Forewords

This document is a translation of the text adopted by the Board of Directors on March 8th, 2019.

The French version is this text is authoritative.

IT Charter of the *Observatoire de Paris*

(Article 7 of the Internal Regulations)

Information System Security Charter of the *Observatoire de Paris*

This charter, associated with the institution's Internal Regulations, is intended to inform Users of their rights and their responsibilities when using the IT resources and internet services of the *Observatoire de Paris*, in application of the General Information Security Policy of the *Observatoire de Paris* and the legislation.

It responds to the *Observatoire de Paris'* concern to protect the information that constitutes its heritage immaterial against any alteration, voluntary or accidental, of its confidentiality, integrity or availability. All breach of the rules governing the security of information systems is indeed likely to have an impact significant (human, financial, legal, environmental, harm to the functioning of the organization or to the potential science and technology).

The User contributes at his level to the security of Information systems. As such, he applies the safety rules in force in the Entity and reports any malfunction or event that appears to it to be abnormal.

The Entity provides the User with the means necessary for the application of the systems security policy of information.

At their level, the supervisory staff promotes the establishment of a "safety culture" by setting an example in the compliance with this charter and through active support from the teams in charge of implementing these rules.

Definitions

The term "User" will designate: the person having access to or using the computer resources and services Internet regardless of its status.

The term "Entity" will designate all the entities created by the *Observatoire de Paris* for the performance of its missions, in particular such as own or joint research or service units as well as departments and administration services.

I. Safety principles

The following rules apply to all Users, and may be supplemented by measures specific to their Entity resulting from the operational information systems security policy.

I.1. Protection of electronic information and documents

All Users are responsible for the use of the IT resources to which they have access.

The User protects the information he is required to handle as part of his duties, according to their sensitivity.

When creating a document, the User determines its level of sensitivity and applies the rules to guarantee.
its protection throughout its life cycle (marking, storage, transmission, printing, deletion, etc.).

When his data is not subject to automatic backups set up by the Entity to which he belongs, the User implements the manual backup system recommended by its Entity.

In order to guard against the risk of theft of sensitive documents, the User, when he is away from his office, ensures that his paper documents, when they exist, are stored under lock and key and that his workstation is locked.

I.2. Protection of means and rights of access to information

The User is responsible for the use of the information systems made with his access rights.

As such, he ensures the protection of the means of authentication which have been assigned to him or which he has generated (badges, password, private keys, private keys linked to certificates, etc.):

- The user never communicates his authentication codes in any way; this rule applies including to his line manager and to the team in charge of the IS of his Entity;

- It applies the rules of "generation / complexity" and renewal in force according to the means of authentication used;

- it shall use all means at his disposal to prevent the disclosure of his means of authentication;

- He modifies or requests the renewal of his means of authentication as soon as he suspects their disclosure;

- He guarantees access to his professional data, in particular within the framework of the recovery policy of data implemented within the Entity.

The User does not use the means of authentication or the access rights of a third party. Of the same way, he doesn't try to hide his own identity.

The User only uses his access rights to access information or services necessary to the exercise of the tasks entrusted to it and for which it is authorized:

- He is prohibited from accessing or attempting to access information system resources for which he has not received explicit authorization;

- It does not connect to the local networks of the Entity - whatever the nature of these networks (wired or wireless) - materials other than those entrusted or authorized by management or the Entity;

- He does not introduce data carriers (USB key, CDROM, DVD, etc.) without respecting the rules of the Entity and takes the necessary precautions to ensure their harmlessness;

. He does not install, download or use, on the Entity's equipment or on personal equipment used for professional purposes, software or software packages whose license fees have not been paid, or do not originate no trustworthy sites, or sites prohibited by the Entity;

. He undertakes not to voluntarily disrupt the proper functioning of IT resources and networks whether through abnormal manipulation of hardware or software.

The User informs the administrators of any evolution of his functions requiring a modification of his rights access.

I 3. Protection of IT equipment

The User protects the equipment made available to him:

- He applies the instructions of the IT team from the Entity's operational ISP in order to ensure in particular that the configuration of its equipment follows good security practices (application of patches security, encryption, etc.);

- He uses the means of protection available (anti-theft cable, storage in a lockable drawer or cupboard, etc.) to guarantee the protection of mobile equipment and the information it contains (laptop, USB stick, smartphones, tablets, etc.) against theft;

- In the event of absence, even temporary, he locks or closes all the sessions in progress on his workstation;

- He reports as quickly as possible to the person in charge of IS security (in charge of ISS within the Entity or, where applicable, ISS manager of the regional delegation) of any loss, theft or any suspected or proven compromise of equipment made available.

The User protects the personal equipment he uses to access, remotely or from the local network of a Entity, to the IS of the *Observatoire de Paris* or to store professional data in accordance with the rules laid down by the *Observatoire de Paris*.

The Entity informs and supports it in the implementation of its protection measures.

I.4. Protection from network traffic

I.4.1. Protection from network traffic

The *Observatoire de Paris* undertakes to provide the User with a personal professional mailbox allowing it to send and receive electronic messages. The use of this nominative address is made under the responsibility of the User.

The nominative aspect of the electronic address constitutes the simple extension of the administrative address: it does not in no way the professional character of messaging.

I.4.2. Content of exchanges on the networks

Electronic exchanges (mails, discussion forums, instant messaging, social networks, sharing of documents, voices, images, videos, etc.) respect the correction normally expected in any type of exchange written than oral.

The transmission of classified defense data is prohibited except for a specific approved device and the transmission of sensitive data must be carried out in accordance with the protection rules in force.

I.4.3. Vigilance

The User is vigilant with regard to the information received (misinformation, computer virus, attempted fraud, chains, phishing, ...).

I.4.4. Status and legal value of the information exchanged

Information exchanged electronically with third parties may legally form a contract under certain conditions or be used for probative purposes.

The User must, therefore, be careful about the nature of the information that he exchanges electronically at the same title as for traditional mail.

I.4.5. Storage and archiving of information exchanged

The User is informed that the email is an administrative document recognized as evidence in the event of litigation.

I.4.6. Protection from access to online services on the Internet

If a private residual use can be tolerated, it is recalled that the connections established thanks to the computer tool made available by the *Observatoire de Paris* are presumed to be of a professional nature.

The User uses his professional contact details, in particular his email address or other identifier, with precaution. By using them on sites unrelated to his professional activity, he facilitates attacks on his reputation, the reputation of the Entity or that of the *Observatoire de Paris*.

Some malicious sites take advantage of browser vulnerabilities to recover the data present on the workstation. Other sites make software available which, under an innocuous appearance, can take control of the computer and transmit its content to the pirate without the knowledge of the User. Finally, some sites do not provide any guarantee on the subsequent use that may be made of the data transmitted. Therefore, the User:

- Avoid connecting to suspicious sites;

- Avoid downloading software whose harmlessness is not guaranteed (nature of the publisher, download mode,etc.);

- Operates data backups, information sharing, collaborative exchanges, only on sites of trusted, made available by the establishment and whose security has been verified by the establishment (via example a security audit);

- Encrypts non-public data that would be stored on third-party sites or transmitted via unsecured messaging.

I.4.7. Publication of information on the Internet

Any publication of information on the Entity's internet or intranet sites is carried out under the responsibility of a designated site manager or publication manager.

No publication of information of a private nature (private pages in the non-professional sense) on the resources of the information system of the Entity is authorized, unless specific provision decided within the Entity.

The ISS manager of the *Observatoire de Paris* provides support to the User for the implementation of all of these measures.

II. Privacy and Personal Computing Resources

II.1. Residual privacy

Computing resources (workstation, servers, applications, messaging, Internet, telephone, etc.) provided to the User, by the *Observatoire de Paris* or its partners, are reserved for the exercise of their professional activity.

However, personal use of these resources is tolerated provided:
- That it stays short during working hours in the office;
- That it does not affect professional use;
- That it does not endanger their proper functioning and safety;
- That it does not violate the law, regulations and internal provisions.

All data is deemed to be professional with the exception of data explicitly designated by the User as having a private character (for example by indicating the mention "private" in the "subject" field of the messages).

The User stores his private data in a data space explicitly provided for this purpose or by mentioning the private character on the resource used. This space must not contain character data professional and should not occupy an excessive share of resources. Protection and regular backup of private data is the responsibility of the User.

II.2. Personal Computing Resources

Personal computer resources (computers, smartphones, tablets, etc. purchased with personal credits, when they are used to access the *Observatoire de Paris'* IS, must not call into question or weaken, the security policies in force in the Entities by insufficient protection or inappropriate use.

When these personal computing resources are used to access, remotely or from the local network of a Entity, to the IS of the *Observatoire de Paris* or to store professional data, these resources are authorized and secured according to the guidelines issued by the PGSI and declared to the IT department that manages the Entity's equipment fleet. Staff wishing to acquire such equipment first seek advice from their department computer science.

I.3. Departure management

The User is responsible for his private data space and it is up to him to destroy it at the time of his departure. In the event of exceptional circumstances (impromptu departure or death), the *Observatoire de Paris* does not retain the private data spaces present on the IT resources provided by the Paris *Observatoire de Paris* that for a maximum period of 3 months (time period allowing the User or his legal successors to recover the information that are there).

Professional data remains at the disposal of the employer. Data retention measures are defined within the Entity.

The user must, at the time of his departure, return to his Entity the computer equipment that will have been placed at his disposal (desktop or laptop computer, peripherals, storage devices, etc.).

III. Compliance with the Data Protection Act

If, in the performance of his duties, the User creates files containing personal data personnel subject to the provisions of the GDPR, he informs the unit director so that the declarations necessary can be carried out with the DPO of the *Observatoire de Paris*.

IV. Respect for intellectual property

The User does not reproduce, download, copy, distribute, modify or use the software, databases data, web pages, images, photographs or other creations protected by copyright or a private right, without having previously obtained the authorization of the holders of these rights.

V. Impact of the rights and duties specific to IS administrators on the user data

The law and regulations require the *Observatoire de Paris* to keep a history of accesses made by agents.
The *Observatoire de Paris* has therefore set up access logging, in accordance with the rules set out in the PGSI and the declaration made to the CNIL in application of law n ° 78-17 of January 6, 1978 as amended.

The administrator has access to the traces left by the User during his access to all IT resources made available to it by the Entity as well as on local and remote networks.

These traces (also called “log files” or “logs”) are saved for a maximum of 12 months.

Administrators may, in the event of a technical malfunction, intrusion or attempted attack on the systems computers, use these traces to try to find the origin of the problem.

These personnel are subject to an obligation of confidentiality. They cannot therefore disclose the information they are brought to know within the framework of their function, in particular when they are covered by the secrecy of the correspondence or concern the privacy of the user, since this information does not call into question or the proper technical functioning of the applications, nor their security.

They can learn or attempt to learn the contents of directories, files or messages manifestly and explicitly designated as personal only in the presence of the agent and with his express authorization, in case of justified emergency or necessity with regard to legislation and safety.

VI. Compliance with the law

The User is required to comply with the entire legal framework related to the use of information systems, as well as any other regulations that may apply.

In particular, the User must complies to:

- the law of 29 July 1881 amended on the freedom of the press. The User does not disseminate information constituting personality attacks (insult, discrimination, racism, xenophobia, revisionism, defamation, obscenity, harassment or threat) or which may constitute incitement to hatred or violence, or damage to the image of another person;
- the regulations relating to the processing of personal data (in particular law n° 78-17 of January 6 1978 amended relating to data processing, files and freedoms);
- the legislation relating to attacks on automated data processing systems (art. L 323-1 and following of the Penal Code) ;
- the Law No. 94-665 of August 4, 1994 as amended relating to the use of the French language;
- the law No. 2004-575 of June 21, 2004 on confidence in the digital economy;
- the provisions of the intellectual property code relating to literary and artistic property. The User does not no illicit copies of elements (software, images, texts, music, sounds, etc.) protected by property laws
intellectual;
- the provisions relating to respect for private life, public order and professional secrecy;
- the provisions relating to the Protection of the Scientific and Technical Potential of the Nation.

Some of these provisions are accompanied by penal sanctions.