CNRS UMR 8507 – CentraleSupélec –
Université Paris Saclay – Sorbonne Université

Site de Gif Sur Yvette 3/11 rue Joliot Curie
91192 GIF SUR YVETTE
Tel : +(33) 01 69 85 16 33
Site de Paris 4 place Jussieu
75252 Paris cedex 05
Tel : +(33) 01 44 27 43 27
direction@geeps.centralesupelec.fr
https://www.geeps.centralesupelec.fr

ORGANIZATION OF COMPUTER SECURITY AT GEEPS

IT CHARTER

The newcomer must sign a **Computer Charter**. This charter defines the rules for the use of the computer resources of the Paris Electrical and Electronic Engineering Laboratory (GeePs), in compliance with the legislation in force and the deontological charter of the National Telecommunications Network for Technology, Education and Research (RENATER), in order to allow the normal functioning of the underlying information systems. It also describes the applicable sanctions in case of non-respect of these rules and reminds the main reference texts.

GeePs is defined as the following entity.

The IS is the GeePs IT Department composed of Olivier Hubert, Anthony Guindon and Pascal Gomez.

Security Principles

This policy applies to anyone who has access to GeePs computer resources. Failure to comply with this policy will result in the signatory's liability.

Protection of information and electronic documents

All Users are responsible for the use of the computer resources to which they have access. The User shall protect the information he/she is required to handle in the course of his/her duties, according to its sensitivity. When creating a document, the User determines its level of sensitivity and applies the rules to ensure its protection throughout its life cycle (marking, storage, transmission, printing, deletion, etc.). When User's data is not automatically backed up by GeePs, User implements the manual backup system. In order to protect against the risk of theft of sensitive documents, the User, when he/she is away from his/her office, ensures that his/her paper documents, if any, are locked away and that his/her workstation is locked. Access to GeePs' computer resources is subject to authorization and may only be used in connection with the Signatory's professional activity. These resources must be used for projects related to the laboratory's missions.

Protection of resources and access rights to information

The User is responsible for the use of the information systems carried out with his access rights. In this respect, he/she ensures the protection of the authentication means that have been assigned to him/her or that he/she has generated (badges, passwords, private keys, private keys linked to certificates, etc.):

- He/she never communicates them, including to his/her line manager and to the team in charge of his/her Entity's IS;

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

- He/she puts in place all the means at his/her disposal to avoid the disclosure of his/her authentication means;

- He modifies or requests the renewal of his means of authentication as soon as he suspects that they have been disclosed.

The User does not use the means of authentication or access rights of a third party. Similarly, the User does not attempt to conceal his or her own identity. The User only uses his access rights to access information or services necessary for the performance of the tasks entrusted to him and for which he is authorized:

- he/she refrains from accessing or attempting to access information system resources for which he/she has not been explicitly authorized;

- he/she does not connect to the Entity's local networks - regardless of the nature of these networks (wired or wireless) - equipment other than that entrusted or authorized by management or the Entity;

- he/she does not introduce data media (USB key, CDROM, DVD, etc.) without respecting the GeePs rules and takes the necessary precautions to ensure their harmlessness;

- he/she does not install, download or use, on the Entity's equipment or on personal equipment used for professional purposes, software or software packages for which the license fees have not been paid, or which do not come from trustworthy sites, or which are prohibited by the Entity;

- he/she undertakes not to voluntarily disrupt the proper functioning of computer resources and networks, whether by abnormal manipulation of hardware or software.

The User shall inform the administrators of any change in his functions requiring a modification of his access rights.

Protection of computer equipment

The User shall protect the equipment made available to him:

- he/she applies the instructions of the IT team from the Entity's Operational Information System Security Policy in order to ensure that the configuration of his/her equipment follows good security practices (application of security patches, encryption, etc.);

- He/she uses the available means of protection (anti-theft cable, storage in a locked drawer or cabinet, etc.) to ensure the protection of mobile equipment and the information they contain (laptop, USB key, smartphones, tablets, etc.) against theft;

- in case of absence, even momentarily, he/she locks or closes all sessions in progress on his/her workstation;

- they report as soon as possible to the IS security officer any loss, theft or suspected or proven compromise of equipment made available to them.

The Entity informs and assists them in the implementation of their protection measures.

Protection against network exchanges

E-mail address

CentraleSupélec (as well as Sorbonne University, Paris Saclay and the CNRS where applicable) undertakes to provide the User with a nominative professional mailbox enabling him/her to send and receive electronic messages. The use of this nominative address is under the responsibility of the User. The nominative aspect of the e-mail address is simply an extension of the administrative address: it does not in any way remove the professional nature of the e-mail.

Content of exchanges on the networks

Electronic exchanges (mail, discussion forums, instant messaging, social networks, sharing of documents, voice, images, videos, etc.) respect the correctness normally expected in any type of written or oral exchange. The transmission of classified defense data is forbidden unless a specific device is approved and the transmission of sensitive data must be carried out in accordance with the protection rules in force.

Vigilance

The User shall be vigilant with regard to the information received (disinformation, computer viruses, attempted fraud, chains, phishing, etc.).

Status and legal value of information exchanged

Information exchanged electronically with third parties can, in legal terms, form a contract under certain conditions or be used for evidentiary purposes. The User must therefore be careful about the nature of the information exchanged electronically1 in the same way as for traditional mail, storage and archiving of the information exchanged.

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

Protection against access to online services on the Internet

If a residual private use can be tolerated, it is reminded that the connections established thanks to the computer tool provided by GeePs are presumed to have a professional character. The User shall use his professional details, in particular his e-mail address or other identifier, with care. By using them on sites unrelated to his professional activity, he facilitates damage to his reputation and the reputation of the Entity.

Some malicious sites take advantage of browser vulnerabilities to retrieve data from the workstation. Other sites provide software that, under a harmless appearance, can take control of the computer and transmit its contents to the hacker without the User's knowledge. 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, method of downloading, etc.);

- Only back up data, share information, and collaborate with others on trusted sites, provided by the institution and whose security has been verified by the institution (e.g., through a security audit);

- Encrypt non-public data that is stored on third-party sites or transmitted via non-secure messaging systems.

Publishing Information on the Internet

Any publication of information on the Entity's Internet or intranet sites is carried out under the responsibility of a named 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 Entity's information system is authorized.

Privacy and Personal Computer Resources

Residual Privacy

The computer resources (workstations, servers, applications, email, Internet, telephone, etc.) provided to the User by the laboratory are reserved for the exercise of his professional activity.

A personal use of these resources is however tolerated on the condition :

- That it remains of short duration during the working hours at the office;

- That it does not affect the professional use;

- That it does not jeopardize their proper functioning and security;

- That it does not violate the law, regulations and internal provisions.

All data is deemed to be professional except for data explicitly designated by the User as private (e.g. by indicating "private" in the subject field of messages). The User shall store 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 any professional data and it must not be used for any other purpose.

All data is considered professional with the exception of data explicitly designated by the User as private (e.g. by indicating "private" in the subject field of messages). The User shall store 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 any professional data and must not take up an excessive amount of resources. The User is responsible for the protection and regular backup of private data.

Personal computer resources

Personal computing resources (computers, smartphones, tablets, etc. purchased with personal funds), when used to access GeePs IS, must not undermine or weaken the Entities' security policies through inadequate protection or inappropriate use. These resources are tolerated for the time GeePs provides equipment to the User. This use must be exceptional and of short duration provided that GeePs IS has been able to analyze the equipment.

When these personal computer resources are used to access, remotely or from the Entity's local network, or to store professional data, these resources are authorized, secured and declared to the IS that manages the Entity's equipment.

Staff wishing to acquire such equipment should consult their IT department beforehand.

Management of departures

The User is responsible for his private data space and it is his responsibility to destroy it when he leaves. In the event of exceptional circumstances (sudden departure or death), the data will be kept for a maximum period of 3 months (period allowing the User or his beneficiaries to recover the information contained therein). Professional data remains at the disposal of the employer. The measures of conservation of professional data are defined within the Entity.

All computer resources provided by GeePs must be returned by the user to the GeePs IT Department at the end of his/her contract or assignment.

Respect of computer ethics

The user undertakes not to intentionally carry out operations that could, in particular, have the following consequences

- Damage the premises where computer equipment is stored;

- steal or use another user's means of access to GeePs' computer resources;

- to mask one's true identity or to usurp the identity of a third party;

- intercept any communication between third parties;

- accessing, deleting or modifying data of third parties without their authorization;

- to infringe on the privacy of a third party;

- to harm the integrity or sensitivity of a third party, in particular by means of provocative, defamatory, discriminatory, hateful or insulting images or texts;

- to incite the consumption of illicit substances;

- to misuse shared computer resources;

- interrupt or alter the normal operation of the network or any of the systems connected to the network;

- to circumvent the access controls and restrictions put in place on the network or the systems connected to the network;

- to reproduce, represent, distribute a work of the mind (musical extract, literary extract, photograph, ...) in violation of the rights of its author;

- to copy commercial software or to circumvent their protection, in contradiction with the principles of the code of the intellectual property.

If, in the course of his work or missions, the User is required to create files of nominative data that are subject to automated processing, he must, prior to any creation, refer to the Correspondant Informatique et Libertés (CIL) of the establishment in question (CS or SU). (Contact details available from the Entity's IT Department)

Management of networks and computer systems

The user is hereby informed and expressly accepts that the IT Department may carry out checks on the proper use of GeePs' IT resources, which may result in the knowledge of data of a private or confidential nature, in particular connection traces kept for a maximum period of one year.

He/she agrees that the IT Department may take emergency measures, such as limiting or temporarily interrupting the operation of some or all of GeePs' networks and computer systems, in order to preserve security in the event of an incident of which the IT Department has been informed.

However, all of these steps will be accompanied by a dialogue with the users concerned and can only be implemented subject to technical and legal feasibility.

Sanctions

In the event of a breach of the rules set out in this charter, the IT Department reserves the right to immediately and indefinitely remove some or all of the offender's access to GeePs' computer resources. After referring the matter to the competent authorities, the User may be subject to disciplinary and/or criminal proceedings depending on the nature of the breach.

Legal framework

The User is required to comply with all the legal framework related to the use of information systems, as well as any other regulation that may apply. In particular, he/she shall respect:

► the amended law of 29 July 1881 on the freedom of the press. The User does not disseminate information constituting attacks on personality (insult, discrimination, racism, xenophobia, revisionism, defamation, obscenity, harassment or threats) or that may constitute incitement to hatred or violence, or an attack on the image of another person, his or her beliefs or sensibilities ;

► the regulations relating to the processing of personal data (in particular Law No. 78-17 of January 6, 1978, as amended, relating to information technology, files and freedoms);

► the legislation relating to attacks on automated data processing systems (art. L 323-1 et seq. of the penal code);

► the law n° 94-665 of August 4, 1994, as amended, concerning the use of the French language;

►the law n° 2004-575 of 21 June 2004 for confidence in the digital economy;

►the provisions of the artistic intellectual property code. The User does not make illicit copies of elements (software, images, texts, music, sounds, etc.) protected by intellectual property laws;

►the provisions relating to respect for privacy, public order, 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.

Modification of the charter

The User is informed that this charter may be modified at any time. The modifications made will be notified to him by e-mail.

CNRS UMR 8507 – CentraleSupélec –
Université Paris Saclay – Sorbonne Université

Site de Gif Sur Yvette 3/11 rue Joliot Curie
91192 GIF SUR YVETTE
Tel : +(33) 01 69 85 16 33
Site de Paris 4 place Jussieu
75252 Paris cedex 05
Tel : +(33) 01 44 27 43 27
direction@geeps.centralesupelec.fr
https://www.geeps.centralesupelec.fr

Box to be signed by the newcomer

And to be given to the IT Service Manager during the interview.

Name : ……

Surname : ……

Date of birth : ……..

Personnel email : ……

Phone : ……..

Status : Permanent ❑ Doctoral Student❑ Post Doc❑ CDD❑ Intern❑ Guest❑ Other❑

Pole :……

Responsible :……..

Period for non permanent :……to ……

Building :……

Gif sur Yvette, le

I agree to have read the computer charter and to respect the conditions of use of the equipment entrusted to me.

Signature of the person concerned Signature of the IT manager