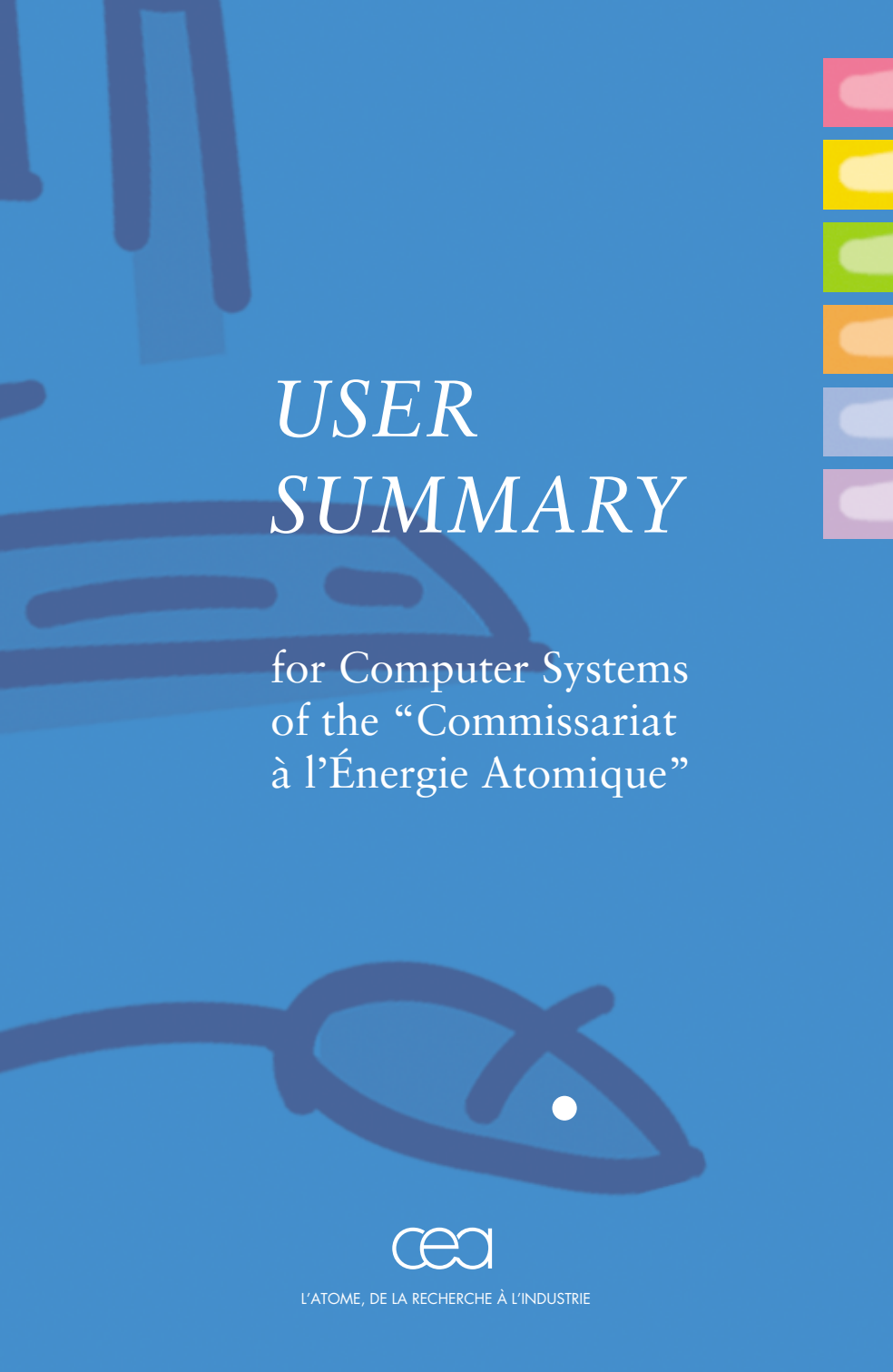
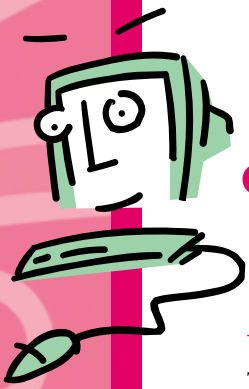


USER SUMMARY

for Computer Systems of the "Commissariat à l'Énergie Atomique"

L'ATOME, DE LA RECHERCHE À L'INDUSTRIE



Field of Application

These notes outline the rules concerning the use of the computer systems of the "Commissariat à l'Énergie Atomique" as defined in "Note d'Instruction Générale n°469 : Utilisation des moyens informatiques du CEA".

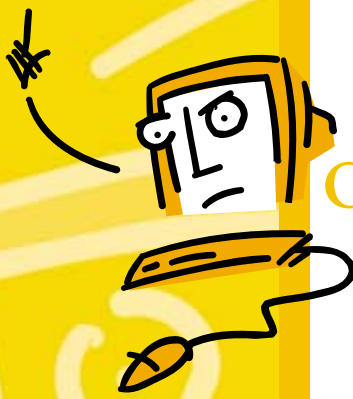
Computer Systems Concerned

This relates to all computerised systems that form part of the CEA information system (local systems and resources which may be remotely accessed from the network administrated under the responsibility of the CEA units), and which are destined to create, process, store, exchange or destroy informations.

The information concerns all of the CEA's fields of activity : scientific, technical, administrative, management, office, etc..

Users Concerned

The NIG provisions are applicable to any person, whatever his or her status, having access to the computerised systems as defined above : CEA employee, temporary personnel, short or long-term trainee, student, researcher from an associated laboratory, personnel from an external company and employees of subsidiaries under the conditions defined by agreement and in general, all other personnel authorised to use these computerised systems.



General Organisation and Responsabilities

The security of the information systems is the responsibility of qualified authority and hierarchical authority.

The Directeur Central de la Sécurité (Central Security Director), as the qualified authority, is responsible for the security of the CEA information systems. In this respect, he defines the security policy for these systems, fixes the security objectives and ensures their control.

The operational directors, both pole and central, as well as department heads, as hierarchical authorities, are responsible for the definition of the security objectives for their information system as well as for the application of the appropriate measures. To do this, they are assisted by the Agent de Sécurité des Systèmes d'Information (Information Systems Security Agent) (ASSI) and by the Correspondant de l'Agent Central de la Sécurité (Central Security Agent's Correspondent) (CACS).

The definition and implementation of the technical and organisational means to guarantee security of the information systems are the responsibility of the Direction des Technologies de l'Information (Information Technology Department), following validation by the Direction Centrale de la Sécurité (Central Security Department).

Regulations for Use and Security

The use of the CEA network and computer systems is carried out within the framework of the missions entrusted to the unit holder of these systems and according to the needs of this unit. Availability of computer equipment or resources (service, electronic mail, remote access, disk space, printer, …) to a user is made under the responsibility of the unit, in accordance with the regulation procedures and the methods laid down by the unit.
The use of these systems ceases when the mission is completed or when the need disappears. The hardware systems are then returned to the unit concerned; they must be subject to a physical follow-up check and, if necessary, subject to the scrapping procedure as defined in the CEA property management Code.

- **Access right**
- **Responsibility**
- **Password**

The user must contribute towards the general security of the CEA, notably by observing the specified rules and recommendations.

The right of use is granted by the unit manager; it is strictly personal and under no circumstances is it transferable to colleagues or a third party, even temporarily.

The right of use is materialized by a precisely defined right of access either to an individual or shared work station (PC, workstation, …) or to network resources (user accounts on remote equipment, …) or to both.

The use of computer equipment or an account is placed under the entire responsibility of the person using it, within the framework of his (her) access rights. As a consequence it is his (her) responsibility to maintain the protection of the equipment and software resources entrusted to him. Access to the machine must as a minimum requirement be protected by a password. Removable information supports (software or data) of any nature must be managed and placed in a safe place in relation to the sensitivity of the information it contains and in accordance with the regulations in force.

Passwords giving access to computer equipment or to accounts must be chosen very carefully. They must be made up of at least 8 characters comprising a mixture of upper and lower case letters, numbers and special characters. They must be changed periodically and never communicated to anyone or left accessible in close proximity of the workstation.

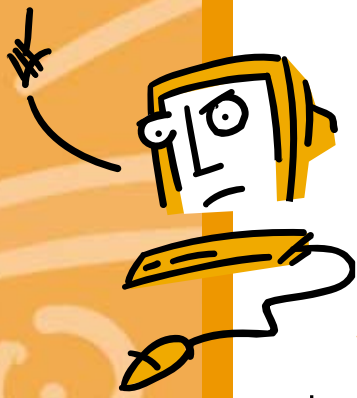
A user who, due to the requirements of the department, shares resources for which he (she) is the owner (files, programs, directories …), **must limit the access rights given to the third party concerned to the strict minimum necessary**. These latter persons are responsible for the data-processing that they carry out on these resources as indicated below.

The user disconnects by leaving his (her) workstation, so as to leave no information accessible.

Anomalies or any problem encountered (theft of equipment or accessories, attempted intrusion, suspicion of a virus, …) must be communicated to the system manager or administrator as soon as possible, to the head of the unit and to the Agent de Sécurité des Systèmes d'Information (Information Systems Security Agent) (ASSI), with whom an appropriate solution will be validated.

Under these circumstances, the ASSI may have cause to work on the computer of the user who will be kept informed, prior to and where possible, of the operations performed.

The user must notify the system manager or administrator of any change in his (her) requirements, especially the resources he (she) no longer needs with regard to his (her) functions or upon his (her) departure from the holding unit.



Principles of Use

- Right of use
- Nominative information files
- Electronic mail
- Internet services
- Viruses

Respecting Confidentiality

Confidentiality relates to information whose access is limited only to those persons permitted to know it for requirements of the service.

User files are restricted to their own use (even if they contain certain possibilities of use by third parties).

As a consequence, **it is forbidden to misappropriate or to attempt to misappropriate the user rights and the access to the accounts of a third party by whatever means,** such as intercepting a password or wrongfully assuming an identity. **This prohibition is also valid for the use of electronic mail.** Access to a workstation belonging to another user is only authorised following agreement of the latter. This use cannot in any case be made under the identity of the user having given the access.

It is recalled that it is a punishable offence to access or fraudulently remain within all or part of a computer system, even if no erasure or modification of data nor any tampering with the operation of the system occurred.

If the activity performed by the user requires the creation or modification of files containing nominative information, the Commission National de l'Informatique et des Libertés (National Commission for Computers and Liberties) (CNIL) must be contacted first by means of an advice note or for the most current processes a simplified declaration. A declaration must also be made when these files are destroyed. The only body within the CEA accredited to carry out these formalities with the CNIL is the Direction Juridique et des relations Commerciales (Legal and Commercial Relations Department) (DJC). The " Computer Information and Liberties " guide issued by the DJC outlines the measures applicable, the creation and processing methods for computer files, as well as the rights held by the persons concerned by these files.

It is recalled that confidentiality is not guaranteed by the electronic mail system. As a result, this must not be used without the appropriate security for the exchange of information or documents of a confidential or sensitive nature, even with regard to draft documents.

Each user who issues or transfers messages exchanged by electronic mail, even partially, is entirely responsible for the respect of the confidentiality attached to it.

Preservation of Availability and Integrity

By availability is understood the aptitude of the information system to fulfil a function relating to the expected objective, under the conditions defined by schedules, time scales and performance.

The use of a unit's computer systems, outside of the field of activity of this unit, notably the opening of personal services or any profit or gaming activity, **is forbidden.**

This prohibition is also valid for the use of Internet and electronic mail services, that must be limited to business requirements, and which especially are not destined for exchange, within the organisation, of information of a social, political, confessional or trade union nature excluding exercising the trade union rights as defined in the collective agreements of the CEA. A reasonable amount of personal use of these systems is permitted insofar as the business activity is not affected in any way.

The sending of " chain " mail messages to lists of persons or individuals as well as sending messages that may cause saturation of the networks or damage the work of a third party is strictly forbidden.

By integrity is understood the guarantee that the system and the information are only modified by a single voluntary and legitimate action : when the information is exchanged, the integrity is extended to authentication of the message, that is, the guarantee of its origin and its destination.

The voluntary spread of viruses, the development and use of software to avoid the security devices in place within the systems as well as the diversion of system use tools for acts of piracy constitute an offence liable for penal or professional punishment.

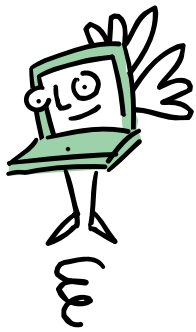
It is recalled that the following are punishable offences :

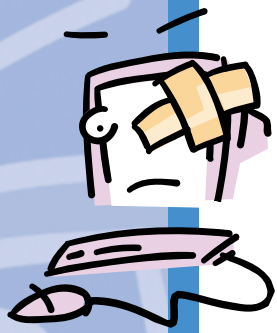
- interfering with or falsifying the operation of a computer system ;
- fraudulently entering data into a computer system or fraudulently modifying the data that it contains.

Users must be aware that exchanges of electronic mail are not anonymous and, especially, that they involve the use of an address indicating that the user is part of the CEA. Positions taken must conform to the interests of the CEA.

Access to common resources must be made with a constant concern for non-abusive use and equal sharing. In particular, the user must ensure that as little disk space as possible is occupied, to disengage from software with " token licence " when no longer in use and not to monopolise dedicated workstations.

Any modification to a workstation's hardware or network equipment may only be carried out by suitably qualified skilled personnel following written agreement from the system manager or administrator.





Protection of Estate

- Information management
- Encryption
- Software and information use
- Network connections

It is recalled that information relating to the defense classification must not be processed on systems connected to non-approved networks, notably the civil CEA connected computer networks.

Divulgence of processed information may compromise the CEA estate. As a consequence, the user is committed to not making information available to a third party without first checking to ensure that he (she) is authorised to do it. He (she) must check that the means of protection are adapted to the level of sensitivity of the information and that the distribution is indeed limited to the scheduled and authorised addressees.

The user must not respond to external requests aimed at obtaining information that might be requested (via computer means, human contact, lists, ...) whatever the form (telephone canvassing, electronic mail, questionnaires, enquiries, ...).

It is recalled that the use of coding for confidentiality means may only be done following agreement from

the Direction Centrale de la Sécurité (Central Security Department) and in accordance with the regulations in force.

The user must not seek to obtain nor to use information or software for which he (she) does not use within the framework of his (her) mission or for which he (she) does not have the rights of use. In particular, it is forbidden to use and even to install protected software onto a workstation (for which a licence must be acquired) that could come from illicit copies or acts of piracy, including for temporary use or to test them.

Each user is committed to not introducing potential security risks into the CEA networks.

He (she) must observe the internal regulations governing access to these networks. In particular, any new special access (RTC, RNIS, TRANSPAC, ...) must be declared and submitted for authorisation from the Direction des Technologies de l'Information (Information Technology Department) of the CEA. It is essential that solutions involving access devices to public networks must use procedures that allow identification of the caller (automatic redial, connections to security servers, ...). When access must be made via telephone network to machines connected to the CEA computer networks, only the use of a centralised means of access managed by the Direction des Technologies de l'Information (Information Technology Department) is authorised.

The DCS circular n°15 of 18/10/95 regulates the information services accessible from outside of the CEA. DCS circular n°16 of 10/05/99 regulates the information services with restricted computerised access. These two types of service can only be set up following agreement from the Direction Centrale de la Sécurité (Central Security Department) and the Direction des Technologies de l'Information (Information Technology Department).

Use of the Internet

By Internet is understood the availability via remote servers outside of the CEA, of means of exchange and information.

- **Adherence to Internet rules : Netiquette**

Use of the Internet must be made in accordance with the principles of use as defined previously and by observing the legislation in force. When the user accesses a site outside of the CEA, he (she) must observe the security policy and the local regulations of the host site. From CEA equipment, a connection to sites that contain information liable to be subject to penal proceedings will not be processed.

It is forbidden to distribute confidential information as defined above, as well as to voluntarily tamper with the correct operation of those servers which it is possible to access.

Useful Information

Systems Administrator or Manager

Tel : _____

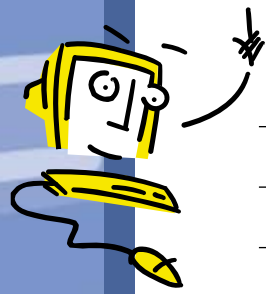
E-mail : _____

Agent de Sécurité des Systèmes d'Information (Information Systems Security Agent) (ASSI)

Tel : _____

E-mail : _____

For more information on Information Systems Security, consult the site http://www-ssi.cea.fr:8000/



Notes

Graphic design Angel'Art : 01 48 05 48 04

DIRECTION CENTRALE DE LA SÉCURITÉ
SERVICE DE PROTECTION DES ACTIVITÉS CLASSÉES ET DES INFORMATIONS
CEA/FAR - ROUTE DU PANORAMA - BP6 - 92265 FONTENAY-AUX-ROSES CEDEX
TEL : 01 46 54 97 35 - FAX : 01 46 54 97 37

Publishing september 2001