PAMANTASAN NG LUNGSOD NG MAYNILA

(University of the City of Manila)
Intramuros, Manila

Board of Regents
Office of the Secretary

Special Meeting
Board of Regents

President Ramon Magsaysay
Entrepreneurial Center

07 September 2016

Board Resolution No. 4107

"Be it **RESOLVED,** as it is hereby **RESOLVED,** to APPROVE the implementation of the Acceptable Use Policy in the utilization of Information and Communications Technology (ICT) systems, assets, facilities and resources; to promote responsible, ethical, legal and secure use of ICT by all members of the PLM community; and to confirm the University's responsibilities in connection with accessing such information."

(Annex 5.5 of the Special Meeting is an integral part of this Resolution)

BENJAMIN I. ESPIRITU
Chairman

MA. LEONORA V. DE JESUS
Vice-Chairman

RAMON S. BAGATSING, JR.
Member

ESTRELLITA P. BAUTISTA
Member

BIENVENIDO E. LAGUESMA
Member

TERESA AQUINO-ORETA
Member

WILFREDO E. CABRAL
Ex-Officio Member

Attested/Certified by:

VITTO A. KINTANAR
University and Board Secretary

Copy Furnished:

Board of Regents
Office of the University President
Office of the Executive Vice-President
Office of the V ice-President for Academic Affairs 10-28-16
Office of the Vice-President for Administration
Office of the Vice-President for Finance and Management 10-28
Office of the Vice-President for Public Affairs - 10/28/16
Office of the University Legal Counsel 10-28-16
Information and Communications Technology Office
File

PAMANTASAN NG LUNGSOD NG MAYNILA
(University of the City of Manila)
Information & Communications Technology Office
Office of the Director and Operations Management Head

MEMORANDUM for the UNIVERSITY PRESIDENT (CSW-ICTO-2016-0811-01)

FOR : **Dr. MA. LEONORA V. DE JESUS**
University President

DATE : 2016 August 11

FOR APPROVAL	The implementation of the Acceptable Use Policy in the utilization of ICT assets
References/ Annexes	Annex A: 7th ITSC Minutes of the Meeting on 2015 Dec 18 Annex B: 8th ITSC Minutes of the Meeting on 2016 May 02
Background	The University has adopted on 2014 December 19 its Information Systems Strategic Plan (ISSP). It prescribed major Information and Communications Technology (ICT) initiatives from 2015 to 2018, through the approval by the Information Technology Steering Committee (ITSC) which is chaired by the University President. Guided by this enterprise development framework, and in support of its vision-mission-objective (VMO) statement, the University acquires, develops, and maintains computers, computer systems and networks. These ICT resources sustain the educational, instructional, research, administrative and community activities of the University. The use of these ICT assets, facilities and resources for university-related purposes is a privilege that is extended to the members of the PLM community. A user of these ICT resources and its services has a privileged access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is of high import for its authorized users to behave in a responsible, ethical and legal manner. During the 7th ITSC Meeting on 2015 Dec 18, the Acceptable Use Policy (AUP) was presented before the ITSC members, and was subsequently endorsed to the VP for Legal Affairs for legal clearance before the ITSC may act. During the 8th ITSC Meeting on 2016 May 02, the AUP, as previously cleared by the VPLA, was recommended for approval. To give ample time for the VPs to study the matter, the approval was deferred. No objection was interposed against the OULC-cleared proposed policy.
Analysis	This policy aims to provide general guidelines in using the ICT systems, assets, facilities and resources of the University. It intends to articulate and promote the responsible, ethical, legal, and secure use of ICT by all members of the PLM community and to confirm the University's responsibilities in connection with accessing such information.
Recommendation	The Acceptable Use Policy (AUP) is recommended for approval by the Board of Regents.

Recommending Officer:	**Recommending Approval:**	**Recommending Approval:**	**Recommending approval by the Board:**	
Date:	Date:	Date:	Date:	Date:
GARRY ERWIN DE GRACIA *Acting Asst. VP & Director, ICTO*	**Prof. JOSE A. ~~CELERIO~~ SILERIO** *Acting Vice President, ICTO*	**Dr. NELSON J. CELIS** *Executive Vice President*	**Dr. MA. LEONORA V. DE JESUS** *University President*	

SEP 07 2016

ANNEX 55
Special Board Meeting

PAGE 1 OF 19 PAGES

PAMANTASAN NG LUNGSOD NG MAYNILA

University of the City of Manila
Intramuros, Manila

Acceptable Use Policy for ICT Assets and Resources

Documentation

Version 1.0

August 2016

ANNEX 5.5
Special Board Meeting

Document Number: AUP-01

SEP 07 2016 PAGE 2 OF PAGES

Document Review and Approval

Revision history:

Version	Authors	Date	Signature	Description
1.0	**Ms. Nerrisol B. Solis** **Mr. Reynaldo R. Medina** **Prof. Leisyl M. Ocampo** **Engr. Jonathan S. Siena** **Engr. Erwin D. Marcelo**			The AUP for 2016-2017 as developed by the ICTO's 5 Sections.

This document has been reviewed by:

Reviewer	Date	Signature
Engr. Garry Erwin N. de Gracia		

This document has been approved by the ITSC:

	Name	Date Reviewed/ Approved	Signature
1	**Engr. Denvert C. Pangayao** Acting University Registrar		
2	**Atty. Vito A. Kintanar** University Secretary		
3	**Atty. Rufino V. Abuda** Acting Vice President for Legal Affairs		
4	**Dr. Cecilia J. Sabio** Acting Vice President for Academic Affairs		
5	**Mr. Manuel I. Inserto** Acting Vice President for Finance and Planning		
6	**Col. Elias C. Juson Jr.** Vice President for Administration		

7	**Engr. Jose A. Silerio** Acting Vice President for ITC		
8	**Dr. Nelson J. Celis** Acting Executive Vice President		
9	**Dr. Leonora V. de Jesus** University President		

Table of Contents

ANNEX 5.5
Special Board Meeting
SEP 07 2016
PAGE 5 OF 19 PAGES

Background

The University has adopted on 2014 December 19 its Information Systems Strategic Plan (ISSP), which prescribed major Information and Communications Technology (ICT) initiatives from 2015 to 2018, through the approval by the Information Technology Steering Committee (ITSC) which is chaired by the University President. Guided by this enterprise development framework, and in support of its vision-mission-objective (VMO) statement, the University acquires, develops, and maintains computers, computer systems and networks. These ICT resources sustain the educational, instructional, research, administrative and community activities of the University. The use of these ICT assets, facilities and resources for university-related purposes is a privilege that is extended to the members of the PLM community. A user of these ICT resources and its services has a privileged access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is of high import for its authorized users to behave in a responsible, ethical and legal manner.

Generally, acceptable use means respecting the rights of other users, the integrity of the physical facilities and data, and all pertinent license and contractual agreements. A violation of this Acceptable Use Policy authorizes the University to take disciplinary action, including the restriction and possible loss of network privileges. A serious violation may result in more serious consequences, up to and including suspension or termination from the University, as the rules may provide. All users are also subject to national laws and local ordinances governing many interactions that occur on the Internet.

SECTION I. PURPOSE

This policy aims to provide general guidelines in using the ICT systems, assets, facilities and resources of the University. It intends to articulate and promote the responsible, ethical, legal, and secure use of ICT by all members of the PLM community and to confirm the University's responsibilities in connection with accessing such information.

SECTION II. GENERAL POLICY STATEMENT

The use of ICT assets, facilities and resources, especially those provided by PLM through public funds, entails the responsibility to use these resources in an efficient, ethical and lawful manner consistent with the VMO statement of PLM. To this end, every user must use the University's ICT resources in a responsible, professional and ethical manner, and within legal and proper boundaries.

SECTION III. SCOPE AND APPLICATION

This policy shall apply to all users of ICT assets, facilities and resources, whether affiliated with the University or not, including personnel employed or contracted by PLM, its offices, as well as scholars and student assistants.

This policy covers the proper use of the ICT assets, facilities and resources of the University which include, but are not limited to, all ICT equipment, software, data in all formats and media, accessories, networking facilities and services, whether central or remote, including

information retrieval services for the public, such as web browsing through the worldwide web (www) and file transfer (upload/download).

For purposes of implementing this policy, any other equipment, computer unit, or external network, when attached to, or used to access and/or interact with any component of the ICT assets, facilities and resources of the University, regardless of the ownership, shall also be considered part of the University's ICT system.

SECTION IV. DEFINITION OF TERMS

The definition of terms herein provided may be updated from time to time to include new equipment, technology and services, as well as new perspectives and development in the use of ICT assets, facilities and resources.

For purposes of these guidelines, the following terms and phrases shall be understood as follows:

Access - means to connect to a computer system or server that enables one to get online and to browse and retrieve data, and communicate electronically through an internet service provider (ISP) via a modem or through network such as a Local Area Network (LAN).

Authorized Users - refer to all employees, consultants, temporary workers, scholars, and other persons authorized by the University to use its computer resources, including, but not limited to, the following:

1. current employees of the University, regardless of the status of the appointment;

2. enrolled or current scholars of the University; and

3. those whose access and usage are specifically authorized to use a particular computer or network resource by the University.

Electronic Mail (E-mail) – refers to electronically transmitted mail.

ICT Assets, Facilities and Resources (or ICT Resources, for brevity) – include, but are not limited to, all ICT equipment, software, data in all formats or media, accessories, networking facilities, and services, whether central or remote, including information retrieval services such as remote login, file transfer, electronic mail, and news groups. The internet is a way of connecting existing computer networks that greatly extends the reach of each participating system.

Local Area Network (LAN) – refers to a network that connects computers in a small pre-determined area like a room, building, or a set of buildings. LANs can also be connected to each other via telephone lines or radio waves. Workstations and personal computers in an office are commonly connected to each other via LAN. These allow them to send/receive files and/or have access to the files, data and services. Each computer connected to a LAN is called a node.

Minimal Additional Expense – is a user's allowable yet limited incidental personal use of the University's equipment such as when the University is already providing equipment or services and the use of such equipment or services shall not result in any additional expense to the University, but only normal wear and tear or small amounts of electricity, ink, toner or paper. Minimal additional expense include occasionally making a few photocopies or use of a computer printer to print a few pages of material not intended for personal financial or other gains; infrequently sending personal e-mail messages, or limited use of the unrestricted Internet pages for personal purposes during breaks.

Such use shall be subject to the recommendation of the dean of the college or the head of the office, and the approval of the vice president concerned, so long as those activities are legal and do not violate University policies, contractual obligations, the safety, security, privacy, reputational, and intellectual property rights of others, or such other restrictions provided by law or policies. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

Network – refers to a communication system that links two or more computers. It can be as simple as a cable strung between two computers a few feet apart or as complex as hundreds of thousands of computers around the world linked through fiber optic cables, phone lines and satellites or other electronic means.

Official PLM Access – refers to the usage in the performance of work-related duties and/or officially authorized activities.

Personal Use – refers to the use other than official PLM access.

Private Files – refer to information that a user would reasonably consider as private. These include the contents of electronic mail boxes, private file storage areas of individual users, and information stored in other areas that are not public even if no measure has been taken to protect such information.

Privilege – means that employees may use a University property to create a more supportive work environment. However, these policies shall not create a right to use University office and equipment for non-official purposes. The privilege shall not extend to modifying such equipment, including loading personal software or making configuration changes.

User Account – refers to a unique identifier which may consist of an account name and a password. This allows the account holder to access network facilities and resources either through a local area network (LAN) or the Internet.

SECTION V. ICT ASSETS, FACILITIES AND RESOURCES MANAGEMENT

To comport with international standards, the centralization of all technical concerns to the ICT Office (ICTO) was adopted by the University through PAO No. 2013-13. The authority and the

responsibility to install, manage, maintain, upgrade, repair or modify any hardware or software rest solely on ICTO.

Similarly, to ensure effective control of ICT resources, the President has approved under CSW-ICTO-2015-0825-01 the centralization of the management of all administrative user accounts to ICTO. Further, all servers and institutional data of PLM shall be centralized in its Data Center that is managed by ICTO, pursuant to the President's memorandum MC-2015-0223-01. Finally, the President's memorandum No. 44, s. 2015 has assigned the ICTO as the Project Management Office for all IT projects and requirements, so as to centralize all ICT needs under one roof. These were reiterated under Pamantasan Administrative Order No. 58, s. 2015.

V.1 The ICT assets, facilities and resources

The ICT assets, facilities and resources include, but are not limited to, the following:

1. All cablings used to carry voice and data;

2. All devices to manage or control the flow of voice and data communication, such as hubs, routers, firewalls, switches, and the like, including the Private Automatic Branch Exchange (PABX);

3. All central processing units, monitors, storage devices, modems, network cards, memory chips, keyboards, cables and accessories;

4. All computer software including applications, utilities, tools, and databases; and

5. All output devices including printers, fax machines, CD writers, and similar devices or equipment.

V.2 Responsibilities

The ICTO shall implement a base configuration for all ICT equipment, corresponding to the responsibility of the authorized user, before deploying the same to the latter. Further, the ICTO shall have the following duties and responsibilities in implementing these policies:

1. Software Upgrade. The following are considered modifications: installing patches provided by the software supplier or downloaded from the internet; installing anti-virus; installing new versions of the operating system or any productivity applications, e.g., word processing or spreadsheet applications.

2. System Inspection and Deletion. The ICTO or its authorized personnel may delete files or software that are unauthorized, provided that this deletion or modification is done in the presence of the user, or his immediate supervisor.

3. Hardware Maintenance. The ICTO or its authorized personnel is the only authorized entity to inspect any ICT equipment. Equipment and software services under warranty shall not be altered or inspected by unauthorized personnel.

4. Equipment Movement. The ICTO or its authorized personnel is the only entity permitted to move or transport equipment from one location to another, except for mobile computers such as notebooks, laptops, and wireless user devices.

5. Authority to Secure Equipment and Services. The ICTO or its authorized personnel shall have the responsibility to maintain the security of Internet resources against intrusion and destruction. It is tasked to research on security and service continuity/disaster recovery to maintain a high degree of reliability of the systems.

SECTION VI. USER RESPONSIBILITY

Users are individually responsible for the appropriate use and security of all ICT resources assigned to them, and are accountable to the University for all use of such resources, including misuse or theft by others, as well as for avoiding any use that interferes with others' legitimate access to and use of such ICT resources. Further, users bear the responsibility for knowing and complying with applicable laws, policies, and rules.

In using or accessing ICT resources, users must comply with the following guidelines:

VI.1 System Access Requirements

Access privilege through a user account shall be extended to all authorized users of the University. An authorized user shall be given a unique login name and password to gain access to the University's ICT resources. He may use or access only the computers, accounts and files for which he has been granted authority. He must not attempt to access restricted portions of the network, an operating system, security software or other applications without appropriate authorization by the system owner or the ICTO.

User ID/Name. The ICTO shall issue a standardized naming convention and format of username for the provisioning of Official PLM Accounts to authorized users.

Responsibility for Passwords. Users shall be responsible in safeguarding their passwords for access to the computer system. They must exercise reasonable effort to protect their passwords and to secure resources against unauthorized use or access. Individual passwords shall not be printed, stored online, or given to others. A password is the key to the legally binding electronic signature and users shall be responsible for all transactions and activities processed or made using the same. No user shall access the computer system by using another user's account, nor attempt to capture or guess other users' passwords.

Limited Exception. Office heads of the University may allow the use of the ICT resources beyond the scope of this access policy, upon prior clearance with the ICTO Director and approval of the University President, under the following conditions:

1. The intended use serves a legitimate office interest;

2. The intended use is for the user's educational and professional development;

3. The use and time to access will be properly logged and reported to the ICTO including the account used for such purpose. No new username or password shall be issued during such use; and

4. The authorized user shall be held accountable for damages that may arise due to the improper use of the password and the ICT resources.

VI.2 User Limitations

Accessing Other User's Files. A user shall not access, alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy such particular file. Users shall not use the computer system to "snoop" or pry into the affairs of other users by reviewing the files and e-mails.

Accessing Other Computers and Networks. A user's ability to connect to other computer systems through the network or modem shall not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems. A user must not use the University's ICT resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

Use of Other Public Information Services. Each user is responsible to ensure that the use of outside ICT resources and networks, such as the internet, shall in no way compromise the security of the University's ICT resources and networks. This duty includes taking reasonable precautions, as provided for but not limited to those stated in this policy, to prevent intruders from accessing the University's network without proper authorization, and to prevent the introduction and spread of viruses.

VI.3 Fair Use and Share of Resources

The ICTO, which manages and maintains computers, network systems and servers, among others, expects to maintain an acceptable level of performance and shall assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, institutional servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the PLM community is explicitly forbidden.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

VI.4 Security Guidelines

Ownership and Right to Monitor. All ICT resources as defined herein are owned by the University, which is a public entity. For this purpose, the University reserves the right to monitor, log and inspect all network-based activities. The user shall be responsible to surrender all passwords, files, and/or other resources, and to provide appropriate access to university-related information even on the user's own personal computer, laptop, cell phone, or other electronic devices, if requested to do so by proper authorities, or persons authorized by the University, and preferably in the presence of the user's office head or persons properly authorized by the University.

The University reserves the right to hold the users liable for damages caused by the user's failure to protect the confidentiality of his/her password in accordance with these guidelines.

Reporting of Troubles or Problems. Users shall report to the ICTO such suspected abuse, damage to, or problems with their files. Failure to cooperate may result to the cancellation of access privileges, and/or other disciplinary actions. Users shall fully cooperate with system administrators in any investigation of system abuse.

Contact Person or Unit. Trouble reports and similar concerns shall be promptly reported to the ICTO so that appropriate action can be taken to address the problem.

System Managers/Administrators to Employ Monitoring Tools to Detect Improper Use. Electronic communications may be disclosed within an agency or department to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access electronic communications.

File Storage. All office files shall be stored in the common storage area for said office, in accordance with the supplemental policy that would be issued by the ICTO.

Encryption. To maintain the integrity of institutional data or files, depending on data classification standards, an adequate level of encryption shall be observed.

Accountability and Turnover. ICT resources shall not be moved from an office location, except for mobile devices under a user's accountability. Files and data generated by the office shall not be transmitted or brought out by any user. Proper equipment turn-over by any user for whatever cause, such as transfer of office or resignation, shall entail the proper endorsement of all data stored in the equipment in favor of the immediate supervisor.

SECTION VII. VIRUS PREVENTION

VII.1 General Guidelines

Each user shall take reasonable precautions to ensure that he or she does not introduce virus into the University's computer network. All materials received on allowed external storage devices and media, and all materials downloaded from the Internet or from computers or networks that do not belong to the University must be scanned for viruses before being placed into the computer system.

VII.2 Authorized Anti-Virus Program

No anti-virus programs are allowed to be installed in any computer, whether stand-alone or networked, except those prescribed by the ICTO Director or his authorized personnel.

Installation. Users may install these anti-virus programs subject to instructions, which shall be made available by the ICTO or the authorized personnel. The installation can be made through the network.

Announcements and Updates. The ICTO shall be responsible for the routine updating of the anti-virus program located in the servers and at the gateway. The ICTO shall periodically give

advisories to all users to keep them informed of the best practices to combat viruses at the endpoint level.

VII.3 User Responsibility in Anti-Virus Protection

The user shall be responsible to keep his or her anti-virus programs updated regularly, at least every week, using only prescribed programs by the ICTO.

Accessing the Internet. To ensure security and avoid the spread of viruses, users authorized to access the Internet through a computer attached to the University's network shall do so through an approved internet firewall.

SECTION VIII. INTERNET USE POLICY

The Internet can be a valuable source of information and research. Thus, certain users or offices may be provided with access to the Internet to assist them in the performance of their jobs. Use of the Internet, however, must be tempered with good judgment in order to maximize its allocated time of usage, without creating unnecessary network traffic. Hence, visiting improper sites and downloading of videos and audio, media streaming are prohibited, while excessive web browsing is discouraged.

VIII.1 Authorized Internet Connection

Only authorized personnel are allowed to have an Internet access or connection to their computer. This account, approved by the ICTO Director based on applicable guidelines, is provided to the users so as to facilitate the task of gathering information. Direct connection to the Internet without proper approval from the ICTO is strictly prohibited. Users found violating this policy may be held responsible for any security breaches and possible virus propagation on and intrusion to the network. The use of prepaid internet connections and such other modes without prior authority from the University, as approved by the ICTO, is strictly prohibited.

The University connects authorized users to network services and its servers with important institutional data through a campus-wide LAN. Authorized users shall best access the Internet by using computers that are not connected to the LAN of the University to avoid the spread of viruses that may be downloaded from the Internet. A user may access the Internet using a computer that is connected to the LAN of the University, provided that a written approval is secured from the Office of the President, duly cleared and endorsed by the ICTO. A user accessing the internet through a computer connected to the LAN without such approval may be held liable for security breaches or virus intrusion that may occur in the network.

VIII.2 Remote Access Privileges

The University, through the ICTO and subject to the availability of resources, may provide a remote connection to authorized users to the network resources and to the Internet, subject to the following conditions:

User-maintained Equipment. The authorized user shall be responsible for the computer, modem and phone line, and all accessories that are used to connect to the University's ICT resources and the Internet.

User Account and Password. Authorized users shall be provided a user account and password to connect to the remote services. The user shall be responsible to keep this user account, and all information regarding remote network access, confidential. Propagating remote access details is considered a security breach and shall constitute a ground for administrative sanction.

SECTION IX. EMAIL AND OTHER INTER-OFFICE ELECTRONIC COMMUNICATION AND ACCESS FACILITIES

IX.1 Users' Duty of Care

The University shall provide Official PLM Accounts to the members of the PLM Community, which shall include e-mail services. Users shall ensure that electronic communications are truthful and accurate. Reasonable care in drafting e-mail and other electronic communications shall be observed as with any other written communication. Any document created or stored in the computer system may be subject to the review and inspection of ICTO as herein authorized by the University.

IX.2 Privacy and Security vis-à-vis University Obligations

Despite measures by the University to secure its ICT resources, users must never consider electronic communications to be private or secure. It is the responsibility of the users to practice "safe computing" by establishing appropriate access restrictions for their accounts.

Employees are granted use of electronic information systems and network services to conduct University business. While every effort is made to insure the privacy of users and while the University does not routinely monitor or limit information contents transmitted through the campus network, the University bears significant and increasingly complex legal, operational and compliance-based duties, which require it, and thus reserve the right, to invariably preserve and secure custody of information from users' accounts and associated storage media without accessing or searching the content. There may be instances that the University may be required to access, search and review the content of user electronic information, and disclose relevant portions to others who are duly authorized to receive it, or as permitted by law or regulation, in order to uphold contractual obligations, to determine compliance with and enforce University policies and legal duties, to gather information relevant to pending or potential litigation, and to maintain the integrity and security of ICT systems.

These include, but are not limited to:

1. Investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that the University is not subject to claims of institutional misconduct.

2. Others often require access to the departed employee's account to ensure continuity of business operations, research, teaching and educational programs.

Likewise, the University often bears clear legal duties to preserve, review and, as appropriate, disclose data generated and/or maintained by the users of the University's ICT resources.

Access to files on University- or privately-owned equipment or information shall only be approved when there is a valid reason to access those files. Authority to access user files may only come from the ICTO Director in conjunction with requests and/or approvals from senior members of the University.

SECTION X. PROPER USE AND PROBIHITED ACTS IN THE UTILIZATION OF THE ICT ASSESTS, FACILITIES AND RESOURCES

X.1 General Principles in Proper Use

A user may access only those services and parts of the ICT resources of the University that are related to or consistent with his or her duties and responsibilities. The ICT resources of the University shall only be used in accordance with their authorized or specified purpose.

X.2 Prohibited Uses and Acts

The following are considered violations in the utilization of the ICT resources:

1. Use of the University ICT Resources for Criminal Activities as defined under the Revised Penal Code and Other Special Laws, including but not limited to the E-Commerce Act of 2000 and the Intellectual Property Code.

2. Use of Copyrighted Material Without Attribution. These include, but are not limited to, copying, reproduction, dissemination, distribution, use importation, removal, alteration, substitution, modification, storage, uploading, downloading, communication, publication or broadcasting of copyrighted material not property attributed; and infringement of intellectual property rights belonging to others through the use of telecommunications networks, which is a criminal offense under Section 33(b) of the Electronic Commerce Act.

Section 33 of RA 8792, the E-commerce law, states "Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunications networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years."

3. Morally Offensive and Obscene Use. Accessing, downloading, producing, disseminating, or displaying material that is offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or

otherwise unlawful or inappropriate shall not be sent by e-mail or other forms of electronic communication (such as messaging, bulletin board systems, news groups, chat groups) or displayed on or stored in the University's ICT resources. A user who encounters or receives this kind of material shall immediately report the incident to their supervisors.

A user shall be professional and respectful when using the ICT systems to communicate with others; the use of ICT resources to libel, slander, or harass any other person is not allowed and could lead to discipline, as well as legal action by those who are the recipients of these actions.

4. Hacking, Spying or Snooping. Accessing or attempting to gain access to archives or systems of the University that contain, process, or transmit confidential information, as well as accessing, or attempting to access, restricted portions of the system, such as e-mail lists, confidential files, password-protected files, or files that the user has no authorization to open or browse shall be prohibited and shall carry the penalties under Section 33 of the E-commerce Law and shall be subjected to Administrative Sanctions independent of the penalties provided under the E-commerce Law.

Further, authorized users shall not exceed their approved levels of access, nor shall they disclose confidential information to unauthorized persons.

5. Plagiarism. Prohibited acts include, but are not limited to, copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the consent or permission of the owner or author of the work; submitting the shared file, or a modification thereof, as one's individual work, when the work is collaborative work, or part of a larger project; and such other related acts of cheating.

6. Uses for Personal Benefit, Business or Partisan Activities

a. Commercial Use. Use of the ICT resources of the University for commercial purposes, product advertisement, peddling of merchandizes and for personal profit, unless allowed under written institutional policies consistent with national or local entrepreneurial principles.

b. Personal Entertainment. Use of ICT resources for personal entertainment such as watching movies, and Internet access and use of other services beyond official matters, except for mobile devices used in the comfort of their homes or other secured places outside of the University.

c. Use for any partisan activities. Use of ICT resources of the University for religious or political lobbying, for disseminating information or gathering support or contributions for social, political or cause-oriented group, which are inconsistent with the activities of the University.

7. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the ICT Assets, Facilities and Resources. These include, but are not limited to:

a. Virus infection due to connection of the ICT resources of the University to any computer unit or external network;

b. Acts that attempt to crash, tie up, or deny any service on the ICT resources of the University, such as, but not limited to: sending of repetitive requests for the same service (denial-of-service); sending bulk mail; sending an email with very large attachments such as videos and pictures; sending data packets that serve to flood the network with bandwidth; and downloading of unusually large files like movies through any means;

c. Concealment, deletion, or modification of data or records pertaining to access to the ICT resources of the University at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use; and

d. Concealment of identity, or masquerading as other users when accessing, sending, receiving, processing or storing through or on the ICT facility and resources of the University.

8. Unauthorized Disclosure. Copying, modification, dissemination, or use of confidential information such as, but not limited to: mailing lists; employee directories and circumstances of any sort; operations data; research materials, in whole or in part, without the permission of the person or body entitled to give it, as well as searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the permission of the owners of the said files, programs or passwords.

9. Distribution or Dissemination of Prohibited Materials, as considered under this policy, include, but are not limited to, the following:

a. Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;

b. Any material that enables others to gain unauthorized access to a computer system. These may include instructions for gaining such access, computer code, or other devices.

c. Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and

d. Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

10. Improvident Use of Resources. Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to:

a. sending mass mailings or chain letters;

b. spending excessive amount of time on the Internet;

c. playing online or network and local games;

d. engaging in online chat groups;

e. printing multiple copies of documents;

f. printing unnecessary documents, files, data, or programs;

g. repeated posting of the same message to as many newsgroups or mailing lists as possible, whether or not the message is germane to the stated topic of the newsgroups or mailing lists targeted;

h. sending large unsolicited files to a single e-mail address or other electronic communications facilities;

i. use of peer-sharing sharing or other means to download and upload movies;

j. or otherwise creating unnecessary network traffic.

11. Unauthorized Repair of ICT Assets, Facilities and Resources. Only the ICTO personnel or personnel allowed by the University (suppliers, contractors, and other similar outsourced agencies) are authorized to repair, open, remove, disconnect or check the University's ICT resources. Users are prohibited to open, remove, disconnect or detach any peripherals or devices. Users who violate this policy may be held liable for any loss or damage to such.

SECTION XI. POLICY AUGMENTATION AND UPDATING

This Policy may be augmented or updated by the ICTO Director, upon Presidential approval, as the need arises, especially if the policy updates, supplemental policies or procedural guidelines are essential in refining the same or aligning the needs with the service capability and output requirements, and other indispensable imperatives.

Although ICTO may promulgate supplemental policies regarding acceptable use and user privacy expectations, those policies cannot diminish University responsibilities or reasonable user privacy expectations as herein before set forth.

SECTION XII. INCORPORATION OF OTHER RULES

All pertinent provisions of law, Civil Service Rules and issuances of the University governing or regulating the conduct of public officers and government employees and the use of ICT in government service are deemed incorporated into these guidelines. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

SECTION XIII. PENAL PROVISIONS

Users who violate this Policy, which violation shall be considered a grave offense, shall be subject to penalties and disciplinary action as applicable rules may provide, and may be a ground for termination of its relationship with the University.

SECTION XIV. EFFECTIVITY

This Policy shall take effect immediately upon approval by the University President and the Board of Regents and shall remain in force unless sooner amended or revised.