Preamble

D-SINE AFRICA implements an information and communication system necessary for its activity, including in particular a physical and virtual computer network, as well as fixed and mobile computer equipment.

Users/researchers, in the exercise of their functions, are required to access and use said computer equipment, as well as the information communication and data collection systems (REDCAP) made available to them.

The use of the information, communication and data collection system (REDCAP) must be carried out exclusively for professional purposes, unless otherwise provided for in this charter.

Furthermore, third parties to D-SINE AFRICA (users, external service providers, partners, etc.) may also have access to D-SINE AFRICA's IT equipment and information and communication systems.

However, the use of computer equipment (hardware and software), communication networks and the information system poses a risk for D-SINE AFRICA concerning the operation, security and integrity of its information system. and communication, but also concerning data (personal or not, sensitive or not) which are processed within the framework of D-SINE AFRICA's activity.

Also, with the aim of transparency towards users, promotion of fair, responsible and secure use of the information system and computer equipment, this charter establishes rules relating to the use of these resources and this in particular in compliance with the rules specific to health professionals, research, etc.

The objectives of this charter are:

- to make users aware of the risks linked to IT security in terms of freedoms and privacy, in particular through the processing of personal data that they are required to carry out;
- to inform users about:
  - the permitted uses of the IT resources made available to it;
  - the safety rules in force;
  - the control measures taken by D-SINE AFRICA;
  - any sanctions incurred by users;
- to formalize the general security rules that users undertake to respect, in return for the provision of information systems and computer equipment, and thus to determine the rights and duties of users.

These rules are part of a responsible approach in order to protect on the one hand the information heritage and the brand image of D-SINE AFRICA, and on the other hand the freedoms and private lives of the persons concerned who are the users and D-SINE AFRICA researcher and third parties linked to D-SINE AFRICA (monitored users, external service providers, partners, etc.).

The Information support technician (IST) or the Information Systems Director (ISD), the General Management (GM) and the Personal Data Protection Officer (PDPO) or the DPO (Data Protection Officer) meet available to users who would like additional information or advice relating to the use of information systems and computer equipment.

D-SINE AFRICA can also identify a Data Controller within the structure.

Definitions

“**IT equipment”:** refers to all the materials, equipment, IT tools made available by D-SINE AFRICA to Users. (Laptops, telephone tablets, removable disks, USB keys, etc.)

“Concerned persons”: refers to natural persons whose personal data are processed by D-SINE AFRICA or by any third party via the information, communication and data collection system (REDCAP) of D-SINE AFRICA, or via IT Equipment.

“Users”: refers to any person who uses D-SINE AFRICA’s information systems and IT Equipment regardless of their status, and in particular corporate officers, users, temporary workers, interns, employees of service providers, occasional visitors, followed users and in general, to any person who has obtained a right to use the D-SINE AFRICA information system or its IT equipment.

Scope

Persons targeted within D-SINE AFRICA

The obligations described in this charter apply to any person who uses D-SINE AFRICA’s information systems. This applies, in particular, to users of D-SINE AFRICA, interns, temporary workers, and in general, to any user who has obtained personal rights of use.

This charter must be annexed to the service contract concluded with third parties concerning IT.

Access by third parties to D-SINE AFRICA information systems

Any user external to D-SINE AFRICA may only have access to D-SINE AFRICA's information systems subject to express prior authorization issued by the Hierarchy and undertakes, therefore, to respect all of the provisions of this charter.

Computer and electronic communication means concerned

This charter concerns all computer and electronic communication means which are made available to users for professional purposes exclusively, as well as all computer and electronic communication means which are the personal property of the user, and for which he has obtained authorization for use within the framework of his professional activity.

The information and communication and data collection systems (REDCAP) of D-SINE AFRICA are notably made up of the following elements:

- laptops or desktop computers,
- peripherals (including USB keys),
- computer networks (servers (Cloud), routers, connectors, WIFI terminals),
- photocopiers,
- telephones (fixed and mobile) and smartphones,
- electronic tablets,
- software,
- computer files and databases,
- individual storage spaces,

messaging,

- Internet, intranet, extranet connections.

Possible exceptions

Any request for exemption from the various elements defined within the framework of this Charter must be presented in writing to the Information support technician (IST). The final decision is then taken in consultation with the hierarchy, which reserves the right to accept or refuse exemption requests.

Use of Information Systems and communication tools

Access

Access to certain elements of the information system (such as electronic or telephone messaging, sessions on workstations, the network, certain applications or interactive services) is protected by connection parameters (username, password).

Each user receives by SMS an individual access right which is materialized by any logical or physical means (user code and password).

These settings are personal to the user and must be kept confidential. In particular, they make it possible to control user access. They must not be communicated to anyone, neither to the line manager nor to IT. As far as possible, these settings should be memorized by the user and not stored in any form whatsoever. In any case, they must not be transmitted to third parties or easily accessible. They must be entered by the user each time they are accessed and not stored in memory in the information system.

When chosen by the user, the parameters must respect a certain level of complexity and be modified regularly. Security instructions are developed by the Information support technician (IST).

The user undertakes to respect the considerations of effectiveness of a password, which depends on the number of alphanumeric characters (X characters at least, and other specificities, etc.), its originality, its regular renewal by the user (every Y months,…).

Each user must identify themselves personally and cannot use the identity of others (even with the latter's consent).

This right of access ceases automatically upon departure or at the end of a Project (the user leaving D-SINE AFRICA) and can be modified during a change of assignment (change of position, transfer, etc..) or if it is found that the user has breached one of the obligations imposed by this charter.

Electronic messaging:

- **General principles**

Each User has, for the exercise of his professional activity, an electronic mail address assigned by the Information support technician (IST)

Electronic messages received on professional email are subject to antiviral control and anti-spam filtering.

Users are invited to inform the IT department of any malfunctions they observe in this filtering system.

Users' attention is drawn to the fact that an electronic message has the same scope as a handwritten letter and can quickly be communicated to third parties. Care should be taken to respect a certain number of principles, in order to avoid malfunctions of the information system, to limit the sending of unsolicited messages and not to incur civil or criminal liability for D-SINE. AFRICA and/or the user.

Users must ensure compliance with laws and regulations, and in particular the protection of intellectual property rights and the rights of third parties. Electronic correspondence must not contain illegal elements, such as defamatory, insulting, infringing or likely to constitute acts of unfair or parasitic competition.

For reasons of memory capacity, electronic messages are kept on the mail server for a maximum period of 2 year(s). A limitation on the size of electronic messages is implemented in order to encourage the user to sort messages regularly. After this period, they are automatically deleted. If the user wishes to keep messages beyond this period, it is up to them to make backups with the help of the Information support technician (IST) if necessary.

- **Sending electronic messages**

Before any sending, it is imperative to carefully check the identity of the recipients of the message and their capacity to receive communication of the information transmitted. In the presence of confidential information, personal data or sensitive data, these checks must be reinforced; If necessary, encryption of messages may also be proposed by the IT department.

In the event of sending to a plurality of recipients, the user must respect the provisions relating to the fight against the mass sending of unsolicited letters. He must also consider the opportunity to hide certain recipients, by putting them in hidden copy, so as not to communicate their email address to all the recipients.

User vigilance must be increased in the presence of confidential information. In this case, the messages must be encrypted, in accordance with the recommendations of the Information support technician.

Important messages should be sent with acknowledgment of receipt or signed electronically.

The form of professional messages must respect the rules defined by the hierarchy, with regard to the formatting and especially the signature of the messages.

The signature of emails is subject to a standardized form. Each user undertakes to respect this form while avoiding any additional elements.

- **Receiving electronic messages**

The user must not open or respond to electronic messages such as spam, repeated electronic messages, nor forward them when these are received without their knowledge on their professional electronic mail and have no relation to their functions and attributions within D-SINE AFRICA. In such cases, it undertakes to destroy them immediately and to notify the Information support technician in the event of obvious abuse of frequency or volume.

- **User absences**

The user is informed and accepts that in the event of prolonged absence or for the continuity of services, the information systems department reserves the right to access their messaging and professional files, without their consent. prior.

In the event of absence, the user must activate the delegation or absence notification function in order to prevent any discontinuity in the processing of messages and allow their interlocutors to take appropriate measures.

In the event of an emergency or for reasons related to the need to maintain a level of quality of service, D-SINE AFRICA may destroy or reset a user's access codes.

The user's electronic mail is kept on the D-SINE AFRICA server for a period determined by the Information support technician.

- **Personal use**

Messages of a personal nature are tolerated, provided that they respect the legislation in force, do not disrupt and respect the principles set out in this charter.

Messages sent must be marked "Private" or "Personal" in their subject and be filed upon sending in a folder named in the same way.

Messages received must also be filed, upon receipt, in a folder called “Private” or “Personal”.

In the event of violation of these rules, messages are presumed to be of a professional nature.

However, users are invited, where possible, to use their personal email for sending personal messages rather than the company email.

Internet/Intranet

As part of their activity, users must have access to the Internet.

The Information support technician (IST), for security reasons, may limit or prohibit access to certain sites. This is authorized to impose browser configurations and restrict the downloading of certain files.

Contribution by users to discussion forums, instant discussion systems, blogs, and sites is prohibited or authorized subject to prior authorization from the Information support technician. Such a mode of expression is likely to engage the responsibility of D-SINE AFRICA, increased vigilance of users is therefore essential.

Please note that users must under no circumstances engage in illicit activity or activity detrimental to the interests of D-SINE AFRICA, including on the Internet.

For security or ethical reasons, access to certain sites may be limited or prohibited by the IT department, which is authorized to impose browser configurations and install filtering mechanisms limiting access to certain sites.

Only consultation of sites related to professional activity is authorized.

In particular, the following are prohibited:

- Use of the Internet for personal commercial purposes with a view to making financial gains or supporting lucrative activities.
- the creation or updating using the D-SINE AFRICA infrastructure of any website, in particular personal pages.
- Connection to Internet sites whose content is contrary to public order, good morals or the brand image of the organization, as well as to those that may pose a risk to the security of the information system of D-SINE AFRICA or financially committing it.

Cessation of use

When leaving D-SINE AFRICA, the user must respect the departure procedure and hand over all the IT and electronic communication means given to them (computer, peripherals, mobile, access card, means of communication). remote authentication, badges, storage media, etc.) in good general working order and do not retain any material or data allowing access to the information system. In addition, the user is prohibited, before his departure, from destroying professional information and data.

Unless necessary for the continuity of the service and for a reasonable period of time which cannot exceed [three months], the user's email account is deleted on the day of their departure.

In the case where the messaging account is still active, even after the departure of a user, a redirection of messages can be set up by D-SINE AFRICA towards the user who has taken over the position of the user who left D- SINE AFRICA or any other person occupying a similar function.

His credentials are also disabled.

Unless an exemption is granted on a case-by-case basis by the Information support technician and which may in no case exceed a duration of [three months], elements marked “private”

or “personal” must be deleted by the user at the latest the day before their departure from D-SINE AFRICA.

Access to the Information System outside the Service (teleworking, in business, mobile center, etc. access to the remote office)

This article concerns the use of D-SINE AFRICA's information systems, its resources, and means of communication by the user when the latter is located outside the physical site of D-SINE AFRICA.

First of all, it should be noted that all the provisions of this charter are applicable to users accessing D-SINE AFRICA's information communication and data collection systems (REDCAP) remotely.

Furthermore, it is imperative that the user informs the IST in advance of the remote access that he will set up, in order to obtain prior authorization and that the security and confidentiality instructions specific to his situation are communicated to him. .

D-SINE AFRICA ensures that it takes out the necessary insurance to protect the IT and electronic communication resources made available.

Any remote access via personal computer equipment is prohibited without express written authorization from the Information support technician(IST).

Professional use

The information systems made available to users are reserved for exclusive professional use. Any use of computer and electronic communication means is deemed to have been made by the beneficiary of the access identification, for professional purposes.

Furthermore and independently of the aforementioned possible exemptions, use of information systems for personal purposes may be residual. Thus, both in frequency and duration, it can only be considered outside of working time and in a limited manner during working time, in accordance with the case law on the subject.

Computer directories and electronic exchanges must then be marked “private” or “personal”. The employer reserves the right to limit or suspend such use in the event of abuse.

Secrecy and confidentiality – transmission of information

Respecting data confidentiality is an essential requirement.

Safeguarding the interests of D-SINE AFRICA requires compliance with a general and permanent obligation of confidentiality and professional secrecy, with regard to the available data made available to the user for the exercise of his professional activity in particularly in the context of the use of information systems, but also of any processing.

Consequently, the user undertakes to respect this charter, as well as the texts in force and in particular to ensure that unauthorized third parties do not have knowledge of such information, in accordance with the rules of professional ethics or ethics, if applicable.

It is prohibited to use cryptology means other than those expressly authorized by D-SINE AFRICA.

IT systems administrators are bound by professional secrecy and they must not disclose information of a nominative nature, of any nature whatsoever, regardless of the hierarchical order. Under no circumstances are directors required to disclose this information unless there is a specific regulatory provision to this effect. In the event of non-compliance with these provisions by directors, they are exposed to sanctions regardless of the circumstances likely to give rise to their liability.

The transmission of confidential data can only be carried out under the following conditions:

- authorization of the issuer;
- designation of an authorized recipient;
- Compliance with a secure procedure.

D-SINE AFRICA reserves, for any reason whatsoever, temporarily or definitively, the right to grant, refuse, modify or delete all or part of the right of access of any person for related reasons. Directly to the continuity and security of services.

General security

Rules to respect

- **General principles**

Due to the collection of data and the processing thereof, D-SINE AFRICA undertakes, within the framework of the legal and regulatory provisions which are required to implement all useful organizational and technical measures in order to preserve the security, integrity and confidentiality of the Data, as well as the security of its information and communication system, on a technological and procedural level, in particular to prevent any unauthorized modification, transfer or deletion of Data, and any unauthorized intrusion into its information system or its damage.

However, the first risk remains the human risk linked to the processing and manipulation of Data by Users, and through the latter's use of the information and communication system and the tools linked to it.

Consequently, the implementation of security tools should not exempt users from reporting any attempted external intrusion, falsification or presence of viruses to the Information support technician.

All users are responsible, at their level, for contributing to the security of the means made available to them and the network to which they have access, mainly by avoiding the intrusion of viruses likely to damage the D-SINE information system. AFRICA.

- **User obligations**

The user undertakes to respect

- do not open attachments received from outside when the sender of the message is unknown;
- destroy “chain of solidarity” type messages;
- do not store and route gadgets received or found on the Internet;
- do not forward alert messages of the arrival of a virus but notify the Information support technician .
- modify the configuration of one's computer workstation carried out by the information systems department, whether by addition, deletion or modification, unless otherwise expressly agreed by the latter;
- provide unauthorized users with access to systems or networks through the equipment they use;
- use [even with their consent) or attempt to use accounts other than those assigned to them or hide their identity;
- do not take D-SINE AFRICA’s IT equipment outside the site of
- D-SINE AFRICA, unless agreed by the information system manager;
- do not download files, particularly media, unrelated to professional activity or presenting a risk to the information system;

The user is required to immediately inform his superiors of any malfunction, alteration, loss, theft, destruction and other events that may affect computer and electronic communication resources.

Any installation or use of software not expressly authorized by the Information support technician is prohibited.

As part of their business trips, regardless of their duration or frequency, the user must adopt an attitude of caution and reserve with regard to the information and resources of the information system that they may be required to access. access, manipulate or exchange.

In particular, it is not recommended to use wifi connection systems in public places.

Information systems control methods

The user is informed that D-SINE AFRICA implements traceability and filtering tools for the use of information and communication systems.

D-SINE AFRICA implements:

- connection logs for all information systems;
- filtering tools, in particular for content and Internet addresses, making it possible to analyze the conditions of use and possibly prohibit this or that protocol, or to restrict or prohibit access to the Internet or to certain categories of sites Internet.

Users' attention is drawn to the fact that it is thus possible to control their activity and their exchanges. Automatic and generalized checks may be carried out to limit malfunctions, in compliance with the rules in force.

The user is informed that the Information support technician (who must ensure the normal operation and security of computer networks and systems) is led

through its functions, to have access to all information relating to users (messages, Internet connection, etc.), including that which is recorded on the hard drive of their workstations but remains subject to the rules governing professional secrecy the Information support technician duly authorized by the director can control the information systems, in order to verify that the latter complies with the clauses defined in this charter.

In the event of suspicion of a serious breach of the provisions of this charter, management may take all necessary investigative measures, in compliance with the rules in force.

Any illicitly installed software or any suspicious file will be deleted by the Information support technician as soon as they are noticed on the workstation.

The “non-professional” nature of computer directories clearly identified as “private” or “personal” does not preclude control methods under the aforementioned conditions.

Additional information

The use of information systems implies respect for the intellectual property rights of the company, its partners and any third party holder of such rights. If in doubt, the user should contact the Information support technician .

Each authorized user undertakes to:

- use the software packages under the conditions of the subscribed license;
- not reproduce or use software packages, databases, web pages or other creations protected by copyright or private rights, without first obtaining authorization from the holder of these rights
- not copy or distribute texts, images, photographs, musical or audiovisual works or any creation copied on the Internet.

The user is informed that counterfeiting is an offense punishable by civil and criminal penalties.

This charter is communicated individually to each employee electronically.

The IST can provide users with any information concerning the use of the information system, in particular on backup and security procedures and on the rights of Data Subjects.

It regularly informs them of the evolution of the technical limits of the information and communication system as well as of the threats likely to weigh on its security.

Each user must comply with the security procedures and rules issued by the IST or DSI within the framework of this charter.

If necessary, users can be trained by the IST to apply the rules for using the information and communication system provided.

Sanctions

Please note that this charter is a document with legal significance, and therefore binding on Users.

Indeed, failure to comply with the rules and security measures described in this charter is likely to incur liability on the part of the user and result in warnings, limitations or suspensions of use of all or part of the system. information and communication, or even disciplinary sanctions, proportionate to the seriousness of the facts concerned.

In the latter case, the procedures provided for in the internal regulations and in the Labor Code will be applied.

D-SINE AFRICA also reserves the right to initiate or have criminal and/or civil proceedings initiated, regardless of the disciplinary sanctions implemented, in particular but not limited to in the event of computer fraud, non-respect of the rights of author or violation of the secrecy of correspondence.

The Information support technician may erase or isolate and retain for the purposes of proof any trace of software, software packages, programs or files created or introduced into the D-SINE AFRICA Information system, in violation of the rights of third parties, in particular of intellectual property, and report any criminal act to the authorities, without prejudice to the application of sanctions within the framework of its status.