INFORMATION TECHNOLOGY POLICY

Use of Information Technology Resources and Internet services

To meet service needs, IT resources in TAAF districts and their supply ships were developed thanks to substantial investment programs. Financial operation and maintenance costs must thus be respected.

This text is a code of best practices—it specifies user responsibilities in the framework of current regulations. It aims to establish a correct use of IT resources and Internet services while respecting rules of courtesy and mutual respect.

Everyone working for TAAF administration must respect this code during their stay in a district or on board the ship Marion Dufresne, whatever their contract or whoever their employer might be.

All users must sign this code that engages their responsibility in case the stated procedures should be flawed.

1. Definitions

The following definitions are used within the present code:

- “Employer”: Organism that the personnel using IT resources and Internet services depends on (IPEV, TAAF, PNRA, CNRS, Universities, etc.). When the employer isn’t TAAF, one must read “employer and TAAF” in any article mentioning authorizations and/or information to transmit.

- “ISP” (Internet service provider): Organism that provides IT resources and on-site means of communication:

  - AMSTERDAM: TAAF/IPEV
  - CROZET: TAAF/IPEV
  - KERGUELEN: TAAF/IPEV
  - DUMONT D’URVILLE: TAAF/IPEV
  - MARION DUFRESNE: TAAF/IPEV
  - ASTROLABE: TAAF/IPEV

- “IT resources”: local computation and management tools that can be remotely accessed either directly or through the ISP's cascade network. All private means, as soon as they are connected to the network, are also concerned.

- “Internet services”: the provision by local or remote servers of sundry exchange and information resources: web, messaging services, chat rooms and forums, etc.

- “User”: any person hosted in a district or on board a ship that can access or use IT resources and Internet services.

- “Network manager”: person responsible for district servers and TAAF information system services (except for Astrolabe ship).

- “Remote site”: TAAF districts or supply ships.

- “Supply ship”: Marion Dufresne

2. Access to IT resources and Internet services

Use of IT resources, Internet services and their access network are strictly reserved to users’ professional activities, in compliance with current regulations (see art. 10) and the provisions of the present code.

Furthermore, the network manager must authorize the use of shared IT resources and the connection of equipment to the network by allocating a user name and password to each user. These authorizations are strictly personal and can by no means be lent, even temporarily, to a third party. They can be taken away at any given moment. All authorizations end at the same time as the professional activities (even if temporary) that justified them.

3. Rules for use, security and best practices

All users are responsible for the use of allotted or shared IT resources and networks they have access to. Furthermore, they are also in charge of contributing, insofar as possible, to general security as well as ISP security.

Use of these resources must be rational and honest in order to avoid saturation or misuse for personal purposes.

In particular, users:

- must protect their information and data by using personal or supplied back-up tools;
- are responsible for the rights they give other users;
- must report any attempted violation of their accounts, and, more generally, any anomaly they may notice;
- must respect the current regulations of the remote site they are in to install software;
- choose safe passwords, keep them a secret and never, under any circumstance, communicate them to third parties;

- commit not to allow unauthorized users to access the systems or networks with their equipment;
- must not use or try to use accounts other than their own, or conceal their real identity;
- must not try to read, modify, copy or delete data that do not directly or indirectly personally belong to them;
- must always log out when they leave their computer or self-service computers to avoid leaving easy access to resources or services;
- must not do anything that might directly or indirectly lead to physical deterioration of IT resources;
- must return all entrusted IT resources when their work ends, or, in any case, at the end of their stay.

4. Terms of Privacy

User access to information and documents kept on IT systems must be limited to their own, or the ones that are public and shared. It is particularly forbidden to look into other users' data, even if they haven't protected them explicitly.

This rule also applies to private conversations, such as emails, that aren't addressed to the user.

TAAF's IT manager and the person in charge of IT and telecom resources in remote sites are linked with a code of ethics and commit to respect the privacy of all data or information that aren't addressed to them and that they may have accessed while doing their job.

Likewise, users commit not to transmit any information likely to harm the logical security of TAAF's IT sites.

5. Respect of regulations regarding software

Intellectual property, as well as commitments taken by employers who have provided commercial software to one or more users in the framework of license agreements, must be respected when using software.

Subject to exemptions provided in the license agreement:

- Copying software, other than back-up copies, is forbidden;
- Installing software on machines belonging to the employer must be authorized beforehand by the person empowered to do so by the employer;
- Software operating licenses are granted for a specific machine or a limited number of machines; flawing this provision constitutes a forgery that is subject to criminal and civil penalties. Prime Minister's memorandum of 17 October 1990 draws the attention

of agents and services on the characteristics of criminal convictions in French law, namely that the author of a forgery will alone be convicted, even if he or she didn't act in his or her personal interest;

- Modifying software developed by an employer can only be done with prior authorization by the employer;
- Installing free software must be authorized by the employer.

When the concerned IT resource is connected to the network, this authorization must be backed up by prior consent from TAAF's ISS manager.

6. Use of Internet services (web, messaging services, forums, etc.)

6.1. Professional use

When using Internet services, users must respect the general principles and specific rules of each site, the provisions of the present code, and current regulations (see article 10).

Based on the founding principles of article 1384, paragraph 5 of the French Civil code, it is reminded that employers are, as principals, civilly responsible for their employees and for the faults they might perpetrate when using the Internet in their worksite. In this capacity, it is reminded to all users who use IT resources provided by their employers that they:

- must not connect or try to connect to a server by other means than those intended by it, or without being authorized to do so by the people in charge;
- must be extremely polite to their interlocutors in all their exchanges, whether they be emails, forums, etc.;
- must not state personal opinions that aren't related to their professional activity and may likely prejudice their employers and the ISPs;
- must comply with the law, especially with regard to defamatory statements, or offensive, racist or pornographic language.

If users must create files for their work that are subject to the provisions of the French Information Technologies and Freedom law, they must first ask the French National Commission for Information Technologies and Freedom (CNIL), via their managers and employers, according to the type of contract, and receive a due authorization. It is reminded that this authorization is valid only for the processing defined in the request and not for the file itself.

All professional downloads are submitted to prior authorization and to a certain time slot given by the concerned site's IT manager.

*6.2. **Personal use***

Given the particular situation of distant sites and conditions of stay, the use of IT resources and Internet services is authorized for personal messaging services.

Communicating information via blogs, websites, etc. about activities carried out in a remote site or about living there, whatever the transmission media might be (messaging service, internet connection), is **tolerated** as long as it strictly respects the provisions exposed in paragraph 6.1.

It is reminded that personnel sent to a Subantarctic or Antarctic polar base camp and on board a supply ship represents its employing organism. In this capacity, it is specified that:

- Publishing information or documents produced with the employer's IT resources is submitted to prior authorization by the organism the author works for. The authorization request must specify the type of publication (blog, website, electronic press article, etc.) and how it will be updated (directly or via emails to a third party);
- Creating a blog or website must be declared beforehand to the ISP and the employer. The following information must be specified:
    - Name of the author
    - Type of publication (open blog, closed blog, website, etc.)
    - Target readers
    - Planned update procedure
- Authors commit not to prejudice any involved organisms through their publications;
- Authors must expose the framework of their missions in a visible manner and insert links towards all the involved organisms' official websites;
- If deemed necessary, employers can ask an author to change the contents concerning them if they feel the form and/or substance harm their image and/or the mission that was entrusted to the author.

In any case, accessing the Internet for personal reasons is submitted to prior authorization and to a certain time slot given by the IT manager of the concerned site.

7. Intellectual property

As far as copying and broadcasting movies or music in public are concerned, it is reminded that it is illegal to put movies or music on a server and that can be downloaded on any computer connected to the network.

The French Intellectual property code specifies that: "Any edition of writings, musical compositions, drawings, paintings or other printed or engraved production made in whole or

in part regardless of the laws and regulations governing the ownership of authors shall constitute an infringement. Any infringement shall constitute an offence."; "Any reproduction, performance or dissemination of a work of the mind, by any means whatsoever, in violation of the author's rights as defined and regulated by law shall also constitute an infringement."

Downloading any piece of work concerned by this article is strictly forbidden.

8. Analysis of and control over the use of IT resources

For maintenance and technical management needs, the use of material or software resources, as well as the exchanges via the network, may be analyzed and controlled in the respect of the current regulation, especially the French Information Technologies and Freedom law.

9. Antivirus software (except for Adelie Land)

All the computers in base camp must be protected by antivirus software whose definitions are kept up to date (less than a week). Antivirus software and their definitions must be provided by the employer.

Personnel must use the dedicated server, called white-listing server, to test all removable devices and media.

Removable devices and media must absolutely be tested on the white-listing server upon arrival at the district and before using it on IT resources.

10. Reminder of TAAF's main legal provisions

Everyone in remote sites must respect TAAF current regulations, especially in the field of IT security:

- Information Technologies and Freedom law of 6 January 1978 (www.cnil.fr),
- Regulations regarding information technology fraud (articles 323-1 to 323-7 of the French Criminal code), (http://www.jurizine.net/index.php/2005/09/04/42-articles-323-1-a-323-7-du-codepenal-fraudes-informatiques)
- Provisions of the intellectual property code practicable to TAAF (articles L811-1 et seq. and R811-1 et seq.), (http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414&dateTexte=20090907)
- law of 4 August 1994 relating to the use of the French language, (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005616341&dateTexte=20090907)
- Prime Minister's memorandum of 17 October 1990, (http://www.dsi.cnrs.fr/rmlr/textesintegraux/volume4/416-cirdu17-10-1990.htm)

- Practicable regulations relating to encryption, (http://www.ssi.gouv.fr/archive/fr/reglementation/regl.html#crypto)

11. Application

The present code is practicable to all the people accommodated in remote sites, whether they be permanent, temporary or external, who use IT resources that can be remotely accessed either directly or through the IT manager and the ISP's cascade network.

It must be signed by all the people staying in a remote site and that may have access to an IT system connected to an IT network.

(All pages must be initialed)

Done at:..…… on…….

Last name:…… First name:…….

Status:……...

Place of assignment:……

Assignment dates (DD/MM/YY):……..

I certify to have read the present information technology code of best practices.

Signature: