Université de Strasbourg

CHARTER ON THE PROPER USE OF UNIVERSITY DIGITAL RESOURCES

Main Document

Valérie GIBERT
Director General of Services

Contact person
Guy BRAND
Chief Information Security Officer
Tel: +33 (0)3 68 85 06 88
gb@unistra.fr

Université de Strasbourg

Contents

Preamble

The aim of this charter is to set out the rules concerning the use of the digital resources of the University of Strasbourg.

The purpose of these rules is to contribute to the security of the information system and to guarantee the integrity and confidentiality of the data hosted there.

The reasonable use of digital resources also contributes to creating a healthy work-life balance as well as reducing the institution's environmental footprint.

Article I. Field of Application

The rules for the use of digital resources included in this charter apply to the University of Strasbourg and all users.

In this charter, the term "digital resources" means all elements or resources constituting the information system of the University of Strasbourg. Thus, digital resources represent all the software and hardware, IT tools and digital services that the University of Strasbourg makes available to its users.

"Users", within the meaning of this charter, are defined as all persons having obtained authorisation to access the information system of the University of Strasbourg.
This access is achieved by means of a registered account created in the information system for the benefit of the user, for the duration of their activity at the University of Strasbourg. Known as the "Unistra account", this consists of a user's own "login", which is assigned when they arrive at the university, and a password of their choosing. The life cycle of Unistra accounts is governed by a set of rules that ensure the account expires after the user's departure. The University of Strasbourg does not recognise a general right to maintain access to the information system and, consequently, to maintain the Unistra account, after the user's departure.

The provisions of this charter also apply to users who are University of Strasbourg members of staff authorised to work remotely in the performance of their duties.

Users having administrator functions for digital resources shall be subject to an additional specific charter detailing their special obligations.

Users whose activity is associated with partner organisations shall be governed by a specific document supplementing this charter.

All of these documents are available online, and in particular on the University of Strasbourg's digital and social workspace, known as "Ernest".

Article II. Conditions of use for information systems and digital resources

Section II.1 Professional / Private Use

The University of Strasbourg makes a range of digital tools and services available to its users for professional purposes.

Within the meaning of this charter, the use of digital resources is professional in nature when it occurs:

- in connection with tasks entrusted by the University of Strasbourg, for users who are members of its staff, including teacher-researchers; teachers; administrative, technical, social and health staff; as well as its service providers and partners;
- in connection with teaching activities, for its student users.

In contrast, use for private purposes must be non-profit in nature and limited, in respect of both frequency and duration. It must not adversely affect either the quality of the user's work or the time that the user spends on it, or the performance of the service.

Use for private purposes must be in strict compliance with the security principles set out in Article III of this charter. Its impact must remain negligible for the University of Strasbourg. Such use must therefore not result in any additional financial or energy cost to the university, nor any increased risk to the security of data and professional equipment.

All information is deemed to be professional, with the exception of data explicitly designated by the user as relating to their private life. Users are responsible for storing their private data in a space set aside for this purpose and unambiguously identified as such. Users shall be responsible for regularly backing up any private data.

Thus, all users shall show the extra-professional nature of a part of their data by using, exclusively, the term "private" to name the folder of files or the subject of the message containing such information.

Section II.2 Continuity of service - management of absences and departures

In the event of a definitive departure or an occasional absence, users shall inform their supervisors of the procedures for accessing the applications and data that enable continuity of service.

Measures to conserve professional data are set out with the designated supervisor within the University of Strasbourg.

In the event of his or her departure, a user's supervisor will ensure that access is deleted or, in the case of internal mobility, that access and rights relating to professional applications are reassessed.

Users are responsible for their private data space. They are responsible for destroying their private data space when the time comes for their definitive departure from the department or the university.

Article III. Security Principles

Section III.1 Applicable Security Rules

The University of Strasbourg implements appropriate protection mechanisms in respect of the digital resources made available to users.

Users are informed that passwords are a security measure designed to avoid any malicious or abusive use. This measure does not make any protected IT tools personal.

The access levels open to users are defined in accordance with the mission entrusted to them. The security of the resources made available require that they:

- comply with all security instructions, in particular rules relating to password management;
- maintain the absolute confidentiality of their password(s) and not disclose it/them to any third party;
- manage access as required, in particular by not using the names and passwords of other users, nor trying to discover them.

In addition, the security of the resources made available to users requires that a number of precautions be taken:

- *by the University of Strasbourg:*
  - ensure that sensitive resources are not accessible in the event of absence (outside the continuity measures implemented by supervisors);
  - limit access to only those resources that the user is expressly authorised to access;

- *by users:*
  - if a user does not have explicit authorisation, they must not access or try to access resources on the information system, even if such access is technically possible;
  - not to connect equipment not entrusted or not authorised by the University of Strasbourg directly to local networks;
  - not to install, download or use any software programs or packages on the University of Strasbourg's equipment without prior authorisation;
  - adhere to the mechanisms put in place by the University of Strasbourg to combat cybersecurity threats and hazards.

Section III.2 Duty to Report and Inform

The University of Strasbourg must inform users of any element likely to enable them to assess the level of risk incurred while using the information system.

Users must inform support at the earliest opportunity of any malfunction noted or any anomaly discovered, such as an intrusion into the information system. They must also inform the site administrator (or, in the absence of such, the institution's CISO) of any possibility of accessing a resource for which they do not have authorisation.

Section III.3 Security Monitoring Measures

Users are informed that:

- in order to carry out corrective, perfective or progressive maintenance, the University of Strasbourg reserves the right to carry out work (remotely, if necessary) on any resources made available to them;
- any remote maintenance requires that users be informed in advance;
- any blocking information or information that cannot be sent to its intended recipient due to a technical difficulty may be isolated, and if necessary deleted.

The University of Strasbourg informs users that the information system may be subject to surveillance and control for the purposes of statistics, traceability, optimisation, security or detecting misuse.

The personnel charged with carrying out monitoring operations are sworn to professional secrecy.

Section III.4 Anti-Virus Protection

The University of Strasbourg has rolled out generalised software protection not only on the servers but also on user workstations.
The aim of anti-virus software is to protect all machines against attacks caused by malicious codes. An anti-virus client is installed on each user station. This charter prohibits deactivating, altering the operation of, or uninstalling this client. It is also prohibited to use other software (anti-virus or other) likely to lead to a malfunction of the anti-virus software installed as part of the University of Strasbourg's security strategy.

The use for professional purposes of equipment other than that made available to users by the University of Strasbourg, in particular personal equipment, must be in strict compliance with the security principles set out in this charter.
Any user wishing to access the resources of the University of Strasbourg information system is thus responsible for ensuring the safety and security of the equipment used. This obligation also applies to members of staff who use computer equipment made available by the university with full administrator status, whether such status is motivated by professional necessity or any other factor.

Article IV. Electronic Communications

Section IV.1 Mail service

The use of the mail service is a central element for the optimisation of work and the pooling of information within the University of Strasbourg.

The mail service is a tool intended for professional use:

- it may form the basis of a private communication within the limits defined in section II.1;
- it is subject to the recommendations of the charter regarding digital quality of life, in the same way as other work tools.

(a) Email addresses

The University of Strasbourg undertakes to make a professional named mailbox available to users to allow them to send and receive emails.

As far as possible, the email address assigned by the administration to each University of Strasbourg staff member takes the form: firstname.surname@unistra.fr, except in special cases or when there are names with identical spelling.

Similarly, the email address assigned by the administration to University of Strasbourg students takes, if possible, the form: firstname.surname@etu.unistra.fr, except in special cases or when there are names with identical spelling.

The named part of the e-mail address is the simple extension of the administrative address. It does not in any way diminish the professional nature of the mail service.

The named email address is allocated to a user who can, as they decide and under their responsibility, authorise a third party to access their mailbox.

A functional or organisational email address may be set up if it is operated by a department or a group of users.

The University of Strasbourg is exclusively responsible for managing email addresses corresponding to institutional distribution lists that designate a category or group of “users”. These addresses cannot be used without express authorisation.

(b) Email content

Emails are used to exchange professional information linked to the activity of the University of Strasbourg or within the University of Strasbourg. In all circumstances, users must behave responsibly and in a manner that complies with the provisions contained in this charter.

With reference to Article II, Section II.1, any message is deemed to be professional unless it contains the word “private” in the subject line, or if it is stored in a specific data space that is identified as such.

Emails whose content, in whole or in part, contain references that are contrary to standards of public decency, or represent an invasion of privacy, or are detrimental to the image of another person, or infringe copyright are prohibited.

Any person writing emails that contain such references is liable to criminal proceedings, as well as disciplinary measures taken by the university.

(c) Sending and receiving emails

To guarantee the confidentiality of the data exchanged, users must check the identity and accuracy of the addresses of the recipients of any email messages.

For the same reason, users must ensure that messages are sent only to the recipients concerned.

To ensure that services continue to operate correctly, limits may be put in place. In this case, the terms of such limits will be described in the user guide.
Recommendations concerning the use of the mail service and the composition of messages are given in the practical user guide appended to this charter, as well as in the charter on digital quality of life.

(d) Status and legal value of emails

Emails exchanged with third parties may legally constitute a contract (Article 1174 of the French Civil Code).

(e) Storing and archiving emails

Each user must organise and ensure the conservation of any emails that may be indispensable for them to carry on their activities, or simply useful as written evidence.

The user guide appended to this charter contains a set of essential rules and recommendations, compliance with which guarantees that the data are preserved.

Section IV.2 Internet

It is recalled that the Internet is subject to all rules of law in force.

The University of Strasbourg provides users with Internet access whenever possible.

That Internet access is designed for professional uses only. It can form the basis for private communication as defined in section II.1, in compliance with the regulations in force.

Users are informed that given the educational mission of the university, the voluntary and repeated consultation of content of a pornographic nature on the premises or via the digital resources of the University of Strasbourg is prohibited.

The University of Strasbourg reserves the right to filter or ban access to certain sites, to monitor the sites visited either a priori or a posteriori, and to monitor corresponding lengths of access. In such cases, users are notified of the measures taken.

Internet access provided by the University of Strasbourg is only authorised through the secure devices in place (captive portal, Eduroam certificate, ...) Specific security rules may be detailed, if necessary, in the user guide appended to this charter.

Users are informed of the risks and limits inherent in using the Internet via training programs or awareness campaigns communicated, in particular, via the digital and social workspace (Ernest).

Section IV.3 Downloads

The download of any file, in particular audio or image files, must be done in compliance with intellectual property rights as defined in Article VI.

The University of Strasbourg reserves the right to limit the downloading of certain files that may prove to be too large or that may pose a risk to the security of the information systems, such as viruses, malicious code or spyware.

Article V. Traceability

The University of Strasbourg has a legal obligation to put in place an Internet access, email and data exchange logging system.

The University of Strasbourg reserves the right to put in place traceability systems on all digital services and tools that it makes available to users.

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and Law no. 78-17 of 6 January 1978 known as the "Data Protection Act", as amended, this data processing is recorded in the university's data processing register.

Users are informed that the legal duration for retaining log files is one year from the date they are saved.

Article VI. Respect for Intellectual Property

General

The University of Strasbourg reminds users that using digital resources implies compliance with its intellectual property rights and those of its partners and, more generally, any third party holders of such rights.

Consequently, each user must:

- use software, databases, web pages, texts, images, photographs or other creations protected by copyright in strict compliance with the licences attached to them;
- refrain from any reproduction, copying, distribution or modification without obtaining the prior and personal consent, if required, of the holder(s) of the intellectual property rights.

Anti-plagiarism system

As part of its strategy of installing plagiarism prevention and detection tools, the University of Strasbourg provides its teaching and research staff with text-matching software.

This service is used to analyse work submitted by students in electronic format, in order to find and identify paragraphs that are similar to texts available online or in reference libraries for which sources have not been cited.

The University of Strasbourg informs its students that their work (internship report, dissertation, thesis, etc.) is likely to be analysed using text-matching software.

An act of plagiarism may constitute the offence of counterfeiting incurring the civil or even criminal liability of the plagiarist via the infringement of intellectual property regulations. This practice also constitutes a

breach of the university's examination regulations, which is punishable by disciplinary sanctions for exam fraud, as determined by the competent disciplinary department in accordance with the provisions of the French Education Code (Articles R712-9 to R712-46 and R811-11).

The signatory of this charter undertakes to comply with both intellectual property regulations and the university's internal regulations.

See also the legal appendix: educational exceptions to copyright law.

Article VII. Protection of data privacy

Users are informed of the need to comply with regulations concerning the processing of personal data (automated or not) in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and Law no. 78-17 of 6 January 1978, the "Data Protection Act", as amended. Personal data is any information relating to a natural person who is likely to be identified, directly or indirectly.

Any processing involving personal data must comply with the provisions of the GDPR and Law no. 78-17 of 6 January 1978, the "Data Protection Act", as amended. In particular, the following operations are considered to be processing: the recording, storage and distribution of personal data in digital or paper format. CCTV systems are also subject to regulations.

Consequently, users wishing to perform such processing must inform the Data Protection Officer (DPO) beforehand, who will take the measures necessary to comply with legal provisions.
In addition, pursuant to the provisions of this law, each user has a right of access, correction and opposition relating to all personal data, including data relating to the use of the information systems. Depending on the case, users also have the right to limit the processing and portability of their data.

These rights are exercised with the university's Data Protection Officer (DPO): dpo@unistra.fr

Article VIII. Limits on use

In the event of non-compliance by a user with the rules as defined in this charter and the procedures set forth in the user guide appended hereto, the Director General of Services may, after notifying the interested party and without prejudice to any sanction proceedings or procedures that may be brought against such user, limit uses, or have uses limited, as a precautionary measure in the following ways:

- limit user access;
- disconnect the user, with or without prior notice depending on the seriousness of the situation;
- withdraw access codes or other access control methods and close accounts;
- delete, compress or isolate any data or file that is too large, or clearly in contravention of the charter, or which would jeopardize the security of the resources;
- prevent users from accessing the resources for which they are responsible.

Any misuse for extra-professional purposes of the resources made available to users is punishable by the sanctions detailed in the legal appendix to this charter.

Article IX. Entry into force of the charter

This charter is incorporated into the internal regulations of the University of Strasbourg.

This charter functions in addition to all other documents or charters relating to the use of digital resources, including:

- the digital quality of life charter;
- the remote working charter;
- the faculty IT asset management charter.

The following documents are appended to the french version of this charter:

- legal appendix;
- user guide;
- administrators' charter;
- decision of the President of Unistra of 10/02/2017.

Director General of Services,

Valérie GIBERT