Rules of the Use of Campus Network at I-Shou University

Adopted on June 28, 2000, by the University Administration Council

Amendments to the Regulations promulgated with the consent from the President dated September 1, 2010

Amendments to Article 4 promulgated with the consent from the President dated March 21, 2013

Amendments to the Regulations promulgated with the consent from the President dated February 13, 2015

Amendments to the Rules adopted by the University Administration Council on October 20, 2021, and promulgated with the consent from the President dated November 29, 2021

I. To make the best of the campus network (including the dormitory network, hereinafter collectively referred to as "the Network"), disseminate the concept of respecting the rule of law, and establish norms for network users to follow, thereby facilitating education and learning, the Rules of the Use of Campus Network at I-Shou University (hereinafter referred to as "the Rules") are made by I-Shou University (hereinafter referred to as "the University") pursuant to the Taiwan Academic Network Management and Norms and the Campus Network User Directions under the auspices of the Ministry of Education.

II. Information appliances that use the Internet Protocol (IP) address of the University or that are used to access the Internet within the territory of the University are considered part of the campus network of the University. The information appliances mentioned herein include but are not limited to computer servers, personal computers, the Network, and portable information devices. Any and all individuals and units that use one of the aforesaid information appliances are considered network users of the University.

III. Network users shall avoid the following acts that might get involved in the infringement of intellectual property rights:

1. using computer programs or software without prior consent or authorization;
2. illegally downloading or copying works protected by the Copyright Act;
3. uploading protected works onto public websites without approval from the copyright owner;

4. republishing any articles posted on online forums even if the author has clearly indicated that no republishing is allowed;
5. setting up a website for the public to illegally download protected works;
6. illegally using or abusing Peer-to-Peer (P2P) networking to share software; or
7. committing an act that might get involved in the infringement of intellectual property rights.

IV. Network users are prohibited from getting involved in one of the following acts:

1. spreading computer viruses or programs that could cause damage to or interfere with normal system operations;
2. intercepting any information transmitted through the Network without authorization;
3. accessing network resources without authorization by means of cracking, embezzling, or using another person's user account and password, or disclosing another person's user account and password to a third party without any reason;
4. letting another person to use his/her user account and password without any reason;
5. hiding his/her user account or using a fake account, which does not apply to users authorized for the use of anonymity;
6. illegally accessing another person's emails or computer files;
7. abusing network resources by any means, including the mass transmission of advertisements, chain letters, or unwanted messages via emails; or interfering with normal system operations by flooding email inboxes or seizing resources;
8. spreading law-violating messages involved with frauds, aspersions, bullying, obscenity, harassment or illegal software trade by means of emails, online chatting, or other ways with similar features;
9. committing an offense against privacy as specified in Chapter 28 of the Criminal Code, an offense against computer security in Chapter 36 of the Criminal Code, or any other offenses in association with gender-based violence enabled by digital technology;
10. setting up a website promoting suicide or luring people to gamble, or engaging in compensated dating, drug trafficking, or other illegal acts on the Internet;
11. disclosing confidential information without prior consent;
12. vandalizing or interfering with the software and/or equipment for network operations at the University;
13. using the University's network resources to conduct illegal activities or any activities

irrelevant to teaching and research; or

14. any other acts that might be considered illegal.

V. To bring the functions of the Rules into full play, the Office of Library and Information Services (hereinafter referred to as "the Office") will take the following measures for network management:

1. The Office accepts applications for accessing network resources filed by network users and assists network users in establishing a self-discipline mechanism.
2. The Office applies suitable segments and control over data amounts.
3. The Office may suspend a network user's right to access the Network if he/she occupies a large number of network resources for no reason or has abnormal traffic, thereby affecting the normal operation of the Network.
4. The Office shall appoint staff members to manage and maintain online forums and other websites. The staff members-in-charge shall delete a post(s) or suspend a network user from accessing the Network if the network user violates the rules concerning the use of the Network. In case of a major offense, a violation of the University's regulations and rules, or a violation of the law, the violator shall be referred to the competent unit of the University or the judicial authorities.
5. If a network user accesses the University's information systems from outside the University, via his/her email account, or with a personal computer, he/she shall be solely responsible for what he/she does on the Internet.
6. Other matters relating to campus network management.

VI. The unit-in-charge at the University shall have respect for network privacy and shall not intercept personal information without authorization or get involved in the invasion of privacy. Notwithstanding the foregoing, exceptions may be permitted under certain circumstances as follows:

1. maintaining or checking system security;
2. acquiring evidence regarding or carrying out an investigation into an alleged violation of the University's regulations and rules on reasonable grounds;
3. cooperating with an investigation conducted by the judicial authorities; or
4. a proper conduct according to law or performed in the course of due business.

VII. Network users who violate the Rules shall receive the following punishment:

1. being suspended from accessing network resources; and
2. receiving punishment or disciplinary action depending on severity; a violator may put

forward an appeal by following the established administrative procedure if he/she has objections against the punishment/disciplinary action.

VIII. The Rules become effective on the third day of promulgation after being adopted by the University Administration Council and ratified by the President.

Note: In case of any disputes or misunderstanding regarding the interpretation of the language or terms of the Rules, the Chinese language version shall prevail.