non liées à l'activité de l'entreprise (incluant mais ne s'y limitant pas à des causes charitables, politiques, religieuses à moins que la cause soit sponsorisée par l'entreprise), du harcèlement électronique, de messagerie pyramidale, d'espaces virtuels de jeux d'argents (paris), d'insultes à caractère raciste, de propos spécifiques à la sexualité, ou tout commentaire qui pourrait offenser une personne à cause de son âge, son sexe, son orientation sexuelle, ses croyances religieuses ou politiques, sa nationalité, son handicap.

4.3.1 Exemples de pratiques informatiques interdites :

- L'usage de clef USB et autres stockages amovibles privés.
- Travailler sous le compte d'accès d'un collègue ou de toute autre personne
- Laisser travailler un collègue ou toute autre personne sous son compte d'accès
- Divulguer ou laisser exposé ses mots de passe
- Quitter l'ordinateur ou son téléphone sans protéger ou verrouiller la session en cours
- Usurper l'identité d'une personne ou intercepter des communications entre tiers
- Conserver sur les disques locaux des PC (C:, D:) des données nominatives ou confidentielles,
- Déposer des documents confidentiels ou nominatifs sur un serveur (répertoire partagé) accessible à des personnes non autorisées à partager ces informations
- Laisser des documents ou impressions confidentiels à la vue de personnes non autorisées

4.3.2 Exemples de bonnes pratiques informatique :

- Se déconnecter
- Verrouiller votre session utilisateur en cours pendant les pauses et en cas d'absence prolongée (utilisez les touches « windows » + « L »)
- Stocker les documents critiques sur le serveur de fichiers
- Ne pas noter ses identifiants sur un papier volant ou au vu et su de tout le monde.
- Utiliser un trousseau sécurisé pour gérer ses mots de passes
- Utiliser des mots de passes différents de ceux que vous utilisez en dehors de l'entreprise
- Commandes vocales : ne les utiliser que pour des informations «Public », désactiver les services inutilisés

4.4 Mots de passe des comptes d'accès

Les mots de passe des comptes d'accès sont strictement personnels et ne doivent pas être divulgués. Le titulaire est responsable des actions effectuées avec ses comptes d'accès.

Les comptes d'accès sont strictement personnels et nominatifs, exceptionnellement des comptes d'accès fonctionnels peuvent être fournis.

Tout utilisateur s'engage à respecter les règles suivantes :

- les mots de passe sont de longueur minimale de 8 caractères et formés de lettres et de chiffres
- pas de mot du dictionnaire toutes langues confondues
- pas de données personnelles, familiales, ou professionnelles
- pas de dates de naissance, noms et prénoms des enfants ou animaux domestiques

Si un utilisateur pense que la sécurité d'un de ses mots de passe a été compromise, il doit le signaler immédiatement au Service Informatique, qui mènera l'action appropriée.

Sur demande d'un utilisateur et dans le cadre de la désignation d'une personne de confiance, le Service Informatique peut réinitialiser les mots de passe des comptes d'accès des systèmes qu'il administre.

Concernant les fichiers (Excel ou autre), en cas de départ et avant son départ de l'entreprise, un utilisateur a obligation de communiquer les mots de passe à son successeur ou à son responsable hiérarchique.

L'entreprise met en œuvre des formations obligatoires de sensibilisation à la sécurité des systèmes d'information, l'utilisateur s'engage à les suivre et à appliquer leur contenu.

4.5 Sauvegardes

Le Service Informatique a obligation de mettre en place des procédures de sauvegarde des données du serveur et des postes de travail.

Les données qui font l'objet d'une sauvegarde sont obligatoirement situées dans :

- *Documents* et *Bureau* du profil de l'utilisateur
- l'espace d'entreprise individuel de l'utilisateur
- les répertoires partagés où un ou plusieurs groupes définis d'utilisateurs travaillent en commun

Ces sauvegardes sont incluses dans la gestion globale des sauvegardes. Toute donnée située en dehors de ces répertoires ne pourra être récupérée par le Service Informatique en cas d'incident.

L'utilisateur peut récupérer les fichiers lui-même en faisant un clic droit sur le répertoire conteneur, puis afficher les versions précédentes dans les propriétés. Il peut alors choisir la version et la restaurer à l'emplacement.

4.6 Accès par un tiers

L'accès d'un tiers aux systèmes d'information de l'entreprise n'est possible qu'avec l'accord préalable du Service Informatique.

En l'occurrence le tiers devra, qu'il soit client ou fournisseur, respecter la politique d'accès en vigueur définie par le Service Informatique.

5 Mesures de contrôles de l'entreprise

L'entreprise s'inscrit dans le respect de la gestion des données à caractère personnel tel que prévu par la CNIL et le Règlement Général sur la Protection des Données « RGPD » (Loi 78-17 du 6 janvier 1978 modifiée), diverses mesures sont mises en œuvre pour atteindre ce but, les voici :

5.1 Mesures techniques

- Autorisation des connexions au réseau de l'entreprise aux seuls équipements maîtrisés
- Attribution des bons droits sur les ressources sensibles du Système d'Information
- Conservation des données de connexion
- Chiffrement des données
- Détection dépose de fichiers non autorisés
- Détection des logiciels soumis à licence
- Filtrages antiviral et anti spams
- Surveillance de la disponibilité des systèmes
- Audit de la robustesse des mots de passe
- Protection des mots de passe stockés sur les systèmes

5.2 Mesures organisationnelles

- Former les utilisateurs à la Sécurité des Systèmes d'Information et évaluer leurs acquis
- Identifier nommément chaque personne accédant aux systèmes et distinguer les rôles utilisateur/administrateur
- Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs
- Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau
- Contrôle des messageries professionnelles
- Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour
- Définir des règles de choix et de dimensionnement des mots de passe
- Changer les éléments d'authentification par défaut sur les équipements et services

6 Sanctions encourues par l'utilisateur

En cas de non-respect de la présente charte, les privilèges de l'utilisateur seront immédiatement suspendus.

Le non-respect de la présente charte par l'utilisateur peut également conduire à l'application des sanctions disciplinaires prévues au TITRE IV du règlement intérieur de l'entreprise.

D'autres sanctions, de nature civile ou pénale, peuvent être prononcées par les juridictions compétentes. L'utilisateur est informé par la présente charte que ses actions peuvent avoir des conséquences juridiques lourdes eu égard à des comportements prohibés.

Liste non limitative des comportements prohibés:

- le non-respect de ses obligations
- le téléchargement illégal
- la consultation de sites à caractère pédopornographique

En complément, si elle le juge nécessaire l'entreprise se réserve le droit d'engager des poursuites conformément aux textes applicables en annexe 1.

7 Validation

En apposant ma signature ci-dessous, je m'engage à respecter toutes les conditions de la Charte d'utilisation des moyens informatiques et des outils numériques de l'entreprise Rhenus Logistics Alsace, et je reconnais avoir lu, compris et j'accepte pleinement le contenu de cette charte et reconnais être lié en totalité de sa disposition.

Nom : _____

Prénom : _____

_____

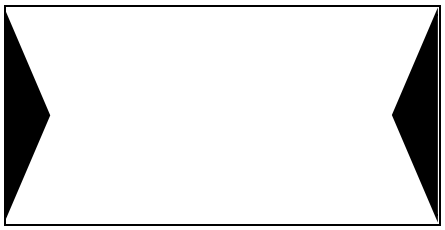
Fonction : _____

Service : _____

Fait à : _____

Le : _____

Signature:



8 Définitions et abréviations

Système d'Information : Un système d'information (SI) est l'ensemble des ressources humaines, matérielles et logicielles permettant de collecter, stocker, rechercher, traiter et diffuser l'information nécessaire à la gestion et à la prise de décision dans un organisme.

Compte utilisateur: Couple identifiant et mot de passe personnels permettant de se connecter aux ressources informatiques d'un SI. Exemple : compte de l'utilisateur dans l'Active directory

Active Directory : Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. Dans le contexte d'un réseau d'ordinateurs, un annuaire (aussi appelé un magasin de données) est une structure hiérarchique permettant de stocker les informations sur les objets du réseau. Ces objets comprennent les serveurs, les volumes partagés et les imprimantes, les comptes d'utilisateur et d'ordinateur réseau, ainsi que les domaines, les applications, les services, les stratégies de sécurité et à peu près tout ce qui reste sur votre réseau. Les informations qu'un annuaire de réseau peut stocker pour un compte d'utilisateur sur un type particulier d'objet sont en général le nom d'utilisateur, le mot de passe, l'adresse de messagerie, le numéro de téléphone, etc
Exemple : l'Active directory RHS.ZZ

Disponibilité : Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

Intégrité : Propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

Confidentialité : Propriété de la non-divulgation à des parties non autorisées.

Données Personnelles : Données qui, au sens de la Loi 78-17 du 6 janvier 1978 modifiée permettent de désigner ou d'identifier, directement ou indirectement, une personne physique.

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ». Une personne peut être identifiée :

- directement : une seule donnée permet d'identifier un individu.
  Exemple : le nom ou le prénom de la personne

- indirectement : une donnée ne permet pas en elle-même de parvenir à l'identification d'un individu, mais une fois recoupée avec une ou plusieurs autres données, la combinaison unique en résultant permet d'identifier la personne
  Exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image

PC : Ordinateur individuel, ordinateur de bureau ou poste de travail.

Carte SIM : La carte SIM (pour « Subscriber Identity Module », terme anglophone) est une puce contenant un microcontrôleur et de la mémoire. Elle est utilisée en téléphonie mobile pour stocker les informations spécifiques à l'abonné d'un réseau mobile, en particulier pour les réseaux GSM, UMTS et

LTE. Elle permet également de stocker des données et des applications de l'utilisateur, de son opérateur ou dans certains cas de tierces parties.

BYOD : abréviation de l'anglais « bring your own device », en français, PAP pour « prenez vos appareils personnels » est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Le BYOD est soumis aux règles de l'entreprise.

9 Documents / processus associés

Numéro de document	Titre	Classe de document
	RHG 005_Policy_Protection of confidential informationen	Usage Interne
RH 2.2.1.14.6	IS.I.USE.20.Administration locale	Usage Interne
RH 2.2.1.14.11	IS.USE.29.Désignation personne de confiance eMail Representative Regulation FR	Usage Interne
n/a	https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee	Public
RH 2.2.1.14.13 A9 AA	IS.D.ORG.9.Organisation Service Informatique Alsace.docx	Usage Interne

10 Annexes

10.1 Annexe 1 –Textes applicables - Code pénal – Extraits concernant le Vol et les systèmes de traitement automatisé de données

Article 311-3

Le vol est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende. […]

Exemple :

- ➔ en utilisant directement un ordinateur (après s'être introduit dans les locaux d'une entreprise par exemple);
- ➔ à distance, en entrant dans un réseau fermé ou prenant le contrôle d'une machine située dans un tel réseau. Cette incrimination vise notamment le fait pour un employé d'utiliser un ordinateur mis à disposition par son employeur pour accéder à des données confidentielles sans relation avec ses fonctions, ou encore pour commettre un délit (par exemple, utiliser les ressources de l'entreprise pour diriger une attaque contre des tiers).

Article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. […]

Exemple :

- ➔ le fait de bloquer un système en organisant une attaque de type déni de service ;
- ➔ le fait de modifier ou d'altérer le fonctionnement du système et de provoquer ainsi une baisse des performances, une altération des résultats, etc. (par exemple par l'introduction volontaire et consciente d'un virus dans le système) ; ou encore
- ➔ le fait de détériorer ou de détruire un système (au niveau matériel et/ou logiciel).

Article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. […]

Exemple :

- ➔ le vandalisme informatique, c'est-à-dire l'accès à un système en vue d'en détruire les données
- ➔ l'utilisateur qui accède illégalement ou non, au serveur de son entreprise et modifie de manière malveillante des fichiers nécessaires aux activités de l'entreprise

Article 323-3-1

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. […]

10.2 Annexe 2 –Textes applicables - Code pénal – Extraits concernant le Wifi et la lutte contre le terrorisme

La mise en place d'un réseau WiFi ouvert au public et ses incidences en matière de traitement de données à caractère personnel est soumise à l'article L34-1 du Code des postes et des communications électroniques.

La loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme, a étendu cette obligation à l'ensemble des personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit.

Le décret du 24 mars 2006 a ainsi créé un nouvel article R.10-13 du CPCE, qui décrit les catégories de données à conserver. Il s'agit :

- des informations permettant d'identifier l'utilisateur (par exemple : adresse IP, numéro de téléphone, adresse de courrier électronique)
- des données relatives aux équipements terminaux de communication utilisés
- des caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication
- des données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs
- des données permettant d'identifier le ou les destinataires de la communication
- Pour les activités de téléphonie : les données permettant d'identifier l'origine et la localisation de la communication

Le décret du 24 mars 2006 fixe la durée de conservation des données à un an, durée au-delà de laquelle elles devront être anonymisées. Ce délai de conservation court dès l'enregistrement des données.

10.3 Annexe 3 – Terminaux mobiles et supports de données à l'étranger

Les lois en vigueur à l'étranger permettent souvent aux personnes employées par les pouvoirs publics d'examiner et de rechercher sur les terminaux mobiles et les supports de stockage de données (y compris les lecteurs MP3, par exemple). Ils font des copies des données existantes et, dans des cas extrêmes, peuvent confisquer l'appareil.

Si les données sont chiffrées, il se peut que l'on vous demande de déchiffrer les données en entrant votre mot de passe. Vous devez vous conformer à cette demande afin d'éviter des problèmes tels que le refus d'entrée ou l'arrestation.

Les pays sont inscrits sur une liste (Pays avec des lois spéciales régissant l'équipement informatique) si nous savons qu'il existe des dispositions légales pertinentes, par ex. les Etats-Unis, la Grande-Bretagne, la Russie, la Chine. Cette liste n'est pas exhaustive et sera mise à jour au besoin (par le biais du retour d'information des employés).

11 Historique de modification

Version	Créé par	Créé le	Modification / Remarque
1.00	Olivier Ueber	26.03.2015	Nouveau model CWA
2.00	Olivier Ueber	04.09.2015	Mise à jour section 3.
3.00	Marc Leitz / Olivier Ueber	15.03.2019	Mise à jour section 3 et intégration bonnes pratiques Sécurité des Systèmes d'Information et cadre légal