Charter regulating the use of information system resources of the University of Orléans

Glossary

Acronyms

DPO	Data Protection Officer
ISSM	Information Systems Security Manager
IS	Information System

Definitions

Academic activity	The academic activity is that which ensues from academic missions defined by the law, namely: activities for research teaching, for technical development, for technologies transfer, for publishing of scientific, technical or cultural information, for experimentation of new services featuring technical innovation, but also every administrative and management activity which ensues from its activities.
Malicious code or malware	Developed code or program to harm information system resources. Virus, worms, Trojan horses or logic bombs are examples of *codes or malware*.
Personal data	Data which allows individuals to be identified directly or indirectly. It can be information not necessarily associated with the name of a person but which allows her to be identifies and to know the habits and tastes of the person. Examples: name, place of residence, profession, biometrical elements.
Entity	Existing entity within the University, its components, joint services and central services for the accomplishment of its missions. Examples: laboratories, education departments or sectors, administrative or technical services.
Messaging service	The messaging service includes systems of email, of instant messaging and text messaging (SMS).
Legally liable person	Any person who can represent the University (President, vice-president, director, etc.).
Information Systems Security Manager	He is entrusted with his assistant to provide a secure information system for the University.
User responsibility	The person responsible for users is: - For tenured staff or non-tenured staff members who have to carry out missions involving the administration of education and interns: the supervisor ; - For teachers, researchers and teachers-researchers: the director of the faculty or the research unit ;

	- For students: the lecturer ; - For providers: the manager of the service contract within the university.
Information System Resources	All technical, applicational, organizational, human and documentary resources which allow to collect, to store, to process, to search for and/or to transmit data, especially : - All fixed hardware : computing stations (including self-service stations), servers, phones, peripheral devices (keyboard, screen, printer, etc.), plugs, cables, … - All mobile hardware : computers, phones, etc. - All software or network/computer services: network access, Internet access, messaging service, office equipment, etc. - All data carriers: electronic, paper, etc.
User	Anyone who has access or who uses *information system resources* of the University of Orléans, whatever his status, especially : - For tenured staff or non-tenured staff members who have to carry out missions involving the administration of education ; - All lecturers or researchers who use the resources of the University, including the premises ; - All registered students in the process of registering for the current year, or who was registered at the University ; - All providers under contract with the University ; - All interns who use the resources of the University, including the premises ; - All authorized readers who have access to the library resources ; - Anyone who has an access to a service hosted by the University, including the website ; - Anyone temporary welcomed within the University and so who has access to a computer station of the University and/or to the computer network (lecturer, visiting scholar, etc.).

Article 1 – Presentation

Section 1.1 - Object

This charter defines usage rules and security rules that commit the user and the University to respect.

It aims to define the rights and duties of everyone as part of the use of *information system resources.*

It is associated with charters from different Internet service providers, such as the RENATER charter, with regard to the means of network access.

Section 1.2 – Field of application

The provisions of this charter apply to the University and to all *users*.

Section 1.3 – Commitments of the University

The University makes *users* aware of this charter.

The University implements all the necessary measures to ensure the security of information and the protection of *users*.

The university facilitates the access of users to the resources of the information system. Resources available to them are firstly intended for university use, but the University has to respect the use of the information system in its private capacity, as it is defined in section 2.3.

Section 1.4 – Commitment of the user

The *user* is responsible, in all cases, for the use he makes of *information system resources* of the University of Orléans.

The user commits himself or herself to respecting the provisions of the present charter.

Article 2 – Terms and rules of the use of IS resources

Section 2.1 - Access and use of information system resources

The use of *information system resources* of the University and the connexion of external equipment to the information system require authorization. Every *entity* can provide specific access restrictions to its organisation (access smart card, filtering secure access, etc.), subject to validation.

The *user* is informed that:

- His access codes are a security measure intended to avoid any misuse or malicious use of *information system resources* ;
- His access is defined by the University according to his status ;
- Every *user* can get one or several access codes to the *information system resources*. These access codes can be set up with a unique user name and identifier assigned by the University and with a password chosen by the *user*.

To ensure access security to the *information system resources*, the *user* has:

- To keep his or her access code strictly confidential and not reveal it to anyone else it. The *user* is responsible for the use of his access codes, their voluntary disclosure to anyone else engages his criminal and civil liability ;

  The storage of access codes must be carried out via the the password safe, made available by the University of Orléans ;

- To respect current rules within the University concerning passwords ;
- To respect safety rules and rules for access codes, especially :
  - Do not use access codes of another *user*, nor try to know it ;
  - To refrain from accessing or trying to access to *information system resources* by getting round assigned rights ;
  - Do not directly connect other equipment than that given or authorized by the University to the information system.
- Commits himself or herself not to not voluntarily cause disturbances to the proper functioning of *information system resources*, either by abnormal manipulations of the equipment (for example, to unplug a network cable), or by the introduction of parasite software known as viruses, Trojan horses, logic bombs, network listening software, etc.

To ensure safety of the access of *information system resources*, the University has:
- To make sure resources are only accessible to the empowered people ;
- To delete, to disable or to modify access codes as soon as the situation justifies it: end of the activity of the *user*, non-compliance with the charter, etc.

For remote access to *information system resources*, it is reminded that charters from different Internet service providers, used by the *user,* must be applied.

Section 2.2 – Use of external equipment (computers, mobiles, tablets) to the information system of the university (private or external) in the professional framework

In general, only equipment supplied, configured and managed equipment by the University (or the CNRS in the case of mixed laboratories) is allowed to be connected to the wired network of the university.

However, in case of need, the use of an external equipment in the professional activities framework can be authorized under conditions:

- The user commits to use this equipment only in a professional purpose.
- The user must have received an authorization from the ISSM of the university after a motivated request from the manager of his entity (service/laboratory/component). The ISSM will give on this occasion prerequisites to the use of this equipment.
- The university can’t be held responsible for potential thefts or damage to the equipment and nor in case of losses of personal data.

The authorization for using external equipment in a professional activities framework sends the equipment in IT resources of the university, and as such in the perimeter of the SSI, which means that:

- The owner must allow the IT department to access without restriction his machine, with respect for the right to a private life and for provisions of the French Data Protection Act
- The computer will be subject to the same rules as quipment from IT stock of the University of Orléans. (especially, it will have to own an updated operating system, an updated antivirus software approved by the ISSM, proxy authenticated configured on a browser)

Section 2.3 – Private use of resources

Information system resources are tools made available for a use in the *university activities* framework. The use of these ways can also establish the support of a private communication in the conditions described below.

The residual use of *information system resources* in a private capacity must be non-profit and sensible, both in its frequency as in its duration. In any case, the resulting override must remain negligible in accordance with the overall operating cost.

This use mustn't to harm the quality of the work of the *user*, the time he spends and the good working of the service. All information are known as academic except for data explicitly appointed by the *user* as a part of his/her private life.

The user has to proceed to the storage of his private data in a data space provided titled « PRIVATE » or « PERSO ». He will has to back up his private data regularly.

The *user*, when he leaves the University, is in charge of the destruction of his private data space, because the University can't be in charge of the preservation of this space.

The data is stored in accordance with current regulations.

The use of information systems in a private capacity has to respect current regulations.

Section 2.4 - Use of software, data and applications

The *user* is required to:

- Not consult, possess, broadcast and import child pornography data, incitation to discrimination, to hatred, to violence or racist / discriminatory data ;
- Not download, reproduce, copy, broadcast, change or use software, data bases, web pages, texts, pictures, photographs, sounds, songs, videos or other creations protected by the intellectual property rights, especially copyright or a privacy rights, without obtaining the permission from holders of these rights beforehand ;
- Not consult, broadcast, delete or distort information or data possessed by the University of Orléans or other *users* without their permission, even if they have not explicitly protected it. This rule applies also to private conversations of *messaging service* type for whom the *user* is not the addressee neither directly, nor in copy ;
- Not install, download or use voluntarily on the information system :
    - Software forbidden by the University or software which is non-compliant with the missions of the University, especially game software ;
    - Software or software packages whose licence fees have not been acquitted, or which don't come from trusted sites, or without the permission of the University ;
    - Trial versions or software assessment versions ;
    - *Malicious codes or malware*
- Not uninstall, modify or stop the proper execution of software, applications and utilities installed on his own computer station by the IT department
- Not make copies of software subject to a licence (except for backup copies) or to make this software available to another person by the network ;
- Not get round use restrictions of a permitted software ;
- Inform the *DPO* before any creation of files which contain *private data* or processing on the same data, in accordance with clauses of the French Data Protection Act ;
- Bring any analysis concerning management data (ex : phone number) which would need updating to the attention of the manager of the application ;
- Bring quickly any noted dysfunction of software, application or utilities installed on the computer station by the IT department to the attention of the IT department ;
- Respect the security policy of the application as well as rules and procedures in force at the time of data handling extracted from the information system.

During a change of post or authorization of a *user*, the concerned *user's manager* has to inform the competent department in accordance with the procedure in force.

Section 2.4.1 – Sensitive data

Data is considered as sensitive if its revelation to unauthorized people, its distortion or its unavailability can harm the achievement of the objectives of the University of Orléans. Information of authentication (passwords, certificates, etc.) is considered as sensitive data.

Storage of sensitive data

The hosting of sensitive data of the administration on the national territory is compulsory.

Sensitive data should not be stored on equipment other than that made available by the University for the user.

An encrypted folder, recommended by the university, can be used to secure the storage of sensitive information.

Sensitive data processing

The processing of sensitive information within reception areas is to be avoided. If such processing is strictly necessary, it has to remain punctual and exceptional.

For mobile computer stations which handle sensitive data, a privacy filter should be put on the screen as soon as the computer is used outside the entity (especially in transport).

Sensitive data transmission

Sensitive data must move preferably on the wired network of the University and on RENATER.

In the event that it should move on another network, the access to sensitive data should be made by the VPN of the University of Orléans.

Section 2.5 – Use of Internet

Section 2.5.1 – Internet access

The use of Internet is subject to the legislation in force. For the Internet access from the information system, charters of different Internet access providers apply.

The *user* is informed that, if private residual use can be allowed, Internet connexions established thanks to *information system resources* made available by the University are supposed to be of a university nature. The University, and also the different Internet access providers, can search for established Internet connexions to identify and to control them in accordance with clauses provided by the law.

The University reserves the right to control or to forbid the access to some sites, to proceed to the control a priori or a posteriori of visited sites and corresponding access durations (ex : limitation of the bandwidth towards download sites).

The consultation of a navigation history of a designed user is only by order of a Court of law.

The Internet access is only allowed through plans established by the University. Particular security rules can be specified, if it is necessary, in a user guide established by the *entity*.

The *user* is informed about inherent risks and limits to the use of Internet by training schemes or awareness campaigns.

Section 2.5.2 – Publication on the website of the University

All publications on the website of the University (personal pages of lecturers and researchers) are the responsibility of a designated person. Publications must respect provisions of the hosting charter of the University.

Section 2.5.3 – Download or transfer of files

All downloads or transfers of files, especially audio or pictures, on the Internet have to be done in accordance with intellectual property rights.

The University reserves the right to restrict the download of some files which can be voluminous or present a risk for *information system resources* (virus which can degrade the good working of the IS of the University, *malicious codes or malware*, spyware, etc.).

Section 2.6 - Electronic communication

Section 2.6.1 – Mail address

The University makes available to some *users* a named university mailbox permitting to send and to receive emails. Then, the use of this named address is the responsibility of the *user*.

The named aspect of the electronic address is the simple extension of administrative contact details: it doesn't remove the University nature of the *messaging service*.

An electronic address, functional or organizational, can be made available for a *user* or a group of *users* for the needs of the University. Named address can't be shared between several *users*.

The management of electronic addresses which are equivalent of university mailing lists, referring to a category or a group of *users*, is the responsibility of the University: these lists can't be used without explicit permission. Their creation by a *user* must be approved by his manager before their use.

The *user* is informed that the University can take conservatory measures on *messaging service* accounts when the situation justifies it (example: account blockage in case of suspicion of comprise of principles, of illicit use or against provisions de this charter).

Section 2.6.2 – Emails contents

All messages are known as university (linked with activities of the school) except if they have a special and explicit indication of their private nature or are stored in a private data folder. In this sense, the user can proceed to the storage de his private emails in a provided file titled « PRIVATE » or « PERSO ».

To preserve the proper operation of services, the University reserves the right to set up limitations, whose terms are detailed and brought to the attention of the *user* by the University.

Messages containing illicit contents are forbidden, no matter what the nature. They are particularly contents against freedom of expression or which harms the private life of the others and more generally provisions of article 2.4.

The consultation of emails (not known as private) of a named user by another person is only allowed by requisition of a Court of law or professional purposes linked with continuity of the public service (consultation conditions are described in section 2.7). Consultation is subject to the right of the respect of privacy.

Section 2.6.3 – Emission and receipt of messages

The *user* has to make sure of the identity and the exactness of addresses of message recipients.

He has to make sure that messages sent are only for concerned recipients, themselves in small number, to avoid a mass sending of messages, the unnecessary clogging up of the *messaging service* and a degradation of the service.

Section 2.6.4 – Status and judicial value of messages

On the judicial level, emails exchanged with the others can be contractual, subject to the respect of conditions fixed by articles from 1369-1 to 1369-11 of the civil code.

As a consequence, the *user* has to be vigilant about the nature of emails he exchanges, just like for traditional correspondence.

Section 2.6.5 – Storage and archiving of messages

All *users* must implement means necessary for the preservation of messages which can be essential or simply useful as elements of proof.

Section 2.7 - Continuity of service

To ensure the continuity of service, the staff of the university has to give priority to the deposit of their work files on shared spaces with all the department or the team.

Also, insofar as possible, the staff of the university has to give priority to the use of functional aliases of messaging service (Example: secretariat.service@univ-orleans.fr).

During an organised departure of a member of staff, the manager plans the transfer of personal data of the leaving agent (documents and messaging service), working in tandem with him.

Anyway, data which is not in the « PRIVATE » or « PERSO » folder is considered as data which belongs to the establishment which dispose of it.

In case of absence, the staff of the University are advised to set up an out-of-office message associated to their messaging service. This out-of-service message can point to another person to contact during the absence. If need be to answer the needs of the department, an out-of-office message can be set up by the IT department, at the request of the staff manager, with the agreement of the ISSM.

In case it would be necessary to access personal data of a staff member of the university when he is absent to ensure the continuity of the service, only the President of the University can give his agreement, in respect of the right of privacy and clauses of the French Data Protection Act. So the President will give his agreement to the ISSM and to the manager of the service where he is working, clarifying data that needs to be accessed.

Section 2.8 - Duty of reporting and information

The *user* has to inform his manager or the *ISSM* about any noted anomaly or dysfunction. He also informs his manager of any access possibility to a resource which doesn't correspond to his authorization.

The *user* has to inform his manager and the *ISSM* if he has doubts concerning the possible revelation of sensitive data.

Section 2.9 - Using and control of information system resources

The *user* is informed:

- That to make the corrective, curative or upgrade maintenance, the University reserves the possibility to intervene (remotely if necessary) on *information system resources* ;
- That every action of remote control (mainly on work stations) has to be preceded by an agreement with the *user* ;
- That any information which blocks the system or which creates a technical difficulty to arrive at its recipient, will be isolated and deleted if necessary ;
- That *information system resources* can give rise to a surveillance and a control for statistical purposes, for regulatory or functional traceability, for optimisation, for security or for detection of excesses, in respect of applicable legislation.

The staff who have to carry out control operations of the information systems are subject to professional confidentiality. They can't reveal information they know as part of their profession as soon as this information is covered by the secrecy of correspondence or identified as such, they come under the private life of the *user*.

On the other hand, they have to convey this information if they harm the proper technical working of the applications or their safety, or if they appear in article 40, paragraph 2 of the code of criminal procedure.

Section 2.10 – Traceability

The University has a legal obligation to set up a log file of some uses of *information system resources*, such as Internet access, *messaging service* and exchanged data.

Conditions of collection and use of newspapers are described in the document « Politique de gestion des journaux informatiques à l'Université d'Orléans », appendixed to this charter.

Article 3 – Applicable laws and rules

Section 3.1 - Intellectual property

The University points out that the use of *information system resources* involves the respect of its intellectual property rights and those of its partners and more generally speaking, of every other holder of those rights.

As a consequence, every *user* must:

- use software in subscribed licence conditions ;
- not reproduce, copy, broadcast, modify or use software, databases, webpages, texts, pictures, photographs or other creations protected by copyright or a private right, without obtaining previously the permission of holders of these rights.

Section 3.2 – Data Protection Act

The *user* is informed of the necessity to respect legal clauses concerning automated processing of *personal data*, in accordance with the modified law No. 78-17 of January 6th, 1978 said «Data Protection Act».

Personal data is information which enables, in any form whatsoever, directly or indirectly, the identification of individuals for whom it applies.

All creations of files which comprise this kind of information and processing requests, including when they are the result of crossing or network between pre-existing files, are subject to the preceding formality provided by the French «Data Protection Act».

As a consequence, any *user* who wishes to proceed to such a creation will have to inform previously the *DPO* who will take steps necessary in respect of legal provisions.

Otherwise, in accordance with clauses of this law, every *user* has an access right and a right of rectification related to all data which concerns him, including data which is about the use *information system resources*.

This right is exercised with the *DPO* or the *processing manager* who is also the president of the University of Orléans.

Section 3.3 – Information Systems Security Policy of the State

The *user* and the University have to respect the following legal and regulatory clauses:

- Circular PM No. 5725, signed on July 17th, 2014, focusing on the application of the Information Systems Security Policy of the state (ISSP)

Section 3.4 - Protection of scientific and technical potential of the nation

The *user* and the University have to respect the following legal and regulatory clauses:

- Decree No. 2011-1425 of November 2nd, 2011 applying the article 413-7 of the penal code and related to the protection of science and technical potential of the nation.
- Order of July 3rd, 2012 related to the protection of science and technical potential of the nation.
- Interministerial circular of the application of protection package of the science and technical potential of the nation of November 7th, 2012.

Section 3.5 – Other applicable laws and rules (non-exhaustive list)

The *user* and the University have to respect the following legal and regulatory clauses:

- Law of July 10th, 1991 related to the secret of correspondences carried out by means of telecommunication ;
- Decree No. 2006-358 of March 24th, 2006 related to the preservation of data from electronic communications ;
- Articles L.323-1 and following of the Penal Code, related to infringements of automated data-processing systems ;
- Law No. 2004-575 of June 21st, 2004 for the confidence in digital economy ;
- Law No. 88-19 of January 5th, 1988 related to computer fraud ;
- Article 9 of the Civil Code related to the right of privacy ;
- Articles R226-1 and following, R623-4 and R625-9 of the Penal Code related to infringements of private life ;
- Article 227-23 of the Penal Code, related to criminal sanction for usual consultation (on Internet), recording, broadcasting and possession of images of child pornography ;
- Articles R625-7 and following related to the Penal Code concerning criminal sanction for incitement to discrimination, to hatred or to violence ;
- Articles R624-3 and following of the Penal Code related to the criminal sanction of defamation ;
- Articles 1369-1 à 1369-11 of the Civil Code related to agreements under electronic form ;
- Circular No. 2004-035 of 18-2-2004 related to the use of Internet in the educational framework and protection of minors.

Article 4 - Sanctions

The *user* is liable to sanctions in the following cases:

- Non-respect of rules previously defined in this charter and terms defined in user guides established by the University ;
- Abuse in the use of the information system for non-university purposes.

In these scenarios, sanctions applicable to the *user* are:

- Disciplinary proceedings and prosecutions expected by legislative and regulatory texts in force ;
- Suspension, suppression or limitation of access and use rights of the information system.

Besides, the *person legally responsible* can limit uses by precautionary measures, without affecting proceedings or sanctions procedures which can be taken against the staff.

Article 5 – Coming into force

This document cancels and replaces any other document or charter related to the use of *information system resources*.

This charter has been approved by the board of directors of the University of Orléans on 29/01/2016 and it is applicable from this day.

Management Policy of logs at the University of Orléans

1. Definitions

- The “establishment” in this document stands for « The University of Orléans » ;
- The « IT charter » in this document stands for the charter regulating the use of information system resources of the University of Orléans.

Entity	Existing entity within the University, its components, joint services and central services for the accomplishment of its missions. Examples: laboratories, education departments or sectors, administrative or technical services.
User	Anyone who has access or who uses *information system resources* of the University of Orléans, whatever his status, especially : - For tenured staff or non-tenured staff members who have to carry out missions involving the administration of education ; - All lecturers or researchers who use the resources of the University, including the premises ; - All registered students in the process of registering for the current year, or who was registered at the University ; - All providers under contract with the University ; - All interns who use the resources of the University, including the premises ; - All authorized readers who have access to the library resources ; - Anyone who has an access to a service hosted by the University, including the website ; - Anyone temporary welcomed within the University and so who has access to a computer station of the University and/or to the computer network (lecturer, visiting scholar, etc.).
Information system resources	All technical, applicational, organizational, human and documentary resources which allow to collect, to store, to process, to search for and/or to transmit data, especially : - All fixed hardware : computing stations (including self-service stations), servers, phones, peripheral devices (keyboard, screen, printer, etc.), plugs, cables, … - All mobile hardware : computers, phones, etc. - All software or network/computer services: network access, Internet access, messaging service, office equipment, etc. - All data carriers: electronic, paper, etc.
Logs	Information that an information system resource records on the activity or the identity of its users.

2. Context

The working of the establishment passes through the use of the information system and means of communication which is based on connected network on a global scale. These networks, which provide an unequalled flexibility, have also an inherent vulnerability, and their use engages the personal responsibility of the users, and in some situations the responsibility of the establishment which makes these means available as work tools.

The use of new communication technologies causes the problem of protection of the sensitive information[1] managed by the users on one hand, and of information systems under the responsibility of the establishment on the other hand. Applied measures must allow the establishment to fulfil its missions satisfying requirements which are ordered by its commitments concerning its partners, rules about the protection of sensitive data and the protection of science heritage, applicable laws and regulations (see IT charter) and especially the law about the protection of private data (respect for the rights of the individual) and security of information systems.

Ethics and a use control are therefore necessary, as well as an information and an awareness of the users. The establishment sets up agreements and means to ensure security and control of the IT means' use, and also fixed conditions of use of these means, to guarantee the individual rights of each user.

3. Basic principles

A control of reliability and security of working of the information systems and guarantee of the legality of operated transactions need a control which is necessarily based on a systematic and temporary recording of some information characterizing each transaction, called logs.

3.1 - Aims of processing

Processing of these logs aim:

- To control the volume of use of the resource, to measure the traffic to detect anomalies to set up a quality of service and to advance equipment according to needs (metrology) ;
- To check rules about information systems security (ISS) are correctly applied ;
- To detect any security failure or anomaly, voluntary or accidental, passive or active, of human or material origin ;
- To detect any violation of law or any misuse of IT means which can engage the responsibility of the establishment ;
- To detect the use of the IT means contrary to the IT charter of the establishment.
- To be able to provide elements of proof necessary to conduct inquiries in case of incident and to answer to any demand from the judicial authority presented in legal forms.

The aforementioned aims require going beyond a recording and a use of statistical data. They necessarily involve the recording, the temporary preservation and the possible using of personal data, as far as elements contained in traces enable to be traced back to the user.

These logs and their processing have to respect rights of everyone and especially to conform to the law of January 6th, 1978 modified by the law of August 6th, 2004 said "Data Protection Act". They must have respected the preceding information principle and transparency principle as well as the declaratory system in force with the, CNIL (French National Data Protection Authority).[2]

[1] Sensitive information insofar as confidentiality (agreement, research data, nominative information...), integrity (information of management...) and availability need a particular protection.

[2] To see the practical guide related to the control of use of IT means in the *how-to book "Informatique et Libertés"*

3.2 - Duration of preservation

The duration of preservation of logs is 1 year at the most. The establishment forbids itself to exploit it beyond 3 months except on official requisition or under an anonymous form.

3.3 - Quality of collected data

Logged information has to be factual and contextual, which means it has to be able to know the environment of the collection, the host system, applied software etc. The logged hour is an important piece of information because it is usually the first element used to compare logs from different servers. So it's essential that machines producing logs are synchronised on a time server.

Possible interruptions of the logging must be visible by recipients of this data.

3.4 - Security and integrity of data

Logs containing personal data have to be identified to guarantee their deletion beyond a year.

In the case of use of anonymous logs, an anonymous copy of logs is made. The fact to make it anonymous is realised in accordance with standard practice, it is irreversible. We will refer especially to the expert assessment[3] published by the CNIL, the French version of National Data Protection Authority in this field.

4. Protagonists

Users

All users, as they are defined in the introduction of this document, have to respect the IT charter in force in the establishment.

4.1- ISS functional chain

Apart from operators of the functional chain specified below, nobody has an access right to logs containing personal data, including the hierarchical chain. They are bound by professional discretion, even by professional confidentiality.

4.1.1 – System and network administrators

They are in charge of the application and general surveillance of systems and network and they make sure security rules of information systems are respected. As such, they manage traces in accordance with general obligations of their post.

They tell the ISSM (rssi@univ-orleans.fr) about any working anomaly or any incident which can suggest an intrusion or intrusion attempt on systems or the network.

They agree to execute processing or to provide information which can include personal data only at the request of the security functional chain.

for the higher education and the research (This book is available on the website of the CNIL and the one of the AMUE)

[3] http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/index.html#/40/

4.1.2 – The other operators of the functional channel ISS:

- Security correspondents of information systems (that is to say IT correspondents)
- The Information System Security Manager (ISSM) and his assistant
- Certified Information Systems Security Professional (CISSP) (French : Autorité Qualifiée de Sécurité des Systèmes d'Information (AQSSI))
- The Security and Defense Official.

They are also bound by professional discretion and in some cases by professional confidentiality according to their mission.

5. Recorded information

5.1 - Information logged by servers (except messaging service and Web) and computer stations

For each attempted connexion, attempted logon or attempted request of an increase of his rights, all or some of the following information can be automatically recorded by logging mechanisms of the service :

- The user name of the person making the request ;
- The date and hour of the attempt ;
- The result of the attempt (success or failure) ;
- The realized orders.

The choice of a policy of centralization of server's logs (except messaging service and web) and computer stations can be set up.

5.2 – Messaging service, service of instant messaging, of forum and of mailing lists

Servers hosting these services applied within the establishment record for each sent or received message all or some of the following information:

- The address of the sender and possibly elements which identify the one who connected to the server ;
- The address of recipients ;
- The date and time of the attempt ;
- The different machines penetrated by the message ;
- The processing « accepted or rejected » of the message ;
- The size of the message ;
- Some headers of the message, such as the digital user name of the message ;
- The result of the processing of non-requested mails (spam) ;
- The result of the antiviral processing ;
- Operations of validation or rejection by the moderators when it is applicable.

Content items of the messages are not logged, however, applications can include archives which don't come under logs (chrono departure and receipt).

5.3 - Web server

We distinguish web servers used within the establishment and those situated out of the establishment.

5.3.1 - Web server of the establishment

For each connexion, Web servers record all or some of the following information according to requirement of quality of service and security of the web application:

- Names or IP addresses, source and destination ;
- The different authentication data in the case of an authenticated access (intranet for example) ;
- The URL of the consulted page and information provided by the client ;
- The kind of x request ;
- The date and time of the attempt ;
- The volume of transferred data ;
- The different passed parameters.

5.3.2 - Web server outside the establishment

When users are members of the establishment, for each web access via internal network towards external servers, all or some of the following information can be recorded:

- Names or IP addresses, source and destination and the different authentication data ;
- The URL of the consulted page ;
- The kind of the request ;
- The date and time of the attempt ;
- The volume of transferred data ;

The article L.34-1 of the French Post and Electronic communications Code explains that electronic communications operators are bound to keep connexion data but that those "can't focus on the content of exchanged letters or consulted information, in any form whatsoever, as part of these communications ". So this ban applies particularly to the URL of consulted pages in the event that the establishment gives Internet access to people outside the establishment. Indeed, so it is possible to assimilate the network service of the establishment to those of an electronic communication operator.

5.4 - Telephony on the Internet (or IP telephony)

The use of IP telephony can engender specific issues in the field of security or in the field of control of the good working of networks, but of course, principles related to the French « Data Protection Act » apply to IP telephony as well as the other telephony systems.

When supporting lists of called phone numbers are established, the last four figures of these numbers are masked. However, the establishment can edit lists containing all called numbers in the event that they ask the staff for the repayment of the cost of personal communications or in the event that an unusual use has been noted.

The declaratory scheme of these logs is the object of the simpler norm No. 47 related to the use of landline or mobile telephony services on workplaces. Besides, practical information No. 11 from the how-to book « informatique et libertés » for the higher education and the research[4] titled « Utilisation du téléphone sur le lieu de travail » details this case.

[4] http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_AMUE_2011.pdf

5.5 – Network equipment

We call « network equipment » routers, firewall, switches, access points, equipment of metrology and network administration, etc. For each packet which goes through the equipment, all or some of the following information can be collected:

- Names or IP addresses IP, source and destination ;
- Numbers of source port and destination as well as the protocol ;
- The date and time of the attempt ;
- The way the packet was processed by the equipment ;
- The number of packets and the number of transferred bytes ;
- Alert messages.

5.6 - Specific applications

We mean by «specific applications», any application other than those mentioned above which need the recording of some parameters of connexion and use, for compatibility, management, security or development reasons.

Among these applications, we can quote the following examples:

- Access to databases ;
- Access to the ENT (espace numérique de travail) (french digital work space) ;
- Authentication service (SSO, radius, …) ;

As in the cases of internal web servers, generic logs are subject to be mad eup of all or some of the following information able to be collected:

- The identity of the sender of the request ;
- The date and time of the attempt ;
- The result of the attempt ;
- Volumes of transferred data ;
- The realized instructions ;

Log processing described here doesn't cover all data kept by these applications which, thanks to their nature, can log some operations. It is reminded that if data which has to ensure traceability is personal, it is subject to obligations of the French Data Protection Act (declaration to the DPO of the establishment).[5]

6. Aims of realised processing and their recipients

The realized processing must enable logs to be obtained which respond to basic principles previously formulated, remaining in compliance with legal obligations about the personal data protection and private life.

[5]The French Data Protection Officer was introduced in 2004 with the reform of the French Data Protection Act. His status allows him to be exempted from the previous obligation to report of ordinary and common processing. Only processing identified as sensitive in the law are still subject to authorizations and keep being the subject of formalities. He has a role of advice and monitoring in the legality of deployment of IT projects and, more generally, personal data management.

6.1 - Statistical results

These are automatically collected and allow to control volumes of use of means which are made available for users as work tools. During the exploitation of these results, we distinguish anonymous results from the results which can be linked to the identity of a person. Among all these processing, there are:

- Statistical processing anonymously, in transferred volume and in number of connexions ;
- Rankings of services mostly used in volume and in number of connexions ;

« Anonymous » results can be kept beyond the deadline mentioned in paragraph 3.2 and can be posted on websites available for anyone. However, systems and network administrators restrict access to results which contain personal data concerning themselves and possibly to the ISS functional chain. Shelf life of these non-anonymous statistics can't exceed those of logs used to produce these statistics.

6.2 – Test results

A systematic analysis of traces can be set up, with the authorization of the ISSM, to detect as soon as possible incidents related to the information systems security.

In case of incidents analysis can be made by system and network administrators on available traces. Results can only be transmitted to the ISS functional chain and to the CERT-Renater or CERTA for security incidents.

In this case, the access to logs is limited to systems managers in charge of analysing the incident and to the ISSM. The extraction of information and its use is strictly limited to the analysis of the incident. If the incident is not recognised, results are not transmitted and they are immediately destroyed.

6.3 – Misuses detection

We mean by « misuses » uses of network which are against laws or the IT charter.
We are talking also about uses which compromise network services of the establishment such as:

- Excessive consumption of the bandwidth
- Introduction of breach in the network security
- Voluminous files
- Massive sending of emails
- Etc.

Also uses which harm the good working of the establishment, even coming from the outside such as:

- Malicious phone calls
- Malicious emails
- Etc.

Logs can be used to highlight these abuses. For example, rankings of machines which have consumed the most network in transferred volume and in connexions number often allow to detect undesirable use of protocols of peer to peer or the presence of cybercriminal servers. It is necessary to refer to the pratical information « Contrôle de l'utilisation des moyens informatiques » from *the how-to book « Informatique et Libertés » for higher education and research*. (This guide is available on the website of the CNIL and those of the AMUE)

When these processes are applied, it is in a systematic manner (they are applied to all machines of the establishment network or of a given part of the network) and don't target anyone, or category of people.

6.4 – Untouched logs

These logs allow to put a particular action in its context, for purpose of investigation. As soon as the appearance of an incident, untouched logs can be required by the ISS functional chain.

The systems and network administrators are in charge of the application of the query, and they are subject to professional confidentiality for this activity.

Untouched logs are delivered to a judicial authority, on its request, to allow it to carry out an investigation.

6.5 – Individual access right

Each member of staff can ask to consult the traces which concern him. Requests have to be made in writing with the DPO or the President of the University. In accordance with the article 39 of the French « Data Protection Act» of January 6th, 1978 modified, and with the article 92 decree of October 20th, 2005 modified in 2007, taken for the application of the aforementioned law, people who wish apply their access right have to justify their identity.

The research is carried out by the administrator, at the request of his line management, and results are directly transmitted to the user who requests, under the form of a «personal mail».

7. Information of users about the management policy of logs

The establishment must inform its users about the management of traces which concern them.

For this purpose, this document will be appendixed to the IT charter of the establishment. It will be made accessible to each user via network and especially:

- via the University website
- via the University intranet
- via the ENT

8. Enforcement

This document cancels and replaces every other document or charter related to the management of logs.
This management Policy of logs at the University of Orléans has been approved by the Senate of the University of Orléans on 29/01/2016 and it is applicable from this day.