APPENDICES

Acceptable Use Policy

- ICTO Computing Facilities, Campus Network and Internet

(Approved by the Rector on 17 May 2021)

1. Introduction

1.1 Purpose

The purpose of this policy is to ensure that the use of information and communication facilities and services provided by Information and Communication Technology Office (ICTO) is consistent with the highest standards and practices of teaching, learning, research and administration.

1.2 Policy

According to the “Regulations of the Organizational Structure of the University of Macau", ICTO is given the major authority to provide the necessary information and communication facilities and services for teaching, learning, research and administration, it also authorizes ICTO to supervise the proper use of rights of the related facilities and services on behalf of the University of Macau. Users shall abide by this policy and are also bound by the applicable laws of Macao and University’s related policies as well.

1.3 Scope

All users (staff, students, visitors, contractors and others) who are using the University's information and communication facilities and services are bound by the provisions of this policy.

2. Code of Use

2.1 Be consistent with academic, research and administration purposes, policies and goals of the University.

2.2 Information and communication facilities and services shall be used appropriately, and only for conduct in accordance with your role in the University.

2.3 The establishment or use of information and communication systems, facilities and services shall comply with the laws of Macao.

2.4 Do not conduct or attempt to conduct in any manner that endanger information security, including but not limited to improper acts of interference, interruption, intrusion or paralysis of services on any network, information and communication systems or facilities inside and outside the University.

2.5 Unless otherwise agreed by ICTO, a user’s right to use the related facilities and services is nontransferable.

2.6 Unless otherwise agreed by ICTO, the security measures of information and communication systems or facilities shall not be disabled, interfered with or removed, and users are not allowed to install and use any unauthorized computer programs.

2.7 Users shall not process, store, publish, broadcast or bulk-distribute the following with information and communication facilities and services:

- Contents that violate the laws of relevant regions and advocate or promote any illegal behavior;
- Contains any contents of harassment, bullying, curse, intimidation, hatred, defamation, threat, discrimination, extremism or rumor, etc., and that may intensify contradictions and conflicts;
- Contains objectionable, obscene or indecent contents;
- Contents used for personal, political, economic, or commercial benefits;
- Information that is not related to your role in the University.

2.8 If you, as a service provider, need to provide information services to users in the University, or set up networks, information and communication systems or facilities in the University, you shall conduct risk assessment, periodic maintenance, defining appropriate security measures and guidelines for related services, systems or facilities. In addition, you shall obtain comment from ICTO first.

2.9 When you need to access University's internal data, you shall take appropriate data protection measures, and you shall use suitable facilities to process, store, and transfer the related data.

2.10 In case you encounter any information security incident, you shall notify ICTO as soon as possible, and shall provide necessary information for incident investigation.

2.11 All users shall follow the Guidelines for User Account and Password, and are responsible for keeping passwords secure and confidential. Password shall be changed periodically or two-factor authentication service shall be enabled for account protection. For any loss occurrence of identity and authorization tools, such as passwords, e-certificates, you shall notify ICTO as soon as possible.

2.12 If a research project has a potential violation of relevant policies, you shall obtain comment from ICTO first.

2.13 Before visitors, outsourced service personnel or service providers having access to any UM systems, the relevant reception unit and personnel shall ensure that they have signed a non-disclosure agreement, and comply with this policy.

3. Relevant examples of the policy mentioned above for reference:

3.1 Abuse of information and communication facilities and services

- Malicious occupy extra computers in learning common;
- Eating and playing in the computer room;
- Unplug the cables of university equipment, such as power cord, network cable etc. in order to connect your own electronic device;
- Use University's facility to play video games or browse pornographic websites;
- Loan, rent or sell your user account to let others obtain computer services of the University;
- Send bulk-mail to the University users to promote promotional activities of your friend's new shop;
- Use the University email address to register a personal online shop for running a business.

3.2 Hazard information and communication facilities:

- Use or access to any computer system without authorization inside or outside the University;
- Delete, modify or insert data to a system without authorization;
- Hire or assist hackers to attack the campus network or information system;
- Unplug the power supply of the wireless network device to interrupt the service;
- Distribute spam mail or viruses to cause network congestion or interfere with the works of others;
- To conduct network scanning activities or experiments to test system vulnerabilities without the consent of ICTO, or to monitor or steal information on the campus network or information system;
- No matter intentionally or unintentionally, whether with or without tangible or intangible damage to information and communication facilities, to alter any university information system, hardware and software without authorization.

3.3 Improper handling of information or abusing of information services:

- Publish tools or methods that can hack the University system in the discussion forum;
- Pick up external storage devices in campus area and read the content without authorization;
- Use personal email to process UM's administrative information or data;
- Store or process any protected information or data by using public cloud services or tools (e.g. online file hosting services or instant messaging tools), or use communication tools or network services in public places to process any protected information or data;
- Click an hyperlink or open an attachment of an suspicious email;
- Browse untrusted websites;
- Use, distribute, or crack any copyright-protected materials, such as computer software, audio-visual products, and works, without the consent of the copyright owner.

3.4 Research project potentially violating this policy:

- Research on wireless network technology (if it would cause interference to the signal of the university's wireless network, users shall obtain comment from ICTO first);
- Research on new technology of cellular base stations must comply with the laws of Macao, users are recommended to seek legal advice before proceeding.

4. Major applicable laws of Macao and the University's policies:

- Law on Combating Computer Crime
- The Macau Cybersecurity Law
- Personal Data Protection Act
- Electronic Governance (Governação electronica)
- Privacy Policy, UM
- University Policy on Use of Computer Software within Campus, UM
- Guidelines for User Account and Password, UM
- Other applicable laws against criminal behaviors on Internet, and other University's policies and guidelines

For relevant applicable laws, policies and guidelines, please refer to https://icto.um.edu.mo/infosec.

5. Consequences of breach

In the event of a breach of this policy, ICTO may, in its sole discretion, suspend or terminate all rights of users to use the information and communication facilities and services. The University may also take disciplinary action or other appropriate measures. If it involves illegal activities, the user may take the legal responsibility.

(The University reserves the right of final interpretation of this policy.)