IT and Osiris Network Acceptable Usage Policy

IT equipment belonging to the University of Strasbourg and the other partner institutions involved in managing the *Osiris* network is dedicated to teaching, research and administration. Most of this equipment is connected to the *Osiris* network, and thus to the Internet. Any user of this equipment therefore belongs to a large community, which implies compliance with certain rules relating to safety and good conduct, as any carelessness, negligence or malice by a user can have serious consequences for the community. This usage policy sets out the rights and duties of each person, and reflects a mutual commitment between individual users and the academic community.

Stakeholders

From an IT perspective, there are three categories of stakeholder in the academic community:

1. users: students, teachers, researchers and staff, who use the IT systems made available to them;
2. system administrators, who are responsible on a technical level for the proper functioning of IT tools (systems, networks and applications);
3. functional managers: the head of the institution, component directors, administrative managers, laboratory or service directors, and teachers supervising students for activities involving IT resources.

Each of these has identical rights and duties, with the system administrators and functional managers having additional, specific rights and duties.
In addition, each establishment connected to Osiris appoints an RSSI (Chief Information Security Officer - CISO), whose task it is to coordinate IT security, and who must be the main contact for all stakeholders.

The rights of all persons

Each person has the right to:

1. information about common resources and services offered by the institution, component or laboratory;
2. information enabling them to make the best use of their available resources;
3. information about the security of the system that they use.

Duties of each person

1. each person must respect intellectual and commercial property, in accordance with the legislation in force;
2. each person has a duty to comply with the safety rules applicable to the system that they use. These rules consist of this usage policy, supplemented by regularly updated appendices, as well as any specific rules related to a particular work environment (laboratory, student resource room). These rules are made available to each user by the functional manager or system administrator;
3. each person undertakes not to become aware of information belonging to another person without his/her consent, not to communicate such information to a third party, and not to communicate any non-public information to a third party to which he/she may have access but of which he/she is not the owner;
4. each person must clearly identify themselves. No person has the right to usurp the identity of others or to act anonymously, and no person can transfer their access rights to another person or persons;
5. each person must strive to achieve their goal by the most economical use of common resources (disk space, printing, occupation of workstations, network transfers, occupation of remote servers, etc.);
6. each person must contribute to improving the functioning and security of IT tools by complying with security rules and advice, by immediately informing managers of any anomaly observed, and by bringing colleagues' attention to any problems of which they are aware;
7. each person must ensure that they use the resources made available to them in a professional context, which excludes any use for commercial purposes. Reasonable use to meet everyday, family needs is tolerated, provided that this does not affect the performance of the system and the network;
8. no person can modify an item of equipment - both hardware and system software - without the agreement of the system manager.

Specific rights and duties of system administrators

Administrators must ensure the normal operation and security of IT tools. Their role requires them to have access to all user information, including information saved on the workstation.

In the course of their duties, system administrators are entitled to:

1. be informed of the legal implications of their work, including the risks they incur in the event that a user of the system for which they are responsible commits a wrongful act;
2. use log files and access private information for diagnostic and system administration purposes, while strictly respecting the confidentiality of this information.

In the course of their duties, system administrators are entitled to:

1. inform users of the information and processes to which they have access by virtue of their role;
2. oversee the declaration of the automated processing of personal information, in accordance with the regulations in force;
3. notify users and make them aware of the IT security problems inherent in the system, and inform users of the security rules they must observe, assisted by the network security correspondent;
4. comply with confidentiality rules, keeping access to confidential information to a minimum and respecting strict professional discretion in regard to this issue;
5. act to improve security, in the interest of both the institution and users;
6. in the event of a security incident, immediately inform their functional manager and cooperate with both the institution's CISO and the security managers of the organisations concerned, where appropriate, in order to resolve the incident.

Specific rights and duties of functional managers

IT systems functional managers are entitled to:

1. suspend access to IT resources and the network in the event of a problem affecting the proper functioning of the system;
2. take any precautionary measures and inform the institution's CISO if a user fails to comply with the usage policy.

IT systems functional managers are entitled to:

1. inform all stakeholders and disseminate this usage policy by any appropriate means;
2. inform the network security correspondent of the names of the system managers for all the machines placed under their authority, and provide the IT Department with the name of a network manager;
3. support the system administrators in their implementation of this usage policy.
4. refer serious breaches resulting from non-compliance with this usage policy to the hierarchical authority and the CISO, as the head of the institution may initiate disciplinary or criminal proceedings.

Penalties for non-compliance

Non-compliance with the rules defined in this usage policy may result in the following sanctions:

1. disciplinary:
    - the functional managers have full authority to take the necessary protective measures in the event of a breach of this usage policy, and to prohibit the offending users from accessing the IT resources and the network,
    - offending users may be referred to the competent disciplinary committee;
2. criminal:
   The use of IT resources and electronic means of communication is subject to common law, such as the French Intellectual Property Code, or the French Criminal Code, and to a few specific texts, such as the French Data Protection Act, or the law relating to computer fraud (the so-called "Godfrain" law).

This usage policy and its appendices apply to all users of the institution's IT resources.