Venice
International
University

Isola di San Servolo
30133 Venice, Italy
P.I. 02928970272
C.F. 94027420275

T +39 041 2719 511
F +39 041 2719 510
viu@univiu.org
www.univiu.org

TERMS OF ACCESS AND USE OF IT SERVICES AT VIU

Premise

The purpose of this document is to define the organizational, physical and logical security measures to be adopted by Venice International University while processing personal data in order to comply with the provisions of Italian Legislative Decree 196/03 and it successive integrations, and GDPR (EU) 679/2016.

Network use policy

Subject and scope

This policy governs the terms of access and use of the IT and telematic network and of the services that can be offered or received by means of it.

General principles – rights and responsibilities

Venice International University fosters the use of the network as a useful instrument for the achievement of its own purposes.
Users may express their thoughts freely without violating the rights of other users and third parties, the integrity of the systems and the relative physical resources, in compliance with the applicable laws, provisions and contract obligations.

Users are aware of the IT and telematic resources potential and undertake to act responsibly, with self-discipline, avoiding any misuse of the network.
The computer workstation is supplied with the software required for the performance of users' functions, it is therefore forbidden to change the computer's configuration.
Personal computers are supplied with the software required for the performance of users' specific tasks. Therefore neither users nor other operators, with the sole exception of the administrator, may install any software. It is the responsibility of the user to make sure that the applications in use are under a valid licence.
Every user is held responsible for the data saved in his/her own personal computer. For this reason, users shall backup these data according to the instructions provided by the data processing controller or his/her delegate.

Misuse and forbidden activities

Misuse is expressly forbidden. In particular, it is forbidden to:

- Use the network for any purpose other than those set out in penal, civil and administrative laws, as well as in this policy;
- Use the network for any purpose other than institutional activity;
- Use a password for which authorization has not been given;
- transfer user's personal access codes (USER ID and PASSWORD) to third parties;
- gain unauthorized access to internal or external network resources;
- violate the privacy of other users or third parties;

Venice
International
University

Isola di San Servolo
30133 Venice, Italy
P.I. 02928970272
C.F. 94027420275

T +39 041 2719 511
F +39 041 2719 510
viu@univiu.org
www.univiu.org

- knowingly perform an act that will interfere
- with the normal operation of the network and restrict other users' use and performance;
- deliberately attempt to distract resources (people, skills, processors);
- perform any unauthorized transfer of information (software, database etc.) or allow third parties to do so;
- knowingly run or install on any computer system and on the network a program intended to damage or to place excessive load on said computer system or network;
- deliberately install or run unauthorized software applications for any purpose other than the institutional ones;
- deliberately cancel, uninstall, copy or remove software applications for personal purposes;
- deliberately install hardware components for any purpose other than the institutional ones;
- deliberately remove or damage hardware components;
- use the hardware and software resources and the available services for personal purposes;
- use institutional e-mail accounts for personal purposes and/or non-institutional purposes;
- use e-mail accounts with other users' access codes;
- use e-mail accounts to send and receive illegal material.
- use Internet access for personal purposes;
- Access the Internet through a modem connected to the user's own personal
- computer, unless express authorization has been given and for special technical reasons;
- gain unauthorized access to other networks;
- monitor or use any kind of IT or electronic system to control users' activities, read, copy or cancel other users' files and software without explicit authorization;
- mask user's identity or use resources that allow to mask user's identity while on the network;
- Enter or change the bios password without the knowledge and previous authorization of the administrator;
- leave the workplace unattended or accessible.

Permissible use

The administrator is authorized to:

- Monitor or use any kind of IT or electronic system to control the use of the network resources, of the clients and applications, to copy and remove files or software only for performing ordinary maintenance, security management and data protection activities in compliance with labour law;
- Create, modify, remove or use any password
  only for performing ordinary maintenance, security management and data protection activities in compliance with labour law; The administrator shall notify the user of the change; the user, in turn, shall inform the data controller or the password custodian;
- Remove software applications only for performing ordinary maintenance,

Isola di San Servolo
30133 Venice, Italy
P.I. 02928970272
C.F. 94027420275
T +39 041 2719 511
F +39 041 2719 510
viu@univiu.org
www.univiu.org

- security management and data protection activities in compliance with labour law;
- Remove hardware components only for performing ordinary maintenance, security management and data
- protection activities in compliance with labour law.

Subjects authorized for network access

Subjects authorized for network access include employees, software suppliers limited to the maintenance of the applications within their competence and external collaborators performing institutional functions limited to the duration of their collaboration.

Access to the network is guaranteed in so far as the equipment allows.

The system administrator may restrict the access to the network of some categories of users for technical reasons.

In order to ensure safety and the best functioning of the available resources, the administrator may propose the data processing controller to adopt specific operational measures which the users shall comply with.

Users who must use the applications for duty reasons are given authorized access.

Terms of access to the network and applications

The user obtaining the access to the network and applications shall comply with this policy and the provisions governing the activities and services performed by means of the network and undertake not to misuse it nor violate the rights of other users and third parties.

The user accessing the network and applications assumes full responsibility for the activities performed by means of the network, even for people whose access is granted as participants of organized courses.

It is the responsibility of the user to make sure that the antivirus software is regularly updated.

Sanctions

In case of misuse, depending on the gravity of the same, users may be subjected to the disciplinary sanctions set forth by the current laws and internal regulations, without prejudice to other penal, civil and administrative prosecution.