Signature Page

Name	Meaning	Date & Time of Signature (DD/MM/YYYY hh:mm:ss UTC)
BATLA Sahar	Writing	23/04/2021 17:50:49
GUILLERMIN Frederic	Writing	26/04/2021 04:48:02
POICHOTTE Jean Yves	Approval	26/04/2021 05:51:50

Table of Contents

French Version

1. PURPOSE

The Information Technology and Solutions Usage Standard of Sanofi is based on principles stated in the Information Systems Security Policy of Sanofi and all its subsidiaries.

This Standard describes the main risks to information systems of Sanofi and its subsidiaries. To avoid these risks, the Standard states **the rules that each user must adhere to** when using these systems. Following these rules will allow Sanofi to maintain and preserve information systems, ensuring confidentiality, integrity and availability of data, therefore creating a secure space with a high level of trust.

These rules rely on the following essential principles:

- Usage of information systems is, by principle, reserved for professional use
    - Only systems and devices provisioned and managed by the Digital function are allowed to connect to Sanofi internal networks
    - Systems and devices not provisioned and not managed by the Digital function must connect to the Guest network only
    - Sanofi employees and contractors must not connect to the Sanofi Guest network with systems and devices provisioned and managed by the Digital function
- Access to information systems must be conducted with the access credentials provided by Sanofi administrators
    - Unique access credentials are assigned to each individual
    - Credentials must never be shared and must be protected to avoid disclosure. Each individual is responsible for protecting these credentials and for every action performed with them
        - The local Service Desk must be contacted if delegation needs to be granted
- Internet connection requires user authentication via services provided by the Digital function
- Software installation must be done exclusively by the Digital function
- Due care must be taken when transmitting information over the Internet to prevent information disclosure
- National laws, Sanofi ethical code, general legislation protecting patents, author rights, human dignity, professional secrecy, etc. must be strictly respected
- Sanofi employees and contractors must be vigilant when processing and handling personal data
- In order to guarantee information systems security of Sanofi, all data exchanged by users may be audited at any time

In the event of a security incident, the confidentiality of private correspondences cannot be maintained or guaranteed due to investigative research that may be required for local legislations.

Each user of information systems of Sanofi and all its subsidiaries must become familiar with the complete text of this document.

2. SCOPE AND APPLICABILITY

This document applies to all users of information systems of Sanofi and all its subsidiaries worldwide.

3. REQUIREMENTS

1.	These requirements are applicable for all Information Systems users.

3.1 INTRODUCTION

2.	The following data constitutes critical information in the Sanofi environment: information of an industrial, financial, commercial or contractual nature, data stemming from research or development and data about employees, customers and patients. These data types are indispensable to the company's daily activities, and some are of capital importance in an increasingly competitive global market. As security is everyone's responsibility, it is necessary that all users of Sanofi's (and its subsidiaries') information systems, data and networks, take into account the many risks that information systems are subject to, especially the ones that pertain to Sanofi. Some risks may be due to technical malfunctions, human error or unintentional user actions, and others to malevolent acts.

3.1.1 Main Risks of Information Systems

3.	Listing all of the risks for information systems risk is impossible due to the constant evolution of technologies in the information systems area. Opening Sanofi networks to the Internet, allowing consultants at Sanofi sites and email exchanges with external correspondents of the company, open the doors to many risks from which we must protect ourselves. For example, below are the main risks, which do not constitute an exhaustive list, but represent some of the potential threats: • Theft (copyright infringement) of information and software • Data disclosure from Sanofi assets concerning the company • Users spoofing in order to hijack or send messages, or using information systems of Sanofi without prior authorization • Denial of Service of Sanofi's information systems due to computer virus infections of servers and workstations, or a deliberate attack aiming to overload Sanofi's internal network to incapacitate servers • Disclosure of information protected by copyright • Disclosure of personal data or sensitive personal data that might affect employees, patients or any individual's privacy • Fraud or embezzlement

	• Unethical use of electronic means of communications for the detriment of Sanofi activities, resulting in a negative company image to the external world

3.1.2 Company Protection Strategy

4.	To face the increased risks that challenge our information systems, Sanofi has put a suitable security organization in place. • The purpose of this security organization is to create a "**Space of Trust**," which means a standard set of information systems and telecommunications for effective data protection • This strategy relies on information systems security rules and specific information systems security policies (such as for email, Internet, etc.) describing the procedures, means, and usage rules • These documents are available in the standard global quality document management system and it is mandatory that each user review this information

3.1.3 Monitoring Connections

5.	Protecting the company interests against potential threats to its information systems requires the implementation of a layered security architecture (secure routers, firewalls, intrusion detection tools, anti-virus servers, encryption software, etc.). This security architecture makes it possible to identify and authenticate every user accessing the company's information systems. In addition, for legal and security requirements, it must be possible at all times to audit any operation conducted by any user of the company's information systems. These operations, which are tracked and archived by security equipment, may include the following information: • User's identity • Communication dates and times • Sites visited and applications used • Details of requests made • Size of messages or volume transferred • Subject of message • Duration of connections

	The retention period of various elements used to track a workstation's activity, depending on the type of operation, can be up to one year. The information on each user is kept in the system's activity logs. This information is covered in a company statement to the applicable authorities in order to maintain compliance with the various laws regarding the protection of individual information. In the event of a security incident, the confidentiality of private correspondences cannot be maintained or guaranteed due to research that may be required for local legislations. Therefore the principle of secrecy of private mail may not be applicable and the actual body of messages as well as attachments can be subject to inspection.

3.2 USERS' RULES OF BEHAVIOR

3.2.1 General Rules

3.2.1.1 Respect for the Sanofi Information Systems Security Policy

6.	Use of the company information systems implies familiarity with the various documents comprising the set of Sanofi's Information Systems Security Policies and adherence to its rules. These documents are available in the standard global quality document management system. • It is mandatory for all users to consult the documents in the company Information Systems Security Policy set and adhere to its rules

3.2.1.2 Use of Information Systems

7.	The company makes hardware, software and tools available to users whose positions require them to have access to the company information systems in order to fulfill their missions. Any liability or penalty for the unlawful use of these computer facilities will be personally incurred by the user. • In principle, the computer facilities made available to users are primarily reserved for professional use • Occasional personal use of the company's information and communication systems can be tolerated, provided that such use: ○ Is in accordance with Sanofi's code of ethics, Sanofi's policies and law/regulations ○ In no case harms the company's interests or reputation ○ Does not impact primary business activities of the user and is confined to a frequency and duration in line with the expectation of the user's management

	○ Respects the security and safety rules stipulated above ○ Does not impact normal usage or performance of the computer systems on the company network
3.2.1.3 Reporting of a Security Incident	
8.	It is mandatory that any security incident concerning the company's information systems be promptly reported by the user to the Service Desk. The Service Desk will notify the local Digital Cyber Security contact or respective Information Systems Security Officer of the incident. (Refer to section 3.1.1 for examples of the types of potential threats that may constitute a security incident). The local Digital Cyber Security contact or Information Systems Security Officer may be contacted directly for sensitive cases.
3.2.1.4 Protection of Sanofi Image	
9.	Users must understand that all internet sites track details of every visit. Internet servers routinely capture and store information about your workstation, including your preferences, as well as your IP addresses and your domain name, i.e., the company's name. • Visits to Internet sites from the company's internal network show the name of Sanofi, therefore all users must take care not to visit sites whose content could harm the company image • This principle is also applicable to email, forums, blogs, social media or any other forms of data exchange or data storage on the Internet • Unless explicitly authorized to do so, users must not communicate any information on behalf of Sanofi
3.2.1.5 Respect for National Legislations	
10.	In addition to the specific rules listed above, users must also diligently respect all rules regarding the violation of: • Personal rights stemming from the use of computer files and processing • Confidentiality of telephone conversations and mail • Privacy, personal misrepresentation • Human dignity, specifically information or messages which: ○ Question a person's honor or reputation ○ Are discriminatory or incite hate

	Similarly, legislation protecting the following must be closely respected: • Automated data processing systems • Intellectual and artistic property, specifically copyright and neighbors' rights • Patents • Trademarks and other distinctive marks • More generally, production secrets, trade secrets, and even national defense secrets
3.2.2 Rules Relating to the Protection of Workstations	
3.2.2.1 Daily Shutdown of the Workstation	
11.	Workstations that are inactive outside of work hours must be powered off. Primarily, this measure helps prevent electrical incidents, the propagation of computer viruses and conserves electricity. Moreover, powering on workstations at the start of the day facilitates the implementation of technical updates, which are generally prepared at night. • Each user must switch off his/her workstations at the end of the day if there is no requirement to function outside of normal business hours
3.2.2.2 Manual Activation of the Screen Saver	
12.	To prevent any fraudulent use of a workstation or the data it contains, (such as identity theft), access to the workstation must be protected during the user's absence. Intentional activation of the screen saver makes it possible to lock access to the workstation. • It is not enough to rely on the automated screen lock. Each user must lock access to his/her workstation whenever it is left unattended.
3.2.2.3 Backing up Users' Data	
13.	Data can be lost following a power outage or an accident, or as a result of an operating error or even a malevolent act. The Information Systems function makes servers available to users for storing their data. • Critical data should not be stored on the local hard drive of the workstation or laptop except temporarily while traveling. Each user is responsible for storing his/her data on servers provided by the Information Systems function.

3.2.2.4 Prevention of Laptop Thefts/Loss of Information	
14.	Given the potential significant damage and disruption to business activities that could result from the loss or theft of a laptop, it is crucial that users diligently apply basic antitheft protection and safety measures. • Outside of work hours, all laptops must be stored in a locked cabinet and hidden from view • During work hours, a suitable security cable delivered with the equipment must secure every laptop • When traveling, it is mandatory that users: ○ Keep the laptop with them or store them in a secure location when not in their custody ○ Do not work on confidential activities on their laptop when on public transportation
3.2.2.5 Use of External Electronic or Magnetic Media	
15.	External electronic or magnetic media used to store data require special vigilance. Since these media can be easily misplaced or stolen, it is crucial that any sensitive data they contain be protected. • It is mandatory that any sensitive data copied onto external media must be protected (by encryption) with the tools provided by the Information Systems function ○ Users must not use unknown electronic media on Sanofi systems (such as media that has been found or provided by an external partner or colleague). In case of doubt, contact your IS Security Officer or the Service Desk for analysis/assistance.
3.2.2.6 Encrypting Data	
16.	For the company, information of an industrial, financial, commercial or contractual nature, data stemming from research or development, and data on employees represent assets that must be protected. Special care should be given to personal data and sensitive personal data. • The encryption tools made available by the Information Systems function must be used whenever the confidentiality of information must be protected

3.2.2.7 Software Installation	
17.	The protection of the user's workstation against computer viruses and respect for copyright is achieved primarily through compliance of the workstation with the applications and software indicated by the Information Systems function. • Only authorized persons in the Information Systems function may install software on a workstation
3.2.2.8 Use of Mobile Devices	
18.	With the increasing popularity of mobile devices (laptops, smart phones, tablets, etc.), it is essential to consider the security risks when accessing Sanofi services and storing Sanofi data using portable devices. Written approval must be obtained from the user's manager for personal mobile devices to access the corporate email system. If approved, this shall be done via approved mobile client software that is configured and supported by authorized persons in the Information Systems function. • User and/or device authentication must be employed to access Sanofi services via the company network • All Sanofi data stored on the mobile device must be encrypted • In the event of loss/theft of the mobile device (with the exception of laptops), all corporate data on the device will be wiped. This includes personal mobile devices (i.e., devices not provisioned and not managed by the Information Systems function). • Users must contact the Service Desk to report any lost/stolen mobile device • No support will be provided by the Service Desk for non-professional applications installed on mobile devices that attach to Sanofi services • The installation of applications that compromise Sanofi services in any way are strictly prohibited and subject to removal • In the event of an incident, all mobile devices connecting to Sanofi services and/or storing Sanofi data are subject to investigations by Digital Cyber Security as deemed necessary and in accordance with local laws and regulations
3.2.2.9 Maintaining a Secure Work Area	
19.	Users are responsible for securing any printed or handwritten information whenever it is not in use or is unattended, in order to protect sensitive corporate and client assets by limiting exposure. The disposal of sensitive documents must be done in a secure manner. Sensitive documents must not be left in meeting rooms or fax/copy areas.

3.2.2.10 Teleworking	
20.	If a user is participating in a teleworking arrangement (to work remotely), the user must ensure adequate protection of Sanofi data and equipment at the remote location in accordance with the rules outlined in section 3.2.2. The user must take the following additional precautions: • Ensure the confidentiality of access to applications and data • Store Sanofi data on Sanofi provisioned/managed devices only • Properly secure the remote use of Sanofi equipment • Ensure that no Sanofi document is placed in the trash but instead shredded on-site or brought to the office for destruction • Avoid improper or fraudulent use of Sanofi resources
3.2.2.11 Company Assets	
21.	Upon termination of employment from Sanofi (or an affiliate), it is mandatory for the user to: • Return all company provisioned assets to their immediate manager or to any other department identified as responsible in accordance with Sanofi's regional off-boarding process, by the last day of his/her employment and prior to leaving the company premises Conversely, it is mandatory for the user's manager or any other department identified as responsible in accordance with Sanofi's regional off-boarding process, to: • Ensure that all assets are collected and returned to Digital (if Digital has not proactively collected the assets already), within two weeks of the user's departure • Ensure that any necessary business data is transferred prior to the user's departure • Contact the Service Desk in the event that assets are lost/stolen or cannot be returned
3.2.3 Rules Relating to Network Access	
3.2.3.1 Authentication of Information System Access	
22.	Access to the company information systems requires the use of unique identifiers and personal passwords. Accordingly, unless proven otherwise, any connection made using these identifiers will be presumed to have been made by their holders.

	• To access information systems, users must use only the access identifiers given to them by administrators, and must keep passwords secret. Passwords must never be shared with anyone for any reason.
3.2.3.2 Accessing Sanofi Internal Networks	
23.	Access points to the company internal networks, indicated and secured by the Information Systems function, ensure that the company's communications and data are secure and protected. • Communication with the company internal networks may only be done through the access points indicated and secured by the Information Systems function • The connection of unauthorized equipment to the company internal networks is prohibited
3.2.3.3 Access Networks Outside Sanofi	
24.	Access points to networks outside the company, indicated and secured by the Information Systems function, ensure that the company's communications and data are secure and protected. • Communication with networks outside the company may only be done on Sanofi premises through the access points indicated and secured by the Information Systems function, with the exception of the Sanofi webmail service, which can be reached from any system • Access to personal home networks or to remote networks for non-Sanofi related work is prohibited
3.2.4 Rules Relating to Using Communication Systems	
3.2.4.1 Transferring Large Files on the Internet	
25.	The use of Internet services, such as visiting sites, e-mail or file transfers must not have a significant effect on the availability of the computer network for other users. If required, due to performance conditions or security, the Internet connection may be cut without notice until the situation returns to normal. • Tools made available by the Information Systems function must be used to securely transfer and share files
3.2.4.2 Validating Email/Messages from the Internet	
26.	Since the identity of the sender of Internet email cannot be guaranteed, the sender's identity or the content of the message could be modified or contain computer viruses. Close attention must be given to the authenticity of messages received.

	• Do not open email/Internet messages or attached files when these files are unsolicited, unexpected or without professional intent • Exercise care when clicking on links embedded in emails as they can be harmful in nature and can introduce viruses or malware to the Sanofi network
3.2.4.3 Email/Messages Sent Internally and Over the Internet	
27.	The use of email requires close attention when selecting email recipients. A routing error to a recipient outside the company can be harmful to the company. • Users are responsible for the emails they send and must accurately verify recipients prior to sending email messages • The use of personal webmail is authorized provided that such use is consistent with the personal usage guidelines described in this document, and personal webmail must not be used to create, send, receive, read or store business-related emails
3.2.4.4 Sending Sensitive Information Over the Internet	
28.	The company's position in an increasingly competitive global market requires that everyone exercise strict control over information they send over the Internet. • Any discussion or publication over the Internet of company data and information must be submitted beforehand to management for approval • Users are responsible for their conduct when using social networking sites and must adhere to Social Media guidelines as outlined by Sanofi • Users must never fill out Internet questionnaires, as they could possibly be in support of a competitive watch that is targeting the company or used to plan a social engineering attack • Users must not transmit or store company data to any external company, service or application that has not been expressly approved by the Digital Cyber Security function
3.2.4.5 Security of Conferencing	
29.	Users must take into account security best practices when conducting Sanofi meetings to prevent unauthorized access. This includes video conferences/VTCs, web sessions, teleconference calls, etc. • Passwords/passcodes must be entered prior to joining Sanofi's internal discussions or confidential meetings

	• Calls must never be recorded • Participants must be verified before any internal or confidential discussions are conducted

4. RESPONSIBILITIES

It is the responsibility of the Global Head of Digital Cyber Security to enforce the use of the requirements in this document.

It is the role of all users of Sanofi information systems to comply with the requirements in this document.

5. REFERENCES

None

6. DEFINITIONS

Not Applicable

7. APPENDICES

CLICK CONTRACT

7.1 SUBJECT

The Information Technology and Solutions Usage Standard of Sanofi relies on principles stated by the Information Systems Security Policy of the company.

This document describes the main risks from which the company information systems could be exposed and by consequence states **the rules that each user must respect** to preserve information systems in its whole and particularly the quality of the professional spaces, secure and therefore of trust.

The objective of the “Click” contract of Sanofi is to inform all users of information systems that they must know the Information Technology and Solutions Usage Standard available on the Intranet and/or standard global document repository.

7.2 IMPLEMENTATION CONDITIONS

All workstations belonging to Sanofi and all its subsidiaries must be configured to ensure the implementation of the “Click” contract.

This implementation consists of displaying to the users a screen of information text which is the “Click” contract before allowing connection to the company network.

The user must use the “Ok to continue” button to access the login screen to allow connectivity to Sanofi networks.

7.3 INFORMATION TEXT OF THE « CLICK » CONTRACT

The information text of the “Click” contract is as follows:

“You will be connected to Sanofi Information Systems.

You commit yourself to read and scrupulously observe the rules exposed in the ITS Usage Policy of Sanofi whose text is available on the Intranet and/or standard global document repository.“

<OK to continue> button

FRENCH VERSION : CHARTE D’UTILISATION DES SYSTEMES D’INFORMATION

8. PROPOS

La Charte d'Utilisation des Solutions & Technologies de l’Information de Sanofi repose sur les principes énoncés par la Politique de Sécurité des Systèmes d’Information de Sanofi et de toutes ses filiales.

Ce Standard décrit les principaux risques auxquels les Systèmes d’Information de Sanofi et des filiales peuvent être exposés. Pour éviter ces risques, le Standard édicte **les règles que chaque utilisateur doit respecter.** Le respect de ces règles permettra à Sanofi de maintenir et préserver la sécurité des systèmes d’information 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 du Système d’Informations 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.

- L'accès aux systèmes d'information 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 ces identifiants de connexion et sont individuellement responsables de toutes les actions réalisées avec ces identifiants.
    - Le Service Desk local doit être contacté 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 d'éthique 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 faire preuve de vigilance en traitant et manipulant des données personnelles.
- Afin de garantir la sécurité des systèmes d'information 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 d'information de Sanofi et de toutes ses filiales doit prendre connaissance du texte complet de ce document.

9. DOMAINE D'APPLICATION

Ce document s'applique à tous les utilisateurs des Systèmes d'Information de Sanofi et à toutes ses filiales.

10. EXIGENCES

30.	Ces exigences s'appliquent à tous les utilisateurs des Systemes d'Information

10.1 INTRODUCTION

31.	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 d'information, des données et réseaux de Sanofi (et de ses filiales) prenne pleinement conscience des nombreux risques qui pèsent sur les Systèmes d'Information, 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.

10.1.1 Principaux Risques Liés Aux Systèmes d'Information

32.	Enumérer l'ensemble des risques liés aux Systèmes d'Information serait une gageure en raison de l'évolution constante des technologies dans le domaine informatique. 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 d'Information de Sanofi sans en avoir été habilité

	• Blocage des Systèmes d'Information 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
10.1.2 Stratégie de Protection de l'Entreprise	
33.	Face à l'accroissement des risques qui pèsent sur notre système d'information, 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 informatiques et de télécommunications au sein desquels la protection des données est effective • Cette stratégie s'appuie sur des Règles de Sécurité des Systèmes d'Information ainsi que sur des Politiques de sécurité des Systèmes d'Information 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.
10.1.3 Controle des Connexions	
34.	La protection des intérêts de Sanofi face aux menaces qui peuvent peser sur son Système d'Information rend nécessaire la mise en place d'une architecture de sécurité en profondeur (routeurs sécurisés, pare-feux, outils de détection d'intrusion, serveurs d'antivirus, logiciels de chiffrement, etc.). Cette architecture de sécurité permet en particulier d'identifier et d'authentifier chaque utilisateur lors de ses accès aux Systèmes d'Information 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 du Système d'Information de l'entreprise.

	Ces échanges, qui sont tracés et archivés par les équipements de sécurité, peuvent comporter les informations suivantes : • L'identité des utilisateurs • Les dates et heures des communications • Les sites consultés et les applications utilisées • Le détail des actions effectuées • La taille des messages ou le volume transféré • L'objet des messages • 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.
10.2 REGLES DE COMPORTEMENT DES UTILISATEURS	
10.2.1 Règles générales	
10.2.1.1 Respect de la Politique de Sécurité des Systèmes d'Information de Sanofi	
35.	L'utilisation des Systèmes d'Information de la société implique la prise de connaissance des différents documents constituant l'ensemble des Politiques de Sécurité des Systèmes d'Information 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 d'Information et respecter les règles énoncées

10.2.1.2 Usage des moyens informatiques	
36.	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 d'Information de la société. Toute utilisation à des fins illicites de ces moyens informatiques engagera la responsabilité personnelle de l'utilisateur. • Les moyens informatiques mis à la disposition des utilisateurs sont, par principe, réservés à un usage professionnel. • Une utilisation personnelle occasionnelle des Systèmes d'Information et de Communication de l'entreprise peuvent être tolérée, à condition qu'une telle utilisation : o Soit conforme avec le code d'éthique de Sanofi, les Politiques de Sanofi et les lois/règlements applicables o Ne nuit en aucun cas avec les intérêts ou la réputation de l'entreprise o 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 o Respecte les règles de sécurité et de sureté mentionnées ci-dessus o *N'impacte pas l'usage normal ou les performances du Système d'Information ou du réseau d'entreprise*
10.2.1.3 Signalement d'un événement de sécurité	
37.	Tout événement de sécurité concernant les Systèmes d'Information doit impérativement être signalé sans délai par l'utilisateur au Service Desk. Le Service Desk avertira de l'incident le contact local de la Cyber Sécurité Digitale ou le responsable de la Sécurité des Systèmes d'Information (cf paragraphe 10.1.1 pour les exemples des types de menaces potentielles pouvant constituer un incident de sécurité). Le contact local de la Cyber Sécurité Digitale ou le Responsable de la Sécurité des Systèmes d'Information pourra être contacté directement pour des cas sensibles.
10.2.1.4 Protection de l'image de Sanofi	
38.	Il est fondamental que chaque utilisateur soit conscient du fait que tous les serveurs Internet conservent les traces détaillées de toutes les visites. Les serveurs Internet 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 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, medias 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
10.2.1.5 Respect des législations nationales	
39.	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 : o Mettent en cause l'honorabilité ou la réputation d'une personne o Revêtent un caractère discriminatoire ou incitent à la haine raciale De même, doivent être rigoureusement respectées les législations protégeant notamment: o Mettent en cause l'honorabilité ou la réputation d'une personne o 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

10.2.2 Règles relatives à la protection du poste de travail

10.2.2.1 Extinction journalière du poste de travail

40.	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

10.2.2.2 Activation manuelle de l'écran de veille

41.	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.

10.2.2.3 Sauvegarde des données utilisateurs

42.	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 Fonction Système d'Information 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 sauf de manière temporaire à l'occasion de voyages. Chaque utilisateur doit veiller à stocker ses données sur les serveurs référencés par la Fonction Systèmes d'Information.

10.2.2.4 Prévention des vols/pertes de postes de travail portables

43.	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. • En dehors des heures de travail, tout portable doit être rangé dans une armoire fermée à clé et hors de vue

	• Pendant les heures de travail, tout portable doit être attaché par un câble de sécurité adéquat, livré avec l'ordinateur portable
	• 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 transports publics

10.2.2.5 Utilisation des supports magnétiques et électroniques externes	
44.	Les supports magnétiques ou électroniques externes permettant le stockage de données, nécessitent une vigilance particulière. Ces supports étant faciles à égarer ou à voler, il est impératif de toujours protéger les données qu'ils contiennent. • Toute donnée sensible à transférer sur un support externe doit obligatoirement être protégée (par chiffrement) avec les outils fournis par la Fonction Systèmes d'Information ○ 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 votre responsable de la sécurité des Systèmes d'Information ou le Service Desk pour analyse/assistance.
10.2.2.6 Chiffrement des données	
45.	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 Systèmes d'Information, doivent être utilisés chaque fois qu'il est nécessaire de protéger la confidentialité des informations
10.2.2.7 Installation de logiciels	
46.	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 Systèmes d'Information. • Seules les personnes habilitées au sein de la Fonction Systèmes d'Information peuvent réaliser les installations de logiciels sur un poste de travail

10.2.2.8 Utilisation d'équipements mobiles

47.	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 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 Systèmes d'Information. • 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 Systèmes d'Information. • 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 Digitale si cela est estimé nécessaire et en accord avec les lois et règlements locaux

10.2.2.9 Maintien d'un environnement de travail sécurisé

48.	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.
10.2.2.10 Télétravail	
49.	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 10.2.2. 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
10.2.2.11 Equipements de l'entreprise	
50.	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

10.2.3 Règles relatives à l'accès aux réseaux

10.2.3.1 Authentification d'accès aux Systèmes d'Information

51.	L'accès aux Systèmes d'Information 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 d'Information, 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.

10.2.3.2 Accès aux réseaux internes de Sanofi

52.	Des points d'accès aux réseaux internes de la société, référencés et sécurisés par la Fonction Systèmes d'information, 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 Systèmes d'Information • La connexion d'un équipement non autorisé au réseau interne de l'entreprise est interdite

10.2.3.3 Accès aux réseaux externes de Sanofi

53.	Des points d'accès aux réseaux externes à *la société*, référencés et sécurisés par la Fonction Systèmes d'Information, 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 Systèmes d'Information 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 distants pour des travaux non en lien avec l'activité de Sanofi est interdit

10.2.4 Règles relatives à l'usage des Systèmes de Communication

10.2.4.1 Transferts de fichiers volumineux avec l'Internet

54.	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 Systèmes d'Information doivent être utilisés pour partager et transférer les fichiers de manière sécurisée

10.2.4.2 Contrôle de la réception des messages Internet

55.	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 modifiés 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

10.2.4.3 Contrôle de l'envoi des messages

56.	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 pas être utilisés pour créer, envoyer, recevoir, lire ou stocker des emails professionnels.

10.2.4.4 Envoi d'information sensible sur internet	
57.	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 Digitale
10.2.4.5 Sécurité des conférences	
58.	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. • Un mot de passe doit être saisi avant de rejoindre une discussion interne Sanofi ou des réunions confidentielles • Les appels ne doivent jamais être enregistrés • La légitimité des participants doit être vérifiée par le responsable de la réunion avant le début d'une discussion confidentielle ou interne

11. RESPONSABILITES

La Direction de la Fonction Cyber Sécurité Digitale est en charge de mettre en œuvre l'utilisation de cette politique.

Les utilisateurs des Systèmes d'Information de Sanofi doivent se conformer à cette politique.

12. REFERENCES

None

13. DEFINITIONS

Not Applicable

14. ANNEXES

CONTRAT CLIC

14.1 OBJET

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

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

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

14.2 CONDITIONS DE MISE EN ŒUVRE

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 d'Information.

14.3 TEXTE D'INFORMATION DU CONTRAT « CLIC »

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

« Vous allez vous connecter aux Systèmes d'Information de Sanofi.

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

15. DOCUMENT HISTORY

Version Number	Version application date	Description of change
1.0	7 Nov 2015	**History of changes (legacy documents) :** Initial version of this Operational Standard is superseding the Usage Policy DSSI-PLUG-001-EN version 5.0. There was no change made in the core document, this new reference is version is only due to publication of the documents in the Global Document Repository.
2.0	16 Sep 2016	Changed title from "Information Systems Usage Charter" into "Information Technology and Solutions Usage Policy" Replaced "Charter" by "Policy" throughout the document Replaced "Information Solution" by "Information Technology & Solutions" (IS by ITS) throughout the document as relevant Revisited the hierarchy of the different sections Addition of the applicable/effective "Click" Contract Usage Policy (DSSI-PLUG-002-EN v4.0), into the Appendix section, due to the consolidation/merge of legacy ITS Security Policy documents performed in June 2016.
3.0	20 Apr 2018	Minor updates to sections 1, 5.1,1 and 5.2.2.6 to include GDPR/data privacy requirements
1.0	N/A	**Creation of new quality document (Standard)** This document will replace "GDPOL-013857 - Information Technology and Solutions Usage Policy" (V3-0) and the "GDPOL-013902 - Charte d'utilisation des Systèmes d'Information" (V1-0). These two documents have been merged to create this new Standard. Replaced "Policy" with Standard" to align with Quality documentation structure (document types) The main changes are: Minor updates to replace "ITS" references with "Digital" and merge the French version of this document, i.e. Charte d'utilisation des Systèmes d'Information (GDPOL-013902) into this document for simplification.

End of Document

Specificities

ITS Security	Information Technology and Solutions	
E - Manage Information System	E.2 - Align, Plan & Organize	
APO13 - Manage Security	No Subsystem	No Subsystem

Applicability

Entity / GBU	Sanofi Company		
Geography	Worldwide		
Applications Services	All		
Migration Number	GDPOL-013857 / GDPOL-013902		