澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

University of Macau

Personal Data Collection Statement

(Monitoring of E-mail and Internet Access)

This statement explains the policies of the University of Macau (hereinafter known as "UM") regarding the use of UM provided computing facilities for sending/receiving e-mail or accessing the Internet.

1. Regulation on sending/receiving e-mail or accessing the Internet

Owing to the need of operation, UM provides facilities to employees, students and other personnel to receive / send email or access the Internet with purpose of learning and teaching or academic or daily work.

UM would allow its employees, students or other personnel to use the above-mentioned facilities for personal reason under the following situations:

- In principle: Not affecting the operation of UM, not affecting individual or other personnel work, teaching activities, and not causing any adverse impact on the UM interests, not violating the law.
- To comply with the Acceptable User Policy - ICTO Computing Facilities, Campus Network and Internet. (Please refer to user document reference number 10-00003 for details**)**
- In general, employees should handle personal matters during his/her own leisure/break time if the above-mentioned facilities are being used.

When accessing e-mail for personal matters, employees, students or other personnel should add a sign 【**PRIVATE**】 to the e-mail subject or put the private e-mails to a

folder namely 【**PRIVATE**】.

When accessing e-mail, employees, students and other personnel should **not** conduct the following activities:

- To provide and spread offensive, obscene, malicious, false contents, abusive language or other message falls under the category as illegal or criminal act.
- To disclose UM confidential matters or sensitive information without UM authorization;
- Using the name of UM to perform unrelated activities to his/her scope of UM duties or studies;
- To perform an illegal practice.

When accessing internet, employees and students should **not** conduct the following activities:

- To access offensive, obscene website and web pages (exclusive of academic purpose);
- To download and/or install unauthorized software to UM computer system without UM authorization;
- To download or spread UM confidential matters or sensitive information without UM authorization;
- To download or spread offensive, obscene, malicious, false contents, abusive language or other message that may fall under the category as illegal or criminal act.
- To perform an illegal practice.

2. Purpose of monitoring of e-mail and Internet access

UM conducts monitoring of email and Internet access, with the following aims and objectives:

- To ensure service quality;
- Information security;
- To appraise employees' and students' performance/behaviour.

3. Personal data collected from monitoring of E-mail and Internet access

Due to the need of monitoring, UM will use some computing software and related technology for recording the below mentioned data and content stored in the UM server:

- The email addresses, date, time, subject and content of users' all incoming/outgoing emails;
- The access time, web pages, and information that they have delivered to or received from Internet.

4. Usage of personal data collected from monitoring of E-mail and Internet access

In order to ascertain the service quality and to appraise employees' performance, UM reserves the right to access employees' e-mails in UM email systems, excluding those emails with sign **【PRIVATE】** in the email subject and the e-mails placed in the **【PRIVATE】** e-mail folder. To appraise employees' performance, UM reserves the right to check the access time and web pages that they have accessed on Internet.

In case of information security investigations, disciplinary investigations or criminal investigations, or under the circumstances as required by law, UM reserves the right to access all e-mails of employees, students or other personnel in UM email systems, including those with a sign **【PRIVATE】**in the email subject and the e-mails placed in the**【PRIVATE】** e-mail folder, as well as the access time, web pages, and information that they have delivered to or received from the Internet..

5. Authorized personnel access to the data collected/processed by monitoring

- UM Network System Administrators are authorized to access the related records stored in UM servers, but cannot read the content of email, the web pages accessed, and information that they have delivered to or received from Internet. Only the person who is in charge of UM and the designated personnel have right to access all

records and content. All UM staff have the obligation to observe the rules set in this Statement and to keep all the data confidential.

- In case of disciplinary investigations, the relevant data may be transferred to the personnel who are responsible for disciplinary investigations.
- In case of criminal investigations, and when it is mandatory as required by law, the data may be passed on to law enforcement authorities, judicial authorities or other competent institutions.

6. Data Retention Period

The above-mentioned data will generally be retained for less than three months. In case of criminal investigations, violating the university's regulations and when it is mandatory as required by law, the relevant data may be retained until it is passed on to authorities or institutions stated in point 5, or one month after the verdict of the trial, or even longer time upon the request of the authorities or institutions concerned.

7. Consequences of Violation

Any person who violates this Statement will be penalized accordingly, including the possibility of dismissal for staff, and the possibility of disciplinary punishment for students.

8. Rights of users

In accordance with the law, users have the right to information, the right of access and the right to object. The request for exercising the right of access has to be done in writing, subject to a reasonable fee.