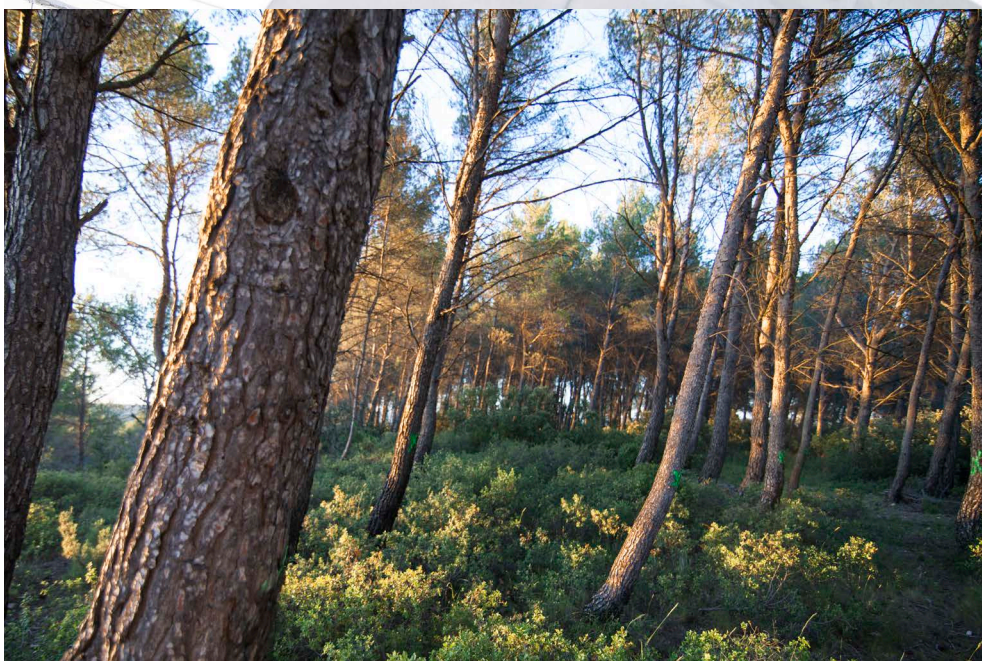

Memorandum dated 16/10/2017
Use of thecamp's IT resources

thecamp has put in place an information technology and communications system required for its operations. Consequently, it makes IT and communication tools available to its co-workers.

This memorandum sets out the conditions for accessing and rules for the IT resources plus the outside resources accessed via thecamp's communications tools. It also aims to make users aware of the risks related to the use of these resources in terms of integrity and privacy of the data processed. These risks require that certain security and good practice rules be complied with. A user's carelessness, negligence or malevolence may have serious consequences for which he or she, together with thecamp, may be held civilly or criminally liable.

PROTECTION OF PERSONAL DATA

The French Data Protection Act no.78-17 dated 6th January 1978, amended in 2004, sets out the terms under which personal data may be processed. It gives the person whose personal data has been recorded the right to access it and have it changed.

The list of all the personal data processing tasks carried out by thecamp can be found in the secured IT tools such as the CRM / Active directory / PMS / ...

thecamp ensures individuals' rights (to access, change and oppose) are upheld. In the event of any problems related to exercising these rights, the person concerned are invited to raise the matter with the IT Manager or thecamp management.

SCOPE OF APPLICATION

This memorandum applies to all persons using the information technology and communications system in a professional capacity. Private use of these tools is tolerated but such use must remain reasonable and not disrupt the service's good functioning.

The information is distributed to all users by way of a memorandum and, as such, made available on thecamp's Dropbox account («Dossier de l'équipe – thecamp» folder). It is systematically handed to each newcomer.

A few definitions:

The term «user» means any person authorized to access and use thecamp's IT and communications tools: employees, interns, service provider personnel, visitors...

The terms «IT and communication tools» cover all IT, communications and duplication equipment at thecamp.

RULES FOR USING THECAMP'S IT SYSTEM

Each user accesses the IT tools required for his or her professional use per the conditions set out by thecamp.

1. Work of the internal IT department

The internal IT department ensures the proper functioning and security of thecamp's networks and IT and communications resources. The department's staff have technical means at their disposal to check and control the use of the IT systems put in place.
They have access to all the technical data but undertake to uphold privacy rules relating to the contents of documents.
They have a duty to preserve the confidential nature of data they may come to be apprised of as part of their work.

2. Authentication

Access to IT resources is dependent upon the use of an account name (login id) provided to the user upon his or her arrival at thecamp. This login id is associated with a password used for connection.

The authentication methods are personal and confidential.

At present, the password must comprise a minimum of 7 characters combining numbers, letters and special characters. It may not include the family name or first name or the login id used to open the work session. It is recommended to change the password regularly (e.g. every 3 months).

3. Rules regarding security

Each user undertakes to comply with the following rules on security:
- notify thecamp's internal IT department of any suspected breach or attempted breach of his or her network account and, generally, of any malfunction;
- never divulge his or her login id or password to another person;
- never ask a colleague or co-worker for his or her login id or password;
- never hide his or her true identity;

- never assume the identity of another person;
- never change the workstation's sharing settings;
- lock his or her computer when leaving the work station;
- never access or attempt to access, delete or modify any data that does not belong to him or her;
- any copying to an external medium requires the authorization of a department superior and must comply with the rules set out by thecamp.

It is also reminded that visitors may not access thecamp's non-public IT system without the internal IT department's prior authorization.

External contractors undertake to ensure their employees' compliance with this memorandum and the compliance of those of any sub-contractors. Consequently, contracts signed between thecamp and any third party that has access to the data, IT programmes or any other resources must contain a clause stipulating this requirement.

IT RESOURCES

1. Workstation configuration

thecamp provides each user with a workstation equipped with the IT tools required to carry out his or her tasks. The user must not:

- Interfere with the IT and communications tools' functioning.

2. Mobile equipment and specific procedures for loaned equipment

Mobile devices

The term «mobile equipment» covers all mobile technical resources (laptop computers, portable printers, mobile cellular phones or smart phones, CD-ROM drives, USB «thumb» drives etc...).

Whenever technically feasible, and given the sensitive nature of the documents they may store, specific security measures must be applied to these devices, notably encryption.

The use of smart phones or Blackberry phones to access electronic mail presents specific risks with regard to protecting message confidentiality, especially in the event the device is lost or stolen. Therefore, devices must be adequately configured in such a way as to lock after a few minutes idle in order to prevent any unauthorized access to the data they contain.

Specific procedures for loaned equipment

The user ensures the good safekeeping of, and assumes responsibility for, any equipment loaned to him or her and undertakes to notify the IT department of any incident (loss, theft, damage) in order to initiate the relevant procedures such as the reporting of the loss or theft or making a complaint. The user ensures the security of the equipment given into his or her possession and shall not circumvent the security policy implemented on same.

3. internet

Users may visit Internet sites of whatever nature that are directly relevant to and necessary for their professional work.

However, occasional and reasonable personal access to Internet sites that are not prohibited under law or present a risk for public order and do not affect the interests or reputation of the institution is allowed.

4. Electronic messaging system

Terms of use

The electronic messaging system put at users' disposal is for professional use only. Personal use of the messaging system is tolerated if such use does not impact the user's work or the security of thecamp's IT system.

Any message that is expressly marked as being personal or is clearly personal in nature will be covered by privacy and correspondence confidentiality rights. Otherwise, the message will be deemed professional in nature.

thecamp undertakes to refrain from accessing folders and messages identified as «personal» in the subject line in the user's mailbox.

Use of the electronic messaging system must comply with the terms of use set out by the internal IT department concerning:
- the volume of mail;
- the maximum size of individual sent and received messages;
- the number of simultaneous addressees a sent message may have;
- message archive management.

Transferring professional messages, including any attachments, to personal mailboxes is covered by the same rules as for copying data to external media.

Users may consult their mailboxes remotely using a web browser (webmail). Any files copied onto the computer being used by the user in the process must be deleted from that computer at the earliest opportunity.

Consulting mailboxes

In a user's absence, and in order not to interrupt the service's proper functioning, the internal IT department may from time to time forward an electronic message with an exclusively professional nature and a subject and/or sender's name identifying it as being exclusively professional to a superior (see terms of use).

The superior does not have access to the user's other messages. The user is provided with the list of messages transferred at the earliest opportunity.
In the event of the user's prolonged absence (long-term illness), the department head, subject to management approval, may ask the IT department to transfer received messages.

Courriel non sollicité

thecamp dispose d'un outil permettant pour lutter contre la propagation des messages non désirés (spam).

Unsolicited e-mail

thecamp provides users with landline and mobile cellular phones for their use in a professional capacity.

The private use of telephones is allowed as long as such use remains reasonable.

thecamp undertakes not to individually monitor the use of telecommunications services. Only global statistics on incoming and outgoing calls are compiled to ensure capacity limits under the contracts signed with operators is not exceeded.

thecamp undertakes not to access the full numbers called via the automatic switchboard and via the mobile phones. Nevertheless, in the event of any clearly abnormal use, and on the request of the General Management, the IT department reserves the right to access the full numbers on the individual records.

IT SYSTEM ADMINISTRATION

Various measures have been put in place to monitor operation of thecamp's IT system's and ensure its security.

1. Automatic filtering

As a preventative measure, automatic filtering is used to reduce thecamp's data flow and ensure its data security and privacy. These filters cover, among other things, Internet sites, unsolicited e-mail and the blocking of certain protocols.

2. Automatic tracing

The IT department at thecamp carries out, unannounced, any investigation required to resolve malfunctions in the IT system or any of its components that may threaten its operation or integrity.

To this end, it makes use of log files that record all connections or attempted connections to the IT system. These files contain the following information: dates, workstation names, IP addresses, login names and event identifiers.
The IT department is the sole user of this information, which is deleted after a period of three months.

3. workstation management

For IT maintenance purposes, thecamp's internal IT department may remotely access all workstations. Such access is subject to the user's express authorization.

For IT system updates and upgrades, and if no users are logged in to their workstations, the IT department may need to carry out work on the workstations' technical environment. However, it undertakes not to access their contents.

PROCEDURE APPLIED WHEN A USER LEAVES

Upon leaving, the user must return any equipment put at his or her disposal to the internal IT department.

The user must first delete all private files and data. Any copying of professional documents must be authorized by the management.

Either way, the user's personal data is deleted one month latest after his or her leaving date.

LIABILITY- SANCTIONS

Failure to comply with the rules and security and privacy measures set out in this memorandum may engage the user's liability and lead to sanctions being taken against him or her.

Internal sanctions may be decided, viz:

- In the first instance, and after consultation with the CIO, a reprimand from the internal IT department in the case of non-compliance with the rules set out in the memorandum;
- in the second instance, after consultation with the General Management and the user's superior, appropriate disciplinary measures in the event of a repeat occurrence.

Non-compliance with the relevant legal provisions regarding the security of information systems (see list in appendix) may lead to criminal proceedings as provided for by law.

Drawn up in _____ on _____

APPENDIX

RELEVANT LEGAL PROVISIONS

Directive 95/46/EC dated 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

French Data Protection Act no.78-17 dated 6th January, 1978, amended by Act no.2004-801 dated 6th August, 2004.

Penal provisions:
- Penal Code (legislative section): Art. 226-16 to 226-24
- Penal Code (regulatory section): Art. R. 625-10 to R. 625-13

Act no.88-19 dated 5th January, 1988 on computer fraud, or Godfrain Act.
Penal provisions: Art 323-1 to 323-3 of the Penal Code.

Act no.2004-575 dated 21st June, 2004 regarding trust in the digital economy (LCEN)

Act no.94-361 dated 10th May, 1994 on intellectual property for software.
Penal provision: Art. L.335-2 of the Penal Code.

thecamp