# OCA Information System Security Charter

This charter, annexed to the internal regulations of Entities, is to inform users of their rights and responsibilities in connection with the use of OCA computer resources and Internet services, according to the General Information Security Policy (PGSI) of the OCA and the relevant legislation in force.

The PGSI in force in mixed units depends on the institution that is responsible for the security policy of the Entity; it is decided by collective bargaining agreements between institutions.

Research and Services units of OCA depend also from the CNRS. As a way to enforce a simplification policy, the present charter was adapted for the OCA from the CNRS's charter.
The present charte applies to all the OCA units's employees whatever their status. It applies to each and every person, with a permanent or temporary status, who is using the IT ressources and the internet access provided by OCA, as well as those they can access directly or with a rebound from the OCA network.
The charter can be consulted by users by any means and especially : by the approval of the charter before the creation of the IT account, by the reception by mail of the URL where they can download the charter, once he/she has read this email, if he/she proceed with the usage of IT ressources, he/she accepts automatically this charter, by a publication on the OCA's web site or by annexing this charter to the OCA's by-laws, and those of its units.

It responds to the concern of the OCA to protect the information that constitutes its intangible assets against tampering, accidental or deliberate, confidentiality, integrity or availability. Any breach of rules governing information systems security is indeed likely to have significant impacts (human, financial, legal, environmental, affecting the functioning of the organization or the scientific and technical potential).

The User makes a contribution to information system security. As such, he applies the security rules in force in the Entity and reports any malfunction or event that appears abnormal.

The Entity provides the User with the means necessary to implement the information systems security policy.

At a management level, executives promote the establishment of a "security culture" through their exemplary conduct in compliance with this charter, and active support for the teams responsible for the implementation of these rules.

## Définitions

"User" means the person accessing or using the computer resources and Internet services regardless of their status.

"Entity" means all entities created by the OCA for the fulfilment of its tasks, such as research units or in-house or mixed services and administrative departments.

# I. Security principles

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

## Protection of Information and Electronic Documents

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

Users protect information that they are required to handle in the course of their duties, according to their sensitivity.
When creating a document, the User determines its level of sensitivity and enforces the rules to ensure its protection throughout its life cycle (marking, storage, transmission, printing, deleting, etc.).

When their data is not subject to automatic backups put in place by the Entity to which they belong, Users implement the manual backup system recommended by the Entity.

To guard against the risk of theft of sensitive documents, when out of the office, the User shall ensure that any paper documents are kept locked up, and their workstation is locked.

## Protection of means and rights of access to information

Users are responsible for information systems use performed with their access rights.

In this respect, the user shall protect the means of authentication that have been assigned to them or generated (badges, passwords, private keys, private keys associated with certificates, etc.), that is to say:

- never disclose them, including to the manager and the IS team of their Entity;
- apply the "generation/complexity" and renewal rules in force depending on the authentication used;
- put in place all the means at their disposal to prevent the disclosure of their means of authentication;
- change or request renewal of their means of authentication if a disclosure is suspected.
- guarantee access to their professional data, especially in the context of the data recovery[1] policy implemented in the Entity.

The user shall not use the means of authentication or access rights of a third party. Similarly, they shall not seek to hide their own identity.

The User shall only use his rights of access to access information or services necessary for carrying out the tasks entrusted to him and for which he is authorized:

- He shall refrain from accessing or attempting to access information system resources for which he has not received explicit authorization;
- He shall not connect to local networks of the Entity - whatever the nature of these networks (wired or wireless) - equipment other than those assigned or authorized by the management or the Entity;
- He shall not insert data media (USB stick, CD-ROM, DVD, etc.) without respecting the rules of the entity and taking the necessary precautions to ensure their security;

1 Recovery is the back-up system allowing an authorised person to access data when the main mechanism is out of use (loss of password, for example)

- He will not install, download or use on the Entity's equipment or personal equipment used for business purposes, software or software whose license fees have not been paid, or do not come from reputable sites, or are prohibited by the entity;
- He undertakes not to voluntarily disrupt the smooth functioning of the computer resources and networks, by abnormal handling of either hardware or software.

The User shall notify administrators of any changes in his functions requiring modification of his access rights.

## Protection of computer equipment

The User shall protect the equipment at his disposal:

- he shall apply the guidelines of the IT team deriving from the operational ISSP of the Entity to ensure that the particular configuration of equipment follows good security practices (application of security patches, encryption, etc.).
- he shall use available means of protection (anti-theft cable, storage in a drawer or locked cabinet, etc.) to ensure the protection of mobile devices and the information they contain (laptop, USB, smartphones, tablets, etc. ) against theft;
- in case of absence, even momentarily, he shall lock or close all sessions running on the workstation;
- he shall report as soon as possible to the head of IT security (responsible for ISS in the Entity or, as applicable, the appropriate ISS manager of OCA) any loss, theft or compromising, suspected or proven, of equipment at his disposal.

The User shall protect the personal equipment he uses for remote access to or from the LAN of an Entity, OCA IS, or to store business data in accordance with the rules laid down by the OCA and the Entity.

The Entity shall inform him and support him in the implementation of his safeguards.

## Protection concerning exchanges on the network

### E-mail address

The OCA is committed to providing the user with a personal business inbox allowing him to send and receive electronic messages. The use of this registered address is the responsibility of the user.

The personal aspect of the email is a simple extension of the administrative address: it in no way removes the professional nature of messaging.

### Content of exchanges on networks

Electronic exchanges (e-mails, chat, instant messaging, social networking, sharing of documents, voice, images, videos, etc.) shall respect the standards normally expected in any type of exchange, both written and oral.

Transmission of classified defense data is prohibited unless vi a specifically authorized device, and transmission of sensitive data must be carried out according to the rules in force on protection.

## Vigilance

The User shall exercise vigilance vis-à-vis the information received (disinformation, computer virus, attempted fraud, chains, phishing, etc.).

## Legal status and value of the information exchanged

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

The User must, therefore, be careful about the kind of information that is exchanged electronically as well as by traditional mail.

## Storage and archiving of information exchanged

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

## Protection vis-à-vis access to online services on the Internet

While residual private use can be tolerated, it should be recalled that connections through the software tool provided by the OCA are presumed to be professional in nature.

The User shall use his business contacts, especially his e-mail address or other identifier, carefully. Using them on sites unrelated to his professional activity may harm his reputation, the reputation of the entity or the OCA.

Some malicious sites take advantage of vulnerabilities in browsers to retrieve data from the workstation. Other sites make seemingly innocuous software available that can take control of your computer and transfer its contents to hackers without the knowledge of the User. Finally, some sites do not provide any guarantee concerning the future use which might be made of data transmitted. Therefore, the User:

- avoids connecting to suspicious sites;
- avoids downloading software whose security cannot be guaranteed (nature of the publisher, download mode, etc.) ;
- only performs data backups, information sharing and collaborative exchanges on trusted sites, provided by the institution and whose security has been verified by the institution (e.g. via a security audit);
- encrypts private data stored on third party websites or transmitted via non-secure messaging.

## Publication of information on the Internet

Any publication of information on the internet or intranet sites of the Entity is carried out under the responsibility of a site manager or the publication manager named in person.

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

The ISS manager of the Entity or the ISS manager responsible for the appropriate office supports the User in the implementation of all these measures.

# II. Privacy and personal computer resources

## Residual privacy

Computing resources (workstations, servers, applications, mail, Internet, phone, etc.) provided to the User by the OCA and its partners, Public Scientific and Technical Research Establishments (PSTRE), university, etc., are reserved for his professional duties.

Personal use of these resources, however, is allowed provided that:

- it is only for a short period during office working hours;
- it does not affect professional use ;
- it does not endanger their proper functioning and security;
- it does not violate the law, regulations and internal rules.

All data is deemed professional with the exception of that explicitly designated by the user as being private (for example by indicating the word "private" in the "subject" field of the message).

The user shall store private data in a data space designed specifically for this purpose, or mentioning the private nature of the resource used. This space should not contain data of a professional nature and must not occupy a disproportionate share of resources. Protection and regular backup of private data is the responsibility of the User.

## Personal computing resources

Personal computing resources (computers, smartphones, tablets, etc., purchased through personal loans), when used to access the OCA IS, should not undermine or weaken the security policies in force in the Entities by insufficient protection or improper use.

When personal computer resources are used for remote access to or from the LAN of an Entity, the OCA IS, or to store business data, these resources are authorized and secured following PGSI guidelines and reported to the IT department that manages the hardware pool of the Entity. Personnel who wish to acquire such materials shall first seek the advice of their IT department.

## Management of departures

The User is responsible for his private data space, and is responsible for destroying data when he leaves. In exceptional circumstances (impromptu departure or death), the OCA shall retain private data spaces present on the computer resources provided by the OCA for a maximum period of 3 months only (a period allowing the user or his beneficiaries to retrieve the information therein).

Business data remains available to the employer. Measures for conserving business data are defined in the Entity.

# III. Compliance with the Data Protection Act

If, in carrying out his tasks, the user creates files containing personal data subject to the provisions of the Data Protection Act, he shall inform the Director of the unit so that the necessary statements can be made to the corresponding Data Processing Correspondent (CIL) of the OCA.

# IV. Respect for intellectual property

The User may not reproduce, download, copy, distribute, alter or use any software, databases, websites, pages, pictures or other creations protected by copyright or private law, without prior permission of the owners of these rights.

# V. The impact of rights and duties specific to IS administrators on user data

The law and regulations[2] require the OCA to keep a history of access by agents. The OCA has developed access logs, in accordance with the rules set out in the PGSI and the declaration made to the CNIL under law no. 78-17 of 6 January 2006, amended.

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

These traces (also called "log files" or "logs") are stored for up to 12 months.

Administrators may, in the event of technical malfunction, intrusion or attempted attacks on computer systems, use these traces to try to find the problem.

These personnel are subject to an obligation of confidentiality. They cannot therefore disclose information they are required to know in the course of their work, especially when they are covered by secrecy of correspondence or information within the private remit of the user, since this information does not call into question either the proper technical operation of the applications, or security.

They may inspect or attempt to read the contents of directories, files or messages clearly and explicitly designated as personal in the presence of the agent and with his express permission, in an emergency or justified necessity due to law or necessity.

# VI. Respect for the law

The User is obliged 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, he shall respect:
► Law of 29 July 1881, as amended, on freedom of the press. The User may not disseminate information constituting personal attacks (insults, discrimination, racism, xenophobia, revisionism, defamation, obscenity, harassment or threat) or which may constitute incitement to hatred or violence or harm to the image of another person, his beliefs or his sensibilities;
►regulations concerning the processing of personal data (including law no. 78-17 of 6 January 1978 relating to computers, files and freedoms);
►legislation on systems with automated data processing (art. L 323-1 et seq of the Criminal Code);
►Act N. 94-665 of 4 August 1994 as amended relating to the use of the French language;
►Act N. 2004-575 of 21 June 2004 on confidence in the digital economy;
►the provisions of the code of artistic intellectual property. Users shall not make illegal copies of elements (software, images, text, music, sound, etc.) protected by intellectual property laws;

2 In particular article 6-II of the Law on Digital Confidence (LCEN) of 21 June 2004 which requires host providers and Internet access providers to preserve identification data for connections to their services, and article L.34-1 of the post and electronic communications code (CPCE) which imposes an obligation to preserve this data)

► provisions relating to respect for private life, public order, professional secrecy.
► provisions relating to the protection of the Scientific and Technical Potential of the Nation.

Some of these provisions are subject to criminal sanctions.