Sanofi Digital Usage Principles

Contents

1. Purpose

The Digital Usage Principles of Sanofi is based on requirements stated in the Information Systems Security Policy set of Sanofi and all its subsidiaries.

This document describes the main risks to information systems of Sanofi and its subsidiaries. To avoid these risks, this document 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.

The French version of this document, *Charte d'utilisation des Technologies Digitales de Sanofi*, is available in the standard global document repository.

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
    - Sanofi does not support personal data recovery from company workstations upon employee departure
- 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 Code of Conduct, general legislation protecting patents, author rights, human dignity, professional secrecy, etc. must be strictly respected
- Sanofi employees and contractors must comply with Sanofi's Global Privacy Policy accessible from the Internet or Intranet 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

These requirements are applicable for all Information Systems users.

3.1 Introduction

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

Listing all 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

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

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, endpoint detection and response, 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 (non-exhaustive list):

- User's identity
- Communication dates and times
- Sites visited and applications used
- Details of requests made
- Subject, size, and metadata of messages or volume transferred
- External data transfer
- Source, activity, and 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

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

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 Conduct, 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

- *REMINDER: Sanofi does not support personal data recovery from company workstations upon employee departure.*

3.2.1.3 Reporting of a Security Incident

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 Cyber 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

Users must understand that all internet sites or public digital services 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

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

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

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

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 Digital function makes services available to users for storing their data.

- Critical data should not be stored on the local hard drive of the workstation or laptop. Each user is responsible for storing his/her data using services provided by the Digital function.

3.2.2.4 Prevention of Laptop Thefts/Loss of Information

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.

- Anti-theft measures (locked cabinet storage, for instance) must be taken by the owner

- When traveling, strengthen security measures based on context. It might include keeping devices visible at all times and immediately alerting the Service Desk if unauthorized persons handle the equipment.
- Do not work on confidential activities on laptop when on public transportation

3.2.2.5 Use of External Electronic or Magnetic Media

Digital standard solutions must be used for data storage and transfer needs. In case standard solutions cannot be used, the following recommendations must be applied:

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 Digital 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 Cyber Security Officer or the Service Desk for analysis/assistance.

3.2.2.6 Encrypting Data

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 Digital function must be used whenever the confidentiality of information must be protected

3.2.2.7 Software Installation

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 Digital function.

- Only authorized persons in the Digital function may install software on a workstation

3.2.2.8 Use of Mobile Devices

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 Digital 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 Digital 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

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

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

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

All Sanofi devices must, without exception, to be returned at the end of the lifecycle to ensure proper reuse or waste management and to protect Sanofi data**.**

3.2.3 Rules Relating to Network Access

3.2.3.1 Authentication of Information System Access

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

Access points to the company internal networks, indicated and secured by the Digital 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 Digital function
- The connection of unauthorized equipment to the company internal networks is prohibited

3.2.3.3 Accessing Networks Outside Sanofi

Access points to networks outside the company, indicated and secured by the Digital 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 Digital 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

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 Digital function must be used to securely transfer and share files

3.2.4.2 Validating Email/Messages from the Internet

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

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
- Personal webmail is permitted for personal use only as outlined in the guidelines. Business-related emails or attachments must never be handled through personal webmail accounts.

3.2.4.4 Sending Sensitive Information Over the Internet

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

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.

- Confidential calls must never be recorded
- Participants must be informed prior to initiating the recording of meetings
- 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. Appendices

CLICK CONTRACT

5.1 SUBJECT

The Digital Usage Principles of Sanofi relies on requirements stated by the Information Systems Security Policy set 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 Digital Usage Principles available on the Intranet and/or standard global document repository.

5.2 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 a screen of information text to the users, which is the "Click" contract, before allowing connection to the company network.

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

5.3 INFORMATIONAL TEXT OF THE « CLICK » CONTRACT

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

"You will be connected to Sanofi's Information Systems.

You commit to read and follow the rules and guidelines outlined in the Sanofi Digital Usage Principles at all times. The Digital Usage Principles is available on the Intranet and/or standard global document repository."

<OK> button to continue.