Charte d'utilisation

du Système d'Information

Date : 01/06/2018

Version : 1.4

Référence : MAYxxx V1.4 MAYOLY - Charte d'utilisation du Système d'Informations.docx

Périmètre d'application : toutes les entités des Laboratoires Mayoly-Spindler

Signée par Marie-Claude CEVALTE, DSI , le 18/06/2018

Table des matières

1. Préambule 3

2. Objet de la charte 4

3. Champ d'application de la charte 5

3.1 Utilisateurs concernés 5

3.2 Outils informatiques et moyens de communication 5

4. Modalité d'application 5

4.1 Diffusion 5

5. Respect de la législation 6

6. Conditions d'accès aux ressources du SI 7

7. Conditions d'utilisation des postes de travail et équipements nomades 8

8. Conditions d'usage de la messagerie électronique 9

9. Conditions de navigation sur l'Internet 10

10. Contrôle de l'utilisation des ressources du SI 11

10.1 Messagerie 11

10.1.1 Contrôle global 11

10.1.2 Contrôle individuel 11

10.1.3 Conservation 11

10.1.4 Non utilisation ou cessation d'activité 12

10.2 Usage de l'Internet 12

10.2.1 Contrôle global 12

10.2.2 Contrôle individuel 12

10.3 Utilisation de l'espace bureautique : accès aux espaces communs et individuels 12

10.3.1 Contrôle global 12

1. Préambule

L'ensemble de nos sociétés dispose d'un patrimoine d'informations sensibles sur lequel reposent sa performance, sa pérennité, sa sécurité et sa capacité à maintenir et développer ses activités et ses résultats.

Ce patrimoine d'informations recouvre :

- Les informations relatives aux produits, à la vente, à la production et à la gestion, nécessaires au fonctionnement de nos différentes entités,
- Le patrimoine intellectuel, composé de toutes les informations concourantes au savoir et au savoir-faire de nos sociétés,
- Les informations relatives aux clients ou aux tiers avec lesquels nos sociétés sont en relation, dont l'altération ou la divulgation pourrait porter atteinte à l'image de marque de nos sociétés, à celle de leurs clients ou des tiers concernés, voire entraîner des poursuites judiciaires,
- Les informations relatives au personnel, telles que les dossiers administratifs, dont la divulgation constituerait une violation de la vie privée.

La protection de ce patrimoine et, par extension, du Système d'Information (SI) qui le gère, est plus que jamais essentielle et s'avère en cela un objectif majeur.

Sa **disponibilité** est essentielle pour garantir les engagements de services que nous avons pris envers nos clients. **L'intégrité** et la **confidentialité** des informations gérées au moyen de ce système doivent être préservées, afin de maintenir nos avantages concurrentiels et de conforter la confiance de nos clients et fournisseurs.

Comme la qualité, la sécurité ne peut être obtenue dans la durée que par **une action à la fois collective et individuelle**.

Chacun doit être **conscient des exigences** qui s'imposent à lui pour **prévenir les risques** et, pour cela, disposer de l'information et de la formation indispensables pour être un acteur de la sécurité, conscient de ses droits et de ses devoirs comme des responsabilités qui sont les siennes envers lui-même et envers sa société.

Afin de nous **guider** dans nos comportements au quotidien, une charte d'utilisation du système d'information a été élaborée. **Son application est l'affaire de tous**, dans l'intérêt de chacun. La méconnaissance de la législation, l'ignorance des risques encourus ou une mauvaise application des règles de sécurité peuvent être lourds de conséquences, pour notre entreprise comme pour chacun d'entre nous, puisque nous engageons notre propre responsabilité.

2. Objet de la charte

Le développement des nouvelles technologies de l'information et de la communication conduit les collaborateurs de nos sociétés à utiliser les outils informatiques, les réseaux et les services de communication au quotidien dans l'exercice de leurs missions.

Afin d'en faciliter l'usage, il est primordial que chaque utilisateur de ces outils, dénommés ci-après « Système d'information », soit informé des règles simples et des bonnes pratiques à appliquer dans le cadre d'une charte d'utilisation. La présente charte a donc notamment, pour objet de :

1) **Définir les conditions d'une bonne utilisation des ressources partagées et dans le respect des lois et de l'éthique.**
2) **Porter, à la connaissance des utilisateurs en parfaite transparence, les règles mises en place pour garantir la sécurité des systèmes.**

La mauvaise utilisation des nouvelles technologies de l'Information et de la Communication peut comporter certains risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées.

Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'entreprise.

D'autres conséquences peuvent être l'altération de l'image de marque ou de la confiance accordée à nos sociétés et la perte de marchés importants.

Cette charte est l'occasion de rappeler que l'usage personnel par les salariés des outils informatiques et des moyens de communication mis à sa disposition par l'employeur est toléré si l'utilisation est **PONCTUELLE durant le temps de travail et ne nuit pas au bon exercice des fonctions tenues**. **Tout manquement à cette règle pourra entraîner des sanctions disciplinaires.**

3. Champ d'application de la charte

3.1 Utilisateurs concernés

Cette charte s'applique à **toute personne se servant** des outils informatiques et des moyens de communication de nos sociétés, quel que soit son statut, notamment : salarié, intérimaire, prestataire et (ses) éventuel(s) sous-traitant(s), stagiaire, personnels, (ci-après dénommé « utilisateur).

3.2 Outils informatiques et moyens de communication

Les termes outils informatiques et moyens de communication recouvrent tous les équipements informatiques, numériques, électroniques, téléphoniques et de reprographie de la société, quels que soient leur propriétaire, (location, leasing …), ainsi que les logiciels, fichiers, données et bases de données, systèmes de messagerie, intranet, extranet, abonnements à des services interactifs.

Le réseau et l'intégralité de ses composants, (matériels et logiciels), sont également considérés comme faisant partie des outils informatiques et moyens de communication.

Pour des besoins évidents de sécurité et de protection du Système d'Information, le matériel personnel des salariés ne doit pas être connecté au réseau de nos sociétés.

4. Modalités d'application

La présente Charte entrera en vigueur un mois après l'accomplissement des formalités d'affichage et de dépôt. Elle s'imposera à tous les salariés dans la mesure où ces derniers utilisent :

- les outils informatiques
- les moyens de communication
- le réseau physique de nos sociétés

La présente charte a fait l'objet d'une information et d'une consultation des Institutions Représentatives du Personnel (IRP), afin de recueillir leurs avis.

La charte sera annexée au règlement intérieur de nos sociétés et toute modification devra faire l'objet d'une nouvelle information aux Institutions Représentatives du Personnel (IRP).

4.1 Diffusion

La présente Charte annulera et remplacera toute charte informatique interne ou dispositions diverses (règlement intérieur, …) existant à ce jour au sein de nos sociétés.

L'existence de cette charte sera communiquée par messagerie interne aux collaborateurs présents dans l'entreprise au moment où elle prendra effet.

La dernière version de la Charte Informatique sera consultable sur l'intranet de l'entreprise.

5. Respect de la Législation

La loi s'appliquant à tous, chaque collaborateur peut être tenu responsable civilement et pénalement dans ses fonctions au quotidien, en cas de manquement aux obligations légales et/ou réglementaires.

Les diverses dispositions du cadre légal français et européen dans le domaine des systèmes d'information doivent être appliquées au sein de nos sociétés. Elles portent notamment sur la **protection des droits d'auteurs de logiciels**, le **secret des correspondances**, la **protection des données à caractère personnel**, la **lutte contre les accès illicites aux ressources du Système d'Information ou leur utilisation frauduleuse** et la **protection de la dignité humaine**.

L'utilisateur doit :

- Protéger les droits de propriété de l'entreprise pour l'ensemble de ses savoirs et savoir-faire.
- Respecter strictement le secret professionnel et garantir la confidentialité des informations internes à nos sociétés.
- Respecter le secret des correspondances et communications adressées à des tiers et la vie personnelle des personnes.

L'utilisateur ne doit pas :

- Consulter, télécharger, diffuser, mettre à disposition ou stocker des informations pouvant porter atteinte à la dignité humaine (diffamation, injure…) ou contraires à la législation (pédopornographie, racisme, apologie des stupéfiants…) ou rentrant dans le cadre de la loi Hadopi (film, musique, …).
- Installer ou distribuer un logiciel commercial sans licence ni déjouer tout dispositif anti-copie, ni dupliquer des installations logicielles au-delà du nombre prévu dans le contrat de licence : il se rendrait alors coupable de délit de contrefaçon.
- Diffuser en dehors de l'entreprise toute information confidentielle sans l'accord préalable de la Direction.
- Accéder sans autorisation aux ressources du SI, perturber leur fonctionnement, introduire ou modifier des données de façon frauduleuse.
- Utiliser ou détourner à son profit ou à celui de tiers tout ou partie du système d'information auquel il a accès, que ce soit ou non dans l'exercice de ses fonctions.
- Collecter des informations nominatives (en dehors des données requises par l'utilisation normale des applications métiers délivrées par la DSI et le service RH) sans information préalable des personnes concernées, divulguer ou utiliser ces informations sans leur consentement préalable ou opérer de tels traitements sans avis favorable de la CNIL, conformément au futur Règlement Général de la Protection des Données (RGPD européen).
- Collecter des informations personnelles interdites au regard de la loi (origines raciales, opinions politiques, philosophiques, religieuses, appartenance syndicale, mœurs, santé et vie sexuelle, ……).

6. Conditions d'accès aux ressources du SI

Le contrôle des accès aux différentes ressources du SI est un dispositif transverse dont l'efficacité est un élément clé pour la sécurité, à la fois pour garantir la disponibilité des ressources de tout dysfonctionnement non accidentel, pour protéger l'intégrité et la confidentialité des informations de malveillances potentielles, et aussi, pour être en mesure de justifier des opérations réalisées à travers le SI.

L'accès aux ressources du système d'information de l'entreprise n'est autorisé que dans le **cadre de l'activité professionnelle** des collaborateurs, définie par leur fonction et dans les limites de délégation qui leur sont accordées. Un usage personnel est autorisé s'il est **ponctuel durant le temps de travail et ne nuit pas au bon exercice des fonctions tenues**.

L'accès aux ressources du système d'information est soumis à l'usage d'un **authentifiant individuel strictement personnel** (mot de passe) dont l'utilisation engage la responsabilité de l'utilisateur ou du visiteur. Les exceptions potentielles à ce principe dans certains environnements sont recensées par les services informatiques et validées par la Direction.

Les droits d'accès peuvent être révoqués à tout moment, et prennent fin en cas de suspension momentanée ou définitive de l'activité professionnelle, en conformité avec le code du travail.

L'utilisateur doit :

- Choisir des mots de passe robustes, c'est-à-dire difficile à découvrir par un tiers (composés d'au moins 8 caractères associant des chiffres, des majuscules et minuscules) et en préserver la confidentialité (mémorisation, saisie à l'abri des regards) et la validité sur la période prévue.
- Changer régulièrement ses mots de passe (au moins tous les 3 mois) et les modifier immédiatement en cas de suspicion de divulgation du secret.
- Limiter son usage du SI dans un contexte non professionnel et identifier clairement sans ambigüité, les informations à caractère privé et/ou personnel dans l'objet d'un message électronique ou le nom d'un support de stockage et assurer la sécurité de ces informations qui est de sa seule responsabilité. Pour la circonstance l'usage du mot « *Privé* » sous cette orthographe sera usité.

L'utilisateur ne doit pas :

- Communiquer ou céder, même temporairement, son authentifiant à un tiers.
- Ecrire son mot de passe Windows ou l'enregistrer sur le système en vue d'automatiser la procédure d'authentification, en dehors des applications validées par la DSI. Utiliser le même mot de passe pour accéder à des sites personnels.
- Usurper l'identité d'un autre collaborateur ou tenter de s'approprier son authentifiant, ni contourner les restrictions d'accès aux ressources mises à disposition.
- Introduire des failles de sécurité dans l'architecture du système d'information, ou exploiter ou tenter d'exploiter une éventuelle faille de sécurité constatée ou en faire la publicité.
- Limiter l'usage des matériels externes (clé USB, disque dur, …) dont vous n'êtes pas certains de la provenance ou qui pourraient présenter une suspicion.

7. Conditions d'utilisation des postes de travail et équipements nomades

Le poste de travail est le principal point d'accès au Système d'Information mis à disposition des collaborateurs.
C'est par conséquent un composant particulièrement sensible quant à la sécurité et potentiellement vulnérable si de bonnes pratiques d'utilisation ne sont pas adoptées par tous.

Les postes de travail sont configurés selon des standards définis par les services informatiques de l'entreprise qui intègrent les mesures de sécurité nécessaires à la protection du système d'information de l'entreprise. Leurs **conditions d'usage** au quotidien ne doivent pas remettre en cause l'efficacité de ces dispositifs de sécurité.

L'utilisateur doit :

- Connecter au réseau uniquement des postes de travail fournis par les services informatiques ou utiliser l'Extranet.
- Afin que les mises à jour des dispositifs de sécurité puissent s'opérer, n'éteindre le poste de travail qu'une fois ces mises à jour effectuées.
- Verrouiller son poste de travail en cas d'absence, même temporaire.
- Stocker les données bureautiques sur les répertoires sécurisés et sauvegardés automatiquement par les services informatiques (« mes documents » ou répertoires partagés).
- Veiller, en toutes circonstances, à mettre en sécurité le matériel, notamment les ordinateurs portables. En cas de nomadisme un effort tout particulier doit être fourni lorsque l'on travaille dans un lieu public (gare, avion, train). Ne pas laisser le matériel apparent (voiture, …). De préférence, ne pas laisser les ordinateurs portables sur les bureaux ou au moins les sécuriser via l'usage d'un cadenas.
- Etre vigilant et signaler tout constat d'anomalie (dysfonctionnement ou comportement anormal, tentative d'accès)
- S'assurer que le matériel mis à sa disposition est traité avec précautions. Les matériels sont, dans la plupart des cas, neufs et il est recommandé d'éviter toute manipulation leur portant atteinte (liquides, rayures, chocs, poussière….).

L'utilisateur ne doit pas :

- Modifier la configuration d'un poste de travail ni le paramétrage des logiciels mis à sa disposition remettant en cause le niveau de sécurité du poste de travail.
- Installer sur un poste de travail, ni connecter au réseau, des composants matériels ou logiciels sans accord préalable des services informatiques.
- Désactiver l'antivirus ou entraver la mise à jour des dispositifs de sécurité.
- Surcharger les serveurs par des données inutiles à l'activité de l'entreprise (photos, musique, films….).
- Permettre à des personnes situées en dehors du réseau de l'entreprise de prendre le contrôle du poste de travail à distance, en dehors des procédures référencées par la DSI.

Concernant les téléphones

L'entreprise met à disposition des utilisateurs, pour l'exercice de leur fonction, des téléphones fixes et/ou des téléphones sans fils et mobiles.

L'utilisation des téléphones à titre privé est admise à condition qu'elle demeure ponctuelle durant le temps de travail et ne nuise pas au bon exercice des fonctions tenues.

Des restrictions d'utilisation des téléphones sont mises en place en tenant compte de la mission des utilisateurs. A titre d'exemple certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

L'entreprise met en oeuvre un suivi des consommations et du bon respect des consignes pour chaque forfait.

8. Conditions d'usage de la messagerie électronique

Le courrier électronique est aujourd'hui un mode de communication privilégié en raison de sa flexibilité et de sa rapidité. Cependant, le mode de fonctionnement de la messagerie électronique et sa facilité d'utilisation induisent de nombreux risques dont les plus préjudiciables concernent la divulgation d'informations confidentielles, la diffusion d'informations à caractère illégal, la propagation de virus et autres codes malveillants ou l'abus d'usage entrainant une dégradation du service.

La réduction de ces risques repose essentiellement sur le comportement des usagers de la messagerie électronique au sein de l'entreprise. Ceux-ci doivent par conséquent respecter un **code de bonne conduite et de sécurité rigoureux** en la matière.

L'utilisateur doit :

- Utiliser exclusivement le serveur de messagerie de l'entreprise.
- Vérifier l'adresse du destinataire avant l'envoi d'un mail afin d'éviter tout adressage erroné et la communication d'informations à des destinataires non habilités à en prendre connaissance.
- Utiliser avec discernement les listes de diffusion pour maîtriser l'envoi de copies à un nombre injustifié de destinataires.
- S'efforcer de limiter le volume des messages (notamment la taille des pièces jointes) afin d'éviter de surcharger les réseaux de l'entreprise (utiliser si besoin les outils de compression mis à disposition par les services informatiques ou mettre les pièces jointes sur des répertoires partagés ou utiliser des outils externes (par exemple WeTransfer).
- Limiter l'usage des copies cachées de message.

L'utilisateur ne doit pas :

- Utiliser de procédure de renvoi automatique des messages professionnels vers une messagerie externe à celle de l'entreprise, la sécurité de ces flux ne pouvant être maîtrisée.
- Ouvrir un message, ou une pièce jointe associée, qui présentent un doute quant à leur provenance ou leur contenu.
- Donner suite ou rediffuser les messages en chaîne ou alarmistes (hoax) qui utilisent inutilement les ressources du système d'information.
- Répondre aux messages électroniques commerciaux non sollicités (spam)
- Utiliser les listes de diffusion pour un usage externe (ex : dans un site web)
- Cliquer, en aucun cas, sur les liens hypertextes contenus dans un message non sollicité et demandant de fournir des données confidentielles (phishing).

9. Conditions de navigation sur Internet

L'Internet étant un média public de portée mondiale constitue à la fois un vecteur de développement fort pour les activités de l'entreprise mais aussi une zone à risques multiformes (détournement d'informations, fraude, sabotage ou intrusions logiques, comportement illégaux…) dont les impacts à la fois juridiques et techniques peuvent atteindre à l'image de marque de l'entreprise ou remettre en cause la continuité de certaines de ses activités (vente en ligne, services au client …).

L'entreprise met en œuvre des dispositifs de sécurité permettant de **protéger le système d'information des actions malveillantes susceptibles d'être conduites depuis l'Internet** tout en fournissant l'accès aux services Internet devenus indispensables à ses activités.

L'utilisateur doit :

- Utiliser exclusivement la connexion fournie et sécurisée.
- Observer un devoir de réserve et se garder d'émettre toute opinion ou d'exercer toute activité susceptible de porter atteinte à l'image de l'entreprise, notamment lors de la participation à des forums.
- Eviter de laisser son adresse de messagerie professionnelle sur les sites non professionnels afin de prémunir l'entreprise contre la réception de mails indésirables (spam).
- Vérifier que toute publication personnelle sur les réseaux sociaux (Twitter, Facebook, Linkedin, …) est en phase avec les valeurs de l'entreprise (Bienveillance, Responsabilité, Pragmatisme) et ne porte pas atteinte aux intérêts de l'entreprise.

L'utilisateur ne doit pas :

- Transmettre ou publier sur Internet des informations non publiques ou confidentielles à propos de l'entreprise, de ses clients, partenaires ou fournisseurs, ou de son personnel (sauf autorisation spécifique validée par la hiérarchie).
- Créer ou administrer des services Internet ou de communication électronique étrangers aux besoins de l'activité professionnelle ou n'ayant pas fait l'objet d'une autorisation des services informatiques.
- Utiliser les réseaux sociaux en ouvrant des comptes sous le nom de Mayoly Spindler ou Topicrem qui sont des marques déposées ou tout autre nom de marques de l'entreprise. Ne pas utiliser de profil ou de logo ayant un rapport avec les activités de l'entreprise ou ses entités.

Faire référence à des données de l'entreprise (intitulés de postes, produits, …) dans des conversations personnelles sur les réseaux sociaux.

- Utiliser des messageries Internet grand public (ex : Yahoo, Hotmail, Gmail, …) ou des messageries instantanées (ex : MSN Messenger, ICQ, …) dont la sécurité ne peut pas être assurée.
- Utiliser des sites de streaming (radios, vidéo, …) afin d'éviter toute surcharge de la bande passante.
- Consulter des sites, télécharger ou échanger des informations dont le contenu est contraire à la loi (cf. § 5 : Respect de la legislation).

10. Contrôle de l'utilisation des ressources du Système d'Information

L'enregistrement des accès ou tentatives d'accès aux ressources du système d'information constitue une mesure de sécurité dont la finalité première est d'en garantir l'utilisation normale. L'employeur doit pouvoir, le cas échéant, identifier et sanctionner les usages contraires à la loi et à ses règles internes, répondre aux requêtes émanant des tribunaux ou des organismes de police relatives au comportement de ses collaborateurs, y compris lors de l'usage de son système d'information.

L'entreprise met donc en œuvre des **moyens d'enregistrement et d'analyse** dans le respect de l'information des personnels concernés et de la législation applicable à l'information, aux fichiers et aux libertés.

Un contrôle du matériel informatique (composants et logiciels) peut être effectué à tout moment dans le cadre d'une investigation. En cas de risque grave imputable à l'utilisateur, de nature à caractériser une faute civile, contractuelle ou pénale, l'accès aux ressources du système d'informations **pourra être restreint, voire fermé, sans préavis.**

Les moyens et techniques de contrôle qui sont mis en œuvre au niveau du système d'information évolueront à mesure que la technologie se perfectionnera.

10.1 Messagerie

10.1.1 Contrôle global

Dans le cadre des services de messagerie électronique, les éléments collectés visent à contrôler globalement :

- Le nombre de messages reçus de l'Internet ;
- Le volume occupé par l'ensemble des boîtes aux lettres sur tout le système et par serveur de messagerie ;

Ces informations pouvant être comptabilisées à des fins statistiques.

10.1.2 Contrôle individuel

La taille des boîtes aux lettres est limitée ; des dépassements de seuil sont autorisés de manière dérogatoire et sont suivis de manière statistique.

Chaque message fait l'objet d'un traitement automatique visant à détecter la présence de virus et à l'éradiquer chaque fois que c'est possible. En cas de présence de virus, les adresses de l'émetteur et du destinataire, l'objet du message et le type de virus détecté sont enregistrées à des fins d'analyse et de statistiques. message infecté ne sera pas délivré.

10.1.3 Conservation

Des sauvegardes sont effectuées de façon à pouvoir restaurer la base de messagerie en cas d'incident. Les messages sont gardés sur le serveur 1 an, sous réserve de la nécessité associée aux obligations légales en matière de lutte anti-terroriste.

La restauration des informations est conditionnée à la règle des bonnes pratiques en termes de suivi et traitement de l'information. A ce titre la procédure de rappel des données se veut encadrée afin de déterminer de façon précise la justification de la restauration.

10.1.4 Non utilisation ou cessation d'activité

En cas de suspension momentanée ou définitive de l'activité professionnelle, la boîte aux lettres n'est plus accessible sauf si l'employé a rédigé une autorisation écrite donnant accès à son employeur ou en cas de force majeure.

10.2 Usage de l'Internet

10.2.1 Contrôle global

La liste des sites visités est collectée, à des fins statistiques et pour adapter les caractéristiques techniques de l'accès Internet.

10.2.2 Contrôle individuel

- La liste des sites visités et le volume des consommations sont collectés. Ces informations sont utilisées:
- A des fins statistiques ;
- Pour vérifier que le trafic reste dans des limites raisonnables ;

La durée de conservation de ces informations individuelles est de 12 mois.

10.3 Utilisation de l'espace bureautique : accès aux espaces communs et individuels

10.3.1 Contrôle global

Des contrôles peuvent être effectués sur la taille des espaces bureautiques.

10.3.2 Contrôle individuel

Peuvent être l'objet de contrôles périodiques : la taille globale de l'espace bureautique, le nombre de fichiers, leurs tailles et leurs types. Ces informations sont utilisées pour veiller au respect des règles d'utilisation des espaces bureautiques.

10.3.3 Non utilisation ou cessation d'activité

En cas de suspension momentanée ou définitive de l'activité professionnelle, les espaces individuels (répertoires bureautiques sauvegardés) sont archivés pour 12 mois puis détruits si le propriétaire n'a pas demandé leur réactivation.