APPROVED ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY (IT) RESOURCES OF THE UP SYSTEM

Section 2. Basic Standards

a. The same standards and principles of intellectual and academic freedom developed for university libraries shall be applied to material received from the network. The same standards of intellectual and academic freedom developed for faculty and student publication in traditional media shall be applied to publication in computer media.

b. As constituents of the academic community, faculty, students, and academic and non-academic staff should be free, individually and collectively, to express their views on

Section 3. Definitions

a. *Agreement Form* means document in which the user undertakes to comply with this Policy. The form may be electronic.

b. *Confidential information* means data or information which on its face is not intended for unrestricted dissemination. Examples include student records, examination archives, proprietary technical information, disciplinary case records, administrative records, and the like.

c. *Document* when used in this Policy shall refer both to the paper and its electronic format.

d. *Information Technology System* or *IT System* includes computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, and software, databases and other data files that are owned, managed, or maintained by any unit of the University of the Philippines.

   For purposes of 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 IT System may also be considered part of the IT System.

e. *Private files* means information that a user would reasonably regard as private. Examples 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.

f. *System and Network Administrator* means a person designated to manage the particular system assigned to her/him, to oversee the day-to-day operation of the system, or to preliminarily determine who is permitted access to particular facilities and resources of the IT System, whether hired on a temporary, contractual or permanent basis.

g. UP SYSTEM means the University of the Philippines System and all its constituent units.

h. *User* means any person, whether authorized or not, who makes any use of the IT System or any of its components by any means or from any location.

Section 4. Scope And Applicability

a. General Coverage.

i. This Policy applies to all facilities within the IT System and all its users.

ii.

Section 5. General Responsibilities

a. General Responsibilities of Users.

In general, users of the IT System must:

i. use the IT System only for its intended purpose, and refrain from misusing or abusing it;

ii. maintain the integrity, reliability, availability, confidentiality and efficiency of computer-based information resources;

iii. refrain from seeking to gain unauthorized access or exceed authorized access;

iv. respect software copyright and licenses and other intellectual property rights;

v.

Section 6. Appropriate Use

a. Appropriate Use

Users may only use the IT System for its authorized purposes, which is to support the research, education, clinical, administrative and other functions of the UP SYSTEM. The particular purposes of any of the components of the IT System, as well as the nature and scope of authorized incidental personal use, may vary according to the duties and responsibilities of a user.

b. Proper Authorization

Users may access only those facilities and components of the IT System that are consistent with their authorization coming from competent authorities.

c. Specific Proscriptions on Use

The following categories of use of the IT System are considered prohibited and/or inappropriate:

i. Uses Contrary To Law

1. **Unlawful use.** Users may not use the IT System for any activity that is contrary to any law or administrative rule or regulation, or to encourage any such unlawful activity. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal

2. **Infringement of protected material.** Users must not infringe on the copyright and other property rights covering software, databases and all other copyrighted material such as text, images, icons, retrieved from or through the IT System. These acts shall include, but is not limited to, the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, unloading, downloading, communication, publication or broadcasting of such material. Users must properly attribute any material they copy from or through the IT System. Users are reminded that the infringement of intellectual property rights belonging to others through

shall suffer a penalty ranging from suspension for one year to expulsion or dismissal. The penalty shall carry with it permanent withdrawal of all IT privileges.

ii. Uses Inconsistent With The Purposes Of The UP System

1. **Cheating.** Users may not use the IT System to engage in cheating or academic dishonesty. Acts prohibited under this provision include but are not limited to the following:
    a. Copying a computer file that contains another person's work and submitting it for one's own credit;
    b. Copying a computer file that contains another person's work and using it as a model for one's own work;
    c. Collaborating on a work, sharing the computer files and submitting the shared file, ora modification thereof, as one's individual work, when the work is supposed to be done individually; and
    d. Communicating with another person on-line during the conduct of an examination. Violators shall suffer a penalty of suspension for not less than one semester. Students found guilty of cheating shall be barred form graduating with honors, even if their weighted average is within the requirement for graduation with honors.

2. **Political use.** Users may not use the IT System for any partisan political activities. Violators shall suffer a penalty ranging from suspension for one month to one year.

3.

offense shall be expulsion or dismissal. The presence of game software or any part thereof may be presumptive evidence of unauthorized gaming or entertainment.

6. **Use contrary to University policy or contract.** Users may not use the IT

such access for the purpose of concealing identity or to hide unauthorized use. Users may not conceal their own identity or masquerade as other users when accessing, sending, receiving, processing or storing through or on the IT System. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

7. **Prohibited material.** Users may not publish (on mailing lists, bulletin boards, and the World Wide Web) or disseminate prohibited materials over, or store such information on, the IT System. Prohibited materials under this provision 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. This may include instructions for gaining such access, computer code, or other devices. This would effectively preclude displaying items such as 'Hackers Guides', etc.;
    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. Violators shall suffer a penalty ranging from suspension for one year to expulsion.

iv. Uses That Encroach On The Rights Of The Users

1. **Wasteful and destructive practices.** Users may not encroach on others' access and use of the IT System through wasteful and destructive practices such as but not limited to the following:
    a. Sending chain-letters or excessive messages including spamming, either locally or off-campus; violators shall suffer a penalty ranging from suspension for one

d. Using more than one computer terminal at a time, unless specifically authorized

b. Users shall treat as confidential such information which may become available to them through the use of the IT System, whether intentionally or accidentally. Users may not copy, modify, disseminate, or use such information, either in whole or in part, without the permission of the person or body entitled to give it. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.

Section 8. Enforcement Procedures

a. **Monitoring.** The UP SYSTEM or its constituent universities may monitor all use of the IT System at all times as may be necessary for its proper management. Activities on the IT System may be automatically and/or continuously logged. System and network administrators may examine these logs anytime. All logs shall be considered confidential.

b. **Access to Private Files.** The UP SYSTEM may access all aspects of the IT System, including private files, without the consent of the user, in the following instances:

   i. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity, reliability, availability, confidentiality and efficiency of the IT System;
   ii. When such access to the IT System is required to carry out essential business functions of the UP SYSTEM;
   iii. When necessary to avoid disrepute to the UP SYSTEM;
   iv. When there are reasonable grounds to believe that a violation of law or a significant breach of this Policy or any other policy of the UP SYSTEM may have taken place, and that access and inspection may produce evidence related to the misconduct;
   v. When required by law or administrative rules or court order; or
   vi. When required to preserve public health and safety. The UP SYSTEM will access private files without the consent of the user only with the approval of the Chancellor except when an emergency entry is necessary to preserve the integrity, reliability, availability, confidentiality and efficiency of the IT System or to preserve public health and safety. e file g-0.2 .2 (e) - -0.2 (y(.) 0.2 (,c0.2 (l),1rg) -0.2 73.7 (.)) 0.2 (,c0.2 (l),1r440.2 (,c0.

the activities or the files of an individual, he or she shall, within 24 hours of the discovery of the possible misuse, notify the Chancellor or his/her duly designated authority.

ii.

Section 9. Waiver

a. **Loss of Data.** Users recognize that systems and networks are imperfect and waive any claim for lost work or time that may arise from the use of the IT System. The UP SYSTEM shall not be liable for degradation or loss of personal data, software, or hardware as a result of their use of the IT System.

b. **Authorization.** Users recognize that the UP SYSTEM provides access to the IT System only as a privilege and not a right; that they have no right to use it for any purpose other than those directly connected with the work of the UP SYSTEM; and that the UP SYSTEM may take whatever measures it deems necessary to enforce this. Users therefore waive any action they may have against the UP SYSTEM under any law or administrative rule or regulation for any act the UP SYSTEM undertakes under this Policy, specifically including, but not limited to, those acts enumerated under Section 7 hereof.