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

Approved by the Board of Regents on its 1165th Meeting, 31 October 2002.

Section 1. Policy Statement

a. Computers and networks are powerful technologies for accessing and distributing information and knowledge. They are strategic technologies for the current and future needs of the UP SYSTEM.

b. For now, computing facilities and network infrastructure are a costly resource and thus must be used solely for teaching, learning, research, and other officially-sanctioned activities. Also, since these technologies allow individuals to access and copy information from remote sources, users must respect the rights of others, particularly to their privacy and intellectual property. There is therefore a need for rules and regulations to ensure equitable, secure and reliable access to these resources. The following regulations will govern the use of computing facilities, networks and other Information Technology (IT) resources of the University of the Philippines System.

c. These regulations aim to:
    i. ensure an information infrastructure that promotes the basic missions of the UP SYSTEM in teaching, learning and research;
    ii. protect the integrity, reliability, availability, confidentiality and efficiency of the IT resources of the UP SYSTEM;
    iii. establish processes for addressing policy violations and providing sanctions for violators;
    iv. emphasize that the UP SYSTEM shall not be liable for any damages incurred from the use of IT resources and for any claims and suits arising from the unauthorized and irresponsible use of the same;
    v. warn users that use of IT resources for partisan political activities as defined in relevant rules and regulations of the civil service commission or the university of the Philippines, or for any unauthorized commercial purposes is prohibited; and
    vi. notify users of the existence of this Policy.

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 issues of institutional policy and on matters of general interest to the academic body. The constituents of the academic community should have clearly defined means to participate in the formulation and application of institutional policy affecting academic and student affairs. The actions of the constituents of the academic community within the areas of its jurisdictions should be reviewed only through orderly prescribed procedures.

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. All users should be aware of these regulations, and should realize that when using the computers within the UP SYSTEM, they are bound by these regulations. Users may be required to sign a form agreeing to comply with this Policy. However, failure to sign the agreement form will not release users from coverage of this Policy.

b. Local and External Conditions of Use.

i. Individual units within the UP SYSTEM may define additional "conditions of use" for components of the ITSystem under their control.

ii. These conditions must be consistent with this overall policy but may provide additional detail, guidelines, restrictions, and/or enforcement mechanisms. These units will be responsible for publishing the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Copies of these policies should be given to the President, Vice-President for Development, the Intellectual Property Office and the Office of Legal Services.

iii. Where use of external networks is involved, policies governing such use will be applicable and must be adhered to.

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. respect the rights of other computer users; and

vi. be aware that although computing and information technology providers throughout the university are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as safeguarding their account and password, taking full advantage of file security mechanisms, backing up critical data and promptly reporting any misuse or violations of the policy.

Every member of the university community has an obligation to report suspected violations of the Acceptable Use Policy for Information Technology of the U.P. System or any of its units. Reports should be directed to the system and network administrators, Chairs, Deans, Chancellors or the President.

b. General Responsibilities Of System And Network Administrators

i. System and network administrators and providers of university Information Technology resources have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

ii. System and network administrators are expected to treat the contents of electronic files as private and confidential. Any inspection of electronic files, and any action based upon such inspection, will be governed by this Policy, other university rules and all applicable laws.

c. General Responsibilities Of University Administrators

i. To be informed and knowledgeable about these policies

ii. To initiate systematic programs to inform academic and non-academic personnel of these policies

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 the use of telecommunications networks is a criminal offense under Section 33(b) of the Electronic Commerce Act. Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal.

3. **Hacking.** Users may not use the IT System to gain unauthorized access into or interfere with another computer, system, server, information or communication system, or to obtain any access in order to corrupt, alter, steal or destroy any such system or information within such system or to introduce viruses. Users are reminded that all of the foregoing acts constitute the crime of Hacking under Section 33(a) of the Electronic Commerce Act and are punishable by mandatory imprisonment and/or a fine. Violators

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. **Unauthorized Commercial use**
    a. Users may not use the IT System for commercial purposes, except as permitted under other written policies of the UP SYSTEM or with the written approval of a competent authority.
    b. Violators shall suffer a penalty ranging from suspension for one month to one year with fine. If the violator is a student, the fine shall be P1,000.00 or the amount equivalent to the earnings, whichever is higher. If the violator is a faculty member or an employee, the fine shall be one-half of his monthly salary or the amount equivalent to the earnings, whichever is higher.

4. **Personal use.** Users may not use the IT System for personal activities not related to appropriate University functions except in a purely incidental manner. Violators shall suffer a penalty ranging from suspension for one month to one year.

5. **Unauthorized gaming or entertainment.** Users may not play games or use entertainment software on or through the IT System unless authorized in writing by competent authorities. Violators shall suffer a penalty ranging from suspension for one week to one year; provided, that the penalty for habitual

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 System in violation of other policies of the University, or in any manner inconsistent with the contractual obligations of the University. Violators shall suffer a penalty ranging from suspension for one week to one year in addition to the penalty of the offense facilitated through IT network.

iii. Uses That Damage The Integrity, Reliability, Confidentiality And Efficiency Of The IT System

1. **Software and hardware installation and removal.** Unless properly authorized, users may not destroy, remove, modify or install any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the IT System; or connect any computer unit or external network to the IT System. Violators shall suffer a penalty ranging from suspension for one month to expulsion.
2. **Unauthorized or destructive programs.** Unless properly authorized and part of her/his administrative or academic duties, users may not develop or use programs on the IT System that may or are intended to:
    a. interfere with the ability of the UP SYSTEM to enforce these policies;
    b. damage any software or hardware component of the system;
    c. modify normally protected or restricted portions of the system or user accounts;
    d. access private or restricted portions of the system; or
    e. interfere with or disrupt other computer users. Violators shall suffer a penalty ranging from suspension for one year to expulsion.
3. **Destructive acts.** Users may not attempt to crash, tie up, or deny any service on, the IT System. Violators shall suffer a penalty ranging from suspension for one year to expulsion.
4. **Unauthorized access.** Users may not attempt to gain unauthorized access, exceed authorized access, or enable unauthorized access to the IT System, or to other networks or systems of which the IT System is a part. Violators shall suffer a penalty ranging from suspension for one month to one year.
5. **Password protection.** A user who has been authorized to use a password-protected account may not disclose such password or otherwise makes the account available to others without permission of the system administrator. Violators shall suffer a penalty ranging from suspension for one week to one year.
6. **Concealing access.** Users may not conceal, delete, or modify information or records pertaining to access to the IT System at the time of access, or alter system logs after

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 week to one month; spamming, includes the act of (1) repeated cross-posting 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, (2) maliciously sending out of unsolicited email in bulk, or (3) sending large unwanted or unnecessary files to a single email address.
    b. Printing excess copies of documents, files, data, or programs; violators shall suffer a penalty ranging from suspension for one week to one month;
    c. Running grossly inefficient programs when efficient alternatives are known by the user to be available; violators shall suffer a penalty ranging from suspension for one week to one month;

d. Using more than one computer terminal at a time, unless specifically authorized by competent authority. Faculty members whose duties require the use of more than one computer shall be exempted. Violators shall suffer a penalty ranging from suspension for one week to one year;

e. Locking public access computers using screen savers or otherwise, unless specifically authorized by competent authority; violators shall suffer a penalty ranging from suspension for one week to one month;

f. Not logging out of the system to allow other users to make use of the public access computer; violators shall suffer a penalty ranging from suspension for one week to one month; and

g. Using a service which has been identified by the System Administrator as causing an excessive amount of traffic on the IT System or its external network links; violators shall suffer a penalty ranging from suspension for one week to one year.

2. Offensive material.

a. Users may not use the facilities of the IT System to produce, disseminate, or display material that could be considered offensive, pornographic, racially abusive, or libelous in nature.

b. Users may not use electronic communication facilities (such as mail, chat, or systems with similar functions) to send messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of the University System or its constituent universities (CU). Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal.

3. Inappropriate messages. Users may not send to a mailing list, including local or network news groups and bulletin boards, any unsolicited material inconsistent with the list's purpose. Users of an electronic mailing list are responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list are deemed to have solicited any material delivered by the list that is consistent with the list's purpose. Violators shall suffer a penalty ranging from suspension for one week to one month.

v. Uses which Violate Privacy

1. Confidential information.

a. Unless properly authorized, users may not attempt to gain access to archives or systems that contain, process, or transmit confidential information. Authorized users may not exceed their approved levels of access, nor should they disclose confidential information to others.

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.

2. **Encrypted information.** Users shall consider as confidential all encrypted information. This includes but is not limited to passwords, digital keys and signatures. Users may not decrypt, attempt to decrypt, or enable others to decrypt such information if they are not the intended recipient. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.
3. **Information belonging to others.** Users may not intentionally seek or provide information on, obtain copies of, or modify files, programs, or passwords belonging to other users, without the permission of those other users. Violators shall suffer a penalty ranging from suspension for one month to expulsion or dismissal.
4. **Wiretapping, traffic capture and snooping.** Unless properly authorized, users may not re-route or capture data transmitted over the IT System. Violators shall suffer a penalty ranging from suspension for one year to expulsion or dismissal.

vi. In addition to the penalties provided, all IT privileges of the offender may be suspended for a maximum of the period of the penalty. If the violation amounts to a penalty punishable by expulsion or dismissal, IT privileges may be revoked permanently.

vii. repeated violations of any of the acts proscribed under this policy shall be considered as gross misconduct.

Section 7. Tolerated Use

From time to time, the UP SYSTEM or its constituent universities may issue a list classifying certain types of use under the category of tolerated use. This list shall form part of this Policy and will be considered binding on all users. Users should consult their system and network administrators if they are not sure whether a certain type of use is considered allowed, tolerated, unacceptable or prohibited.

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. The UP SYSTEM through the system and network administrators will document all instances of access without consent.

c. **Reporting Problems and misuse.** Users must report to the appropriate system administrators any defects discovered in system accounting or system security, all known or suspected abuse or misuse of the IT System, and especially any damage to or problems with their facilities or files.

d. **User Cooperation.** Users, when requested, are expected to cooperate with UP SYSTEM in any investigation of IT system abuse.

e. **Guidelines for Immediate Action.**

   i. **Notification.** When any system administrator or member of the faculty or staff has persuasive evidence of abuse or misuse of the IT System, and if that evidence points to

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. **Suspension.** In such cases, the system administrator may temporarily suspend or restrict the user's access privileges for a period not exceeding 72 hours. A user may appeal such suspension or restriction and petition for immediate reinstatement of privileges through the Chancellor or his/her duly designated authority. The Chancellor may extend the suspension for thirty (30) days.

iii. **Removal.** In addition, in such cases, the system administrator may immediately remove or uninstall from the IT System any material, software or hardware which poses an immediate threat to the integrity, reliability, availability, confidentiality and efficiency of the IT System or any of its components or if the use might be contrary to this Policy. The user shall be notified of the action taken. A user may appeal such removal and petition for reinstatement of the material within fifteen (15) days from removal.

f. **Investigation.** The investigation and prosecution of academic and administrative personnel and students shall be in accordance with the regulations of the UP SYSTEM. The investigating committee, body or tribunal must have at least one member knowledgeable about IT. The actions the proper officer may undertake include but are not limited to the following:

i. Extend the suspension or restriction of a user's privileges for the duration of the investigation, or as may be deemed necessary to preserve evidence and protect the system and its users;

ii. Call and interview potential witnesses; and

iii. Summon the subject of the complaint to provide information.

g. **Filing of Criminal Charges.** In cases where there is evidence of serious misconduct or possible criminal activity, the Chancellor shall file the appropriate criminal charges with the proper courts. Where proceedings have been instituted against a user for violation of this Policy, the Chancellor may indefinitely suspend or restrict the user's access privileges for the duration of such proceedings.

h. **Cumulative Remedies.** The procedures under this Policy shall not exclude any other remedy available to any injured or interested party under any relevant law, administrative rule or regulation, or other policy of the UP SYSTEM.

i. **External Legal Processes.** The UP SYSTEM shall comply with any lawful order to provide electronic or other records or other information related to those records or relating to use of the IT System which may result from coercive processes in administrative investigations, or judicial actions or proceedings.

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.