# Sanofi Digital Usage Principles FRENCH VERSION: Charte d’utilisation des Technologies Digitales de Sanofi

# Contents

# *1. Propos*

La Charte d'Utilisation des Technologies Digitales de Sanofi repose sur les principes énoncés par la Politique de Sécurité des Systèmes Digitaux de Sanofi et de toutes ses filiales.

Ce document décrit les principaux risques auxquels les systèmes digitaux de Sanofi et des filiales peuvent être exposés. Pour éviter ces risques, ce document édicte **les règles que chaque utilisateur doit respecter.** Le respect de ces règles permettra à Sanofi de maintenir et préserver la sécurité de ses systèmes digitaux en assurant la confidentialité, l'intégrité et la disponibilité des données, créant ainsi un espace d'usage doté d'un haut niveau de confiance.

Ces règles reposent sur les principes essentiels suivants :

- L'utilisation des systèmes digitaux est **réservée par principe à un usage professionnel**.
    - Seuls les systèmes et équipements fournis et administrés par la Fonction Digitale sont autorisés à se connecter aux réseaux internes de Sanofi.
    - Les systèmes et équipements non fournis et administrés par la Fonction Digitale doivent se connecter seulement au réseau Guest.
- Les employés de Sanofi et les prestataires ne doivent pas se connecter au réseau Sanofi Guest avec des systèmes et équipements fournis et administrés par la Fonction Digitale.
- Sanofi ne procède, en aucun cas, à la récupération de données personnelles hébergées sur un poste de travail professionnel. Il appartient au salarié de conserver une copie de ses données personnelles sur un équipement lui appartenant en propre.
- L'accès aux systèmes digitaux doit être réalisé avec les identifiants de connexion fournis par les administrateurs de Sanofi.
    - Un identifiant de connexion unique est assigné à chaque utilisateur.
    - Les identifiants de connexion ne doivent pas être partagés et doivent être protégés pour éviter leur divulgation. Chaque utilisateur est responsable de protéger ses identifiants de connexion et est individuellement responsable de toutes les actions réalisées avec ses identifiants.
    - Le Service Desk local doit être contacté sans délais si une délégation d'accès a besoin d'être mise en place.
- La connexion à Internet nécessite une authentification de l'utilisateur par des services fournis par la Fonction Digitale.
- L'installation de logiciels est réalisée exclusivement par la Fonction Digitale.

- L’échange d’informations par Internet doit faire l’objet d’une grande vigilance pour éviter la divulgation d’information sensibles appartenant à Sanofi.
- Les lois nationales, le Code de Conduite et Intégrité de Sanofi, les législations générales protégeant les brevets, les droits d'auteurs, la dignité humaine, le secret professionnel, etc., doivent être strictement respectés.
- Les employés Sanofi et les prestataires doivent traiter et manipuler les données personnelles dans le respect des politiques de protection des données personnelles publiquement accessible sur Internet et sur le site Intranet de Sanofi.
- Afin de garantir la sécurité des systèmes digitaux de Sanofi, toutes les données échangées par les utilisateurs peuvent être auditées à tout moment.

Sous réserve des législations locales, le principe du secret des correspondances privées ne pourra pas trouver d’application dans le cadre de recherches liées à la survenance d’un incident de sécurité.

Chaque utilisateur des systèmes digitaux de Sanofi et de toutes ses filiales doit prendre connaissance du texte complet de ce document.

## *2. Domaine d’application*

Ce document s’applique à tous les utilisateurs des systèmes digitaux de Sanofi et à toutes ses filiales.

# *3. Exigences*

Ces exigences s'appliquent à tous les utilisateurs des systèmes digitaux.

## 3.1 Introduction

Les données suivantes constituent des informations critiques dans l'environnement de Sanofi : les informations à caractère industriel, financier, commercial ou contractuel, les données issues de la recherche ou du développement ainsi que celles concernant les salariés, les clients et les patients.

Ces types de données sont indispensables à l'ensemble des activités quotidiennes et certaines d'entre elles revêtent une importance capitale dans un contexte international de plus en plus concurrentiel.

La Cyber Sécurité étant de la responsabilité de chacun des collaborateurs et des partenaires du Groupe Sanofi, il est nécessaire que chaque utilisateur des systèmes digitaux, des données et réseaux de Sanofi (et de ses filiales) prenne pleinement conscience des nombreux risques qui pèsent sur les systèmes digitaux, sur ceux de Sanofi en particulier. Certains risques peuvent être dus à des défaillances techniques, d'autres à des erreurs humaines, des actions non intentionnelles des utilisateurs, d'autres enfin constituent de véritables actes de malveillance.

### 3.1.1 Principaux Risques Liés Aux Systèmes Digitaux

Enumérer l'ensemble des risques liés aux systèmes digitaux serait une gageure en raison de l'évolution constante des technologies de l'information.

L'ouverture des réseaux de Sanofi à Internet, permettant la consultation de sites d'information et l'échange de courriers électroniques avec des correspondants externes à l'entreprise, ouvre le champ à de nombreux risques contre lesquels Sanofi doit se protéger.

A titre d'exemple, les principaux risques suivants constituent une liste non exhaustive mais représente quelques-unes des menaces potentielles :

- Vol (piratage) d'informations, de logiciels
- Divulgation d'informations issues du patrimoine de Sanofi
- Usurpation d'identité en vue de récupérer ou d'émettre des messages, ou d'utiliser les systèmes digitaux de Sanofi sans en avoir été habilité
- Blocage des systèmes digitaux de Sanofi par une infection virale des serveurs et postes de travail, ou par une attaque délibérée visant à saturer nos réseaux internes pour rendre indisponibles nos serveurs
- Divulgation d'informations protégées par le droit d'auteur
- Divulgation de données personnelles ou sensibles pouvant affecter les employés, patients ou de la vie privée

- Fraudes et détournements divers
- Utilisation non professionnelle des moyens électroniques de communication au détriment des activités de Sanofi, entraînant une image négative de l'entreprise vis-à-vis de l'extérieur

### 3.1.2 Stratégie de Protection de l'Entreprise

Face à l'accroissement des risques qui pèsent sur nos systèmes digitaux, Sanofi se devait de mettre en place une organisation de sécurité adaptée.

- L'objectif de cette organisation de sécurité est de créer un « **espace de confiance** », c'est-à-dire d'un ensemble homogène de systèmes digitaux et de télécommunications au sein desquels la protection des données est effective

- Cette stratégie s'appuie sur des Règles de Sécurité des systèmes digitaux ainsi que sur des Politiques de Sécurité des systèmes digitaux spécifiques (messagerie électronique, Internet, etc.) décrivant des procédures, des moyens et des règles d'utilisation

- Ces documents sont disponibles dans le système standard de gestion de document électronique de la Qualité Globale. La revue de cette information par tous les utilisateurs est obligatoire.

### 3.1.3 Contrôle des Connexions

La protection des intérêts de Sanofi face aux menaces qui peuvent peser sur ses systèmes digitaux rend nécessaire la mise en place d'une architecture de sécurité en profondeur (routeurs sécurisés, pare-feux, outils de détection d'intrusion, détection et réponse sur les endpoints, logiciels de chiffrement, etc.).

Cette architecture de sécurité permet en particulier d'identifier et d'authentifier chaque utilisateur lors de ses accès aux systèmes digitaux de l'entreprise.

En outre, pour des raisons d'obligations légales et de sécurité, il est possible d'auditer à tout moment les transactions réalisées par n'importe lequel des utilisateurs des système digitaux de l'entreprise.

Ces échanges, qui sont tracés et archivés par les équipements de sécurité, peuvent comporter les informations suivantes (liste non limitative) :

- L'identité des utilisateurs
- Les dates et heures des communications
- Les sites consultés et les applications utilisées
- Le détail des actions effectuées
- Le sujet et les métadata des emails, la taille des messages ou le volume transféré
- Les flux de données vers l'externe

- La source, la nature et la durée des connexions

La durée de conservation des différents éléments retraçant l'activité d'un poste de travail peut, selon la nature des échanges, aller jusqu'à une année.

Les informations concernant chaque collaborateur sont conservées dans les journaux d'activité des systèmes. Celles-ci ont fait l'objet par Sanofi d'une déclaration auprès des autorités compétentes, en conformité avec les différentes lois relatives à la protection des données à caractère personnel.

En outre, en respectant la législation locale et en fonction des impératifs de sécurité, en cas de recherche liée à la survenance d'un incident de sécurité, le principe du secret des correspondances privées ne pourra pas trouver d'application et le corps même des messages ainsi que les pièces jointes pourront également faire l'objet d'un contrôle.

## 3.2 Règles de Comportement des Utilisateurs

### 3.2.1 Règles générales

#### 3.2.1.1 Respect de la Politique de Sécurité des Systèmes Digitaux de Sanofi

L'utilisation des systèmes digitaux de la société implique la prise de connaissance des différents documents constituant l'ensemble des Politiques de Sécurité des systèmes digitaux et le respect des règles énoncées.

Ces documents sont disponibles dans le système standard de gestion de document électronique de la Qualité Globale.

- Tout utilisateur doit consulter les documents de l'ensemble de la Politique de Sécurité des systèmes digitaux et respecter les règles énoncées

#### 3.2.1.2 Usage des moyens informatiques

Afin de permettre à chacun de remplir ses missions dans de bonnes conditions, Sanofi met à la disposition des utilisateurs dont la nature des fonctions le justifie, les moyens matériels, logiciels et outils leur permettant l'accès aux systèmes digitaux de la société. Toute utilisation à des fins illicites de ces moyens informatiques engagera la responsabilité personnelle de l'utilisateur.

- Les moyens digitaux mis à la disposition des utilisateurs sont, par principe, réservés à un usage professionnel.
- Une utilisation personnelle occasionnelle des systèmes digitaux et de Communication de l'entreprise peut être tolérée, à condition qu'une telle utilisation :
    - Soit conforme avec le code de Conduite et Intégrité de Sanofi, les Politiques de Sanofi et les lois/règlements applicables

- Ne nuit en aucun cas avec les intérêts ou la réputation de l'entreprise
- N'impacte pas les activités professionnelles principales de l'utilisateur et est limité à une durée et fréquence en phase avec les attentes du responsable de l'utilisateur
- Respecte les règles de sécurité et de sureté mentionnées ci-dessus
- N'impacte pas l'usage normal ou les performances des systèmes digitaux ou du réseau d'entreprise

RAPPEL IMPORTANT : Sanofi ne procède, en aucun cas, à la récupération de données personnelles hébergées sur un poste de travail professionnel. Il appartient au salarié de conserver, en permanence, une copie de ses données personnelles sur un équipement lui appartenant en propre.

#### 3.2.1.3 Signalement d'un événement de sécurité

Tout événement de sécurité concernant les systèmes digitaux doit impérativement être signalé sans délai par l'utilisateur au Service Desk. Le Service Desk avertira de l'incident le contact local ou central de la Cyber Sécurité (cf paragraphe 3.1.1 pour les exemples des types de menaces potentielles pouvant constituer un incident de sécurité).

Le contact local ou central de la Cyber Sécurité Digitale pourra être contacté directement pour des cas nécessitant de la confidentialité.

#### 3.2.1.4 Protection de l'image de Sanofi

Il est fondamental que chaque utilisateur soit conscient du fait que tous les serveurs Internet et les services numériques publiques conservent les traces détaillées de toutes les visites. Ainsi, les serveurs Internet par exemple, enregistrent systématiquement des informations relatives à votre poste de travail, vos préférences ainsi que votre adresse IP et votre nom de domaine, c'est-à-dire le nom de l'entreprise.

- Les accès aux sites Internet à partir du réseau interne laissent apparaitre le nom de Sanofi. Dès lors, tous les utilisateurs devront attentivement veiller à ne pas se connecter sur des sites dont le contenu pourrait nuire à l'image de l'entreprise.
- Ce principe s'applique également aux échanges par messagerie, forum, blogs, médias sociaux et toute autre application d'échange et de stockage d'information sur Internet.
- A moins d'être explicitement autorisés à le faire, les utilisateurs ne doivent pas communiquer des informations au nom de Sanofi

#### 3.2.1.5 Respect des législations nationales

Au-delà des règles spécifiques énumérées ci-dessus, tout utilisateur se doit de respecter scrupuleusement les règles générales réprimant notamment les atteintes :

- Aux droits de la personne du fait de fichiers ou traitements informatiques
- Au secret des correspondances ou des communications téléphoniques
- A l'intimité de la vie privée ou à la représentation de la personne
- A la dignité humaine, notamment au regard des informations ou messages qui :
    - Mettent en cause l'honorabilité ou la réputation d'une personne
    - Revêtent un caractère discriminatoire ou incitent à la haine raciale

De même, doivent être rigoureusement respectées les législations protégeant notamment :


    - Mettent en cause l'honorabilité ou la réputation d'une personne
    - Revêtent un caractère discriminatoire ou incitent à la haine raciale

De même, doivent être rigoureusement respectées les législations protégeant notamment :


- Les systèmes de traitements automatisés de données eux-mêmes
- La propriété intellectuelle et notamment le droit d'auteur, les droits voisins
- Les brevets
- Les marques et autres signes distinctifs
- Plus généralement, les secrets de fabrication, le secret professionnel, voire le secret de la Défense Nationale

### **3.2.2** Règles relatives à la protection du poste de travail

#### 3.2.2.1 Extinction journalière du poste de travail

Les postes de travail inactifs en dehors des heures ouvrées doivent être éteints. Cette mesure contribue à prévenir principalement les incidents électriques, la propagation de virus informatique et contribue aux économies électriques. En outre, le redémarrage des postes de travail en début de journée facilite la prise en compte des mises à jour techniques, généralement préparées pendant la nuit.

- Chaque utilisateur doit éteindre son poste de travail en fin de journée si celui-ci n'est pas destiné à fonctionner en dehors des heures ouvrées

#### 3.2.2.2 Activation manuelle de l'écran de veille

Afin de prévenir toute utilisation frauduleuse d'un poste de travail ou l'accès indu à des données qu'il contient, il est nécessaire de protéger l'accès au poste de travail en l'absence de l'utilisateur. L'activation volontaire de l'écran de veille permet de verrouiller l'accès au poste de travail.

- Il n’est pas suffisant de se fier à la mise en veille automatique. Chaque utilisateur doit verrouiller l’accès à son poste de travail dès qu’il prévoit de s’en éloigner.

#### 3.2.2.3 Sauvegarde des données utilisateurs

La perte de données peut survenir à la suite d’une panne électrique ou d’un accident, à la suite d’une erreur de manipulation ou encore d’une malveillance. La Direction Digitale met à la disposition des utilisateurs des espaces de stockage leur permettant d’héberger leurs données de façon sécurisée.

- Les données critiques ne doivent pas être stockées sur le disque local de l’ordinateur fixe ou portable. Chaque utilisateur doit veiller à stocker ses données sur les serveurs référencés par la Direction Digitale.

#### 3.2.2.4 Prévention des vols/pertes de postes de travail portables

Compte tenu des préjudices importants et de la perturbation possible de l’activité pouvant résulter de la perte ou du vol d’ordinateurs portables, il est impératif que les utilisateurs de tels matériels observent rigoureusement les mesures de protection et de prévention élémentaires contre le vol.

Lors des déplacements, l’utilisateur doit impérativement :

- Conserver son ordinateur portable avec lui ou le déposer dans un lieu sécurisé quand il n’est pas sous sa garde
- Ne doit pas travailler à des activités confidentielles sur son ordinateur portable dans les espaces publics.
- Alerter sans délais le Service Desk et/ou sa hiérarchie si une personne externe à l’entreprise manipule, même temporairement, un équipement digital appartenant à Sanofi.

#### 3.2.2.5 Utilisation des supports magnétiques et électroniques externes

Les solutions standards de stockage ou de partage de données fournies par Sanofi doivent être utilisées. En cas d’impossibilité, les recommandations de sécurité suivantes doivent impérativement être appliquées.

Les supports magnétiques ou électroniques externes permettant le stockage de données, nécessitent une vigilance particulière. Ces supports étant faciles à compromettre, égarer ou à voler, il est impératif de toujours protéger les données qu’ils contiennent.

Les solutions standard proposées par Sanofi doivent être utilisées pour le stockage et le transfert de données.

Dans le cas où ces solutions ne pourraient pas être utilisées, les consignes suivantes sont à mettre en œuvre :

- Toute donnée sensible à transférer sur un support externe doit obligatoirement être protégée (par chiffrement) avec les outils fournis par la Fonction Digitale
- Les utilisateurs ne doivent pas utiliser des supports électroniques inconnus sur les systèmes de Sanofi (tels que des médias trouvés ou fournis par un partenaire externe ou un collègue). En cas de doute, contacter un contact de la Sureté ou de la Cyber Sécurité ou le Service Desk pour analyse/assistance.

#### 3.2.2.6 Chiffrement des données

Pour l'entreprise, les informations à caractère industriel, financier, commercial ou contractuel, les données issues de la recherche ou du développement ainsi que celles concernant les salariés constituent un patrimoine qu'il est impératif de protéger. Une attention particulière doit être portée aux données personnelles et aux données sensibles.

- Les outils de chiffrement, mis à disposition par la Fonction Digitale, doivent être utilisés chaque fois qu'il est nécessaire de protéger la confidentialité des informations

#### 3.2.2.7 Installation de logiciels

La protection du poste de travail de l'utilisateur vis à vis des infections informatiques et du respect du droit d'auteur passe notamment par la conformité de ce poste aux applications et logiciels référencés par la Fonction Digitale.

- Seules les personnes habilitées au sein de la Fonction Digitale peuvent réaliser les installations de logiciels sur un poste de travail

#### 3.2.2.8 Utilisation d'équipements mobiles

Avec la popularité croissante des équipements mobiles (ordinateurs portables, smartphones, tablettes), il est essentiel de considérer les risques de sécurité lors de l'accès aux services digitaux de Sanofi à partir des équipements mobiles ainsi que les risques liés au stockage de données de Sanofi sur ces équipements mobiles.

Un accord écrit du responsable de l'utilisateur est nécessaire afin que des équipements mobiles personnels accèdent au système de messagerie de l'entreprise. Si approuvé, l'accès doit se faire via les logiciels approuvés par Sanofi. L'équipement mobile est configuré et supporté par les personnes autorisées au sein de la Fonction Digitale.

- L'authentification Sanofi de l'utilisateur et/ou de l'équipement doit être utilisée pour accéder aux services de Sanofi via le réseau d'entreprise

- Toutes les données de Sanofi stockées sur un équipement mobile doivent être chiffrées
- En cas de perte ou de vol d'un équipement mobile (à l'exception des ordinateurs portables), toutes les données de l'entreprise stockées sur l'équipement seront effacées. Ceci s'applique également aux équipements mobiles personnels et aux données personnelles associées (i.e. équipements non fournis et non gérés par la Fonction Digitale).
- Les utilisateurs doivent contacter sans délai le Service Desk pour signaler toutes pertes/vols d'équipements mobiles
- Aucun support ne sera fourni par le Service Desk pour les applications non professionnelles installées sur des équipements mobiles attachés à des services Sanofi
- L'installation d'applications pouvant compromettre des services Sanofi de quelque manière que ce soit est strictement interdite et sujette à désinstallation ou déconnexion de l'équipement mobile aux ressources informatiques de Sanofi
- Dans le cas d'un incident, tous les équipements mobiles connectés à un service Sanofi et/ou stockant des données de Sanofi seront sujets à des enquêtes par la Cyber Sécurité si cela est estimé nécessaire et en accord avec les lois et règlements locaux

#### 3.2.2.9 Maintien d'un environnement de travail sécurisé

Les utilisateurs sont responsables de sécuriser les informations imprimées ou écrites, en en limitant l'exposition, afin de protéger les actifs sensibles des clients et de l'entreprise. La mise à disposition de documents sensibles doit être faite de manière sécurisée. Les documents sensibles ne doivent pas être laissés dans les salles de réunion ou dans les espaces de fax/impression/copie.

#### 3.2.2.10 Télétravail

Si l'utilisateur participe à un accord de télétravail (pour travailler à distance), l'utilisateur doit assurer une protection adéquate des données de Sanofi et des équipements dans le lieu distant en accord avec les règles exposées au paragraphe 3.2.2.

L'utilisateur devra prendre les précautions additionnelles suivantes :

- S'assurer de la confidentialité des accès aux applications et données
- Stocker les données de Sanofi uniquement sur des équipements fournis et gérés par Sanofi
- Sécuriser de manière appropriée l'utilisation à distance des équipements de Sanofi
- S'assurer qu'aucun document de Sanofi ne soit jeté dans une poubelle mais plutôt détruit sur place ou ramené dans les locaux de Sanofi pour destruction

- Ne pas utiliser de manière frauduleuse ou inappropriée les ressources de Sanofi

#### 3.2.2.11 Equipements de l'entreprise

Suite à la cessation d'un contrat de travail de Sanofi (ou d'une filiale), il est impératif que l'utilisateur :

- Rende tous les équipements fournis par l'entreprise à son responsable direct ou à tout service identifié comme responsable en accord avec les procédures de départ régionales de Sanofi, le dernier jour de son contrat de travail et avant de quitter les locaux de l'entreprise

Inversement, il est obligatoire que le responsable de l'utilisateur ou tout service identifié comme responsable en accord avec les procédures de départ régionales de Sanofi :

- S'assure que tous les équipements sont récupérés et rendus à la Fonction Digitale (si la Fonction Digitale n'a pas de manière pro active récupéré les équipements), dans les deux semaines suivant le départ de l'utilisateur

- S'assure que toutes les données professionnelles nécessaires restent accessibles après le départ de l'utilisateur

- Aucun équipement Digital de Sanofi ne peut et ne doit être cédé à un employé, gracieusement ou contre paiement.

### **3.2.3** Règles relatives à l'accès aux réseaux

#### 3.2.3.1 Authentification d'accès aux Systèmes Digitaux

L'accès aux systèmes digitaux de la société nécessite l'utilisation d'identifiants uniques et de mots de passe personnels. Toutes les connexions réalisées avec ces éléments seront donc, sauf preuve contraire, présumées être le fait de leur détenteur.

- Pour accéder aux systèmes digitaux, chaque utilisateur doit exclusivement utiliser les identifiants d'accès qui lui ont été remis par les administrateurs, et conserver ses mots de passe secrets. Les mots de passe ne doivent pas être partagés avec qui que ce soit pour aucune raison.

#### 3.2.3.2 Accès aux réseaux internes de Sanofi

Des points d'accès aux réseaux internes de la société, référencés et sécurisés par la Fonction Digitale, garantissent la sécurité des communications et la sécurité et la protection des données.

- Toute communication vers les réseaux internes de la société ne doit se faire qu'à travers les points d'accès référencés et sécurisés par la Fonction Digitale

- La connexion d'un équipement non autorisé au réseau interne de l'entreprise est interdite

#### 3.2.3.3 Accès aux réseaux externes de Sanofi

Des points d'accès aux réseaux externes à la société, référencés et sécurisés par la Fonction Digitale, garantissent la sécurité des communications et la protection des données.

- Toute communication vers des réseaux externes à la société ne peut être réalisée dans les locaux de Sanofi qu'à travers les points d'accès référencés et sécurisés par la Fonction Digitale à l'exception du service de Webmail Sanofi, qui peut être atteint depuis n'importe quelle connexion réseau
- L'accès au réseau personnel ou au réseau distant pour des travaux non en lien avec l'activité de Sanofi est interdit

### **3.2.4** Règles relatives à l'usage des Systèmes de Communication

#### 3.2.4.1 Transferts de fichiers volumineux avec l'Internet

L'utilisation des services Internet, tels que la consultation de sites, la messagerie ou les transferts de fichiers, ne doit pas avoir d'effet notable sur la disponibilité du réseau informatique pour les autres utilisateurs. Si les conditions de performance ou de sécurité l'exigent, la connexion avec le réseau Internet peut être suspendue sans préavis, jusqu'au rétablissement d'une situation normale.

- Les outils mis à disposition par la Fonction Digitale doivent être utilisés pour partager et transférer les fichiers de manière sécurisée

#### 3.2.4.2 Contrôle de la réception des messages Internet

Les messages électroniques provenant d'Internet étant dépourvus de tout contrôle d'authenticité, l'identité de l'émetteur comme le contenu du message peut avoir été modifié ou comporter des virus informatiques. Il convient donc d'être particulièrement attentif à l'authenticité des messages reçus.

- Ne pas ouvrir les messages et les fichiers attachés en provenance d'Internet lorsque ces messages ne sont pas sollicités ou sans objet professionnel
- Prendre soin en cliquant sur des liens inclus dans les messages, ils peuvent être nuisibles par essence et introduire des virus ou malware sur le réseau de Sanofi

#### 3.2.4.3 Contrôle de l'envoi des messages

L'utilisation de la messagerie requiert une vigilance particulière lorsqu'il s'agit de sélectionner les destinataires d'un courrier électronique. Une erreur dans la sélection d'un destinataire externe à la société peut dans certains cas s'avérer préjudiciable pour l'entreprise.

- Chaque utilisateur étant responsable des courriers électroniques qu'il émet, il doit impérativement s'assurer de la pertinence des destinataires avant chaque envoi

- L'utilisation de services de webmail personnel est autorisé à condition qu'en tel usage soit consistant avec les lignes directrices sur l'usage personnel décrites dans ce document.

- Les webmails personnels ne doivent jamais être utilisés pour créer, envoyer, recevoir, lire ou stocker des emails contenant des informations professionnelles.

#### 3.2.4.4 Envoi d'information sensible sur internet

La position de Sanofi dans un contexte international de plus en plus concurrentiel impose à chacun une vigilance stricte vis-à-vis des informations qui sont communiquées sur le réseau Internet.

- Tout échange et publication d'informations appartenant à Sanofi, à travers le réseau Internet, doit être soumis à l'autorisation préalable de la hiérarchie
- Les utilisateurs sont responsables de leur comportement lors de l'utilisation des réseaux sociaux et doivent adhérer aux lignes directrices définies par Sanofi pour l'usage des media sociaux
- Ne jamais répondre aux questionnaires provenant d'Internet qui peuvent, en réalité, être le support d'une action de veille concurrentielle dont la société serait la cible ou être utilisés pour lancer une attaque de social engineering
- Les utilisateurs ne doivent pas transmettre ou stocker des données de l'entreprise dans des environnements externes à Sanofi ou des services ou applications qui n'ont pas été expressément approuvés par la fonction Cyber Sécurité

#### 3.2.4.5 Sécurité des conférences

Les utilisateurs doivent prendre en compte les bonnes pratiques de sécurité lors de l'animation de réunions Sanofi pour empêcher les accès non autorisés. Ceci inclut les conférences vidéo/VTC, les sessions web, les appels en téléconférence, etc.

- Les appels confidentiels ne doivent jamais être enregistrés
- Les participants à une réunion doivent être informés de l'enregistrement en amont de celle-ci
- La légitimité des participants doit être vérifiée par le responsable de la réunion avant le début d'une discussion interne ou confidentielle

# 4. Responsabilités

La Direction de la Fonction Cyber Sécurité est en charge de mettre en œuvre l'utilisation de cette politique. Les utilisateurs des systèmes digitaux de Sanofi doivent se conformer à cette politique.

# 5. Annexes

## CONTRAT CLIC

### 5.1 OBJET

Le standard d'Usage des systèmes digitaux de Sanofi s'appuie sur les principes définis par la Politique de Sécurité Digitale de l'entreprise.

Ce document décrit les risques principaux auxquels les systèmes digitaux de l'entreprise pourraient être exposés et par conséquence indique **les règles que chaque utilisateur doit respecter** pour préserver les systèmes digitaux dans leur ensemble.

L'objectif du contrat « Clic » de Sanofi est d'informer tous les utilisateurs des systèmes digitaux qu'ils doivent connaitre le standard d'Usage des systèmes digitaux disponible sur l'intranet.

### 5.2 CONDITIONS DE MISE EN OEUVRE

Tous les ordinateurs appartenant à Sanofi et à toutes ses filiales doivent être configurés afin de permettre la mise en œuvre du contrat « Clic » dans la mesure où la réglementation locale autorise et reconnait ce contrat « Clic ».

La mise en œuvre consiste en l'affichage aux utilisateurs d'un écran avec un texte d'information constituant le contrat « Clic » avant de permettre la connexion au réseau de l'entreprise.

L'utilisateur doit utiliser le bouton « OK pour continuer » afin d'accéder à l'écran de connexion permettant la connectivité aux réseaux Sanofi, reconnaissant par ce clic son acceptation de la Politique d'Usage des Systèmes Digitaux.

### 5.3 TEXTE D'INFORMATION DU CONTRAT « CLIC »

The information text of the "Click" contract is as follows:

Le texte d'information du contrat « Clic » est le suivant :

*« Vous allez vous connecter aux Systèmes Digitaux de Sanofi.*

*Vous vous engagez à lire et respecter les règles exposées dans la Politique d'Usage des Systèmes Digitaux de Sanofi dont le texte est disponible sur l'Intranet et/ou le référentiel standard et global de stockage des documents. » Bouton <OK >*