STANDARDS FOR THE ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

UNIVERSIDAD DE PUERTO RICO

Issued on April 4, 2008

Approved by:

4/7/08

Emma Fernández-Repollet, Ph.D.
Vice President for Research and Technology

Date

TABLE OF CONTENTS

INTRODUCTION TO USING INFORMATION TECHNOLOGY RESOURCES

The information within this document is subordinate and subject to the Board of Trustee's Certification # 35, 2007-2008 Series: the *System-Wide Policy for the Acceptable Use of Information Technology Resources Throughout the University of Puerto Rico* (henceforth, the "IT Policy"). The standards contained herein must be adhered to by all users and technology administrators. Compliance with these Standards ensures compliance with the IT Policy; and enables the best possible use of the IT resources available to the University of Puerto Rico.

All IT procedures as well as campus IT policies throughout the University must be aligned with the IT Policy as well as with these Standards. Final interpretation of the meaning, intent, and approach towards their application lies within the exclusive domain of the Vice President for Research & Technology.

REFERENCE SOURCES

Several sources of information have been used as input for this document, to guarantee comprehensiveness. They include existing policies and guidelines from other universities both within and outside the U.S., applicable federal and Commonwealth legislation, best practices from recognized industry authorities and experts, and other peer reviewed sources.

ACQUIRING AND ADMINISTRATING IT RESOURCES

The ISO will identify the minimum hardware and software specifications for acquiring information technology equipment and software. ISO will make these specifications available to the general university population. Users and technology administrators will use these specifications when requisitioning computers and software. However, University researchers may choose to follow these specifications or not depending on their specialized needs, due to the specialized nature of their institutional work.

Acquisition and installation of hardware and software (including operating systems) for which ISO support is expected and required must be coordinated through the ISO; that ISO may confirm its ability to support this hardware and software.

Industry guidelines establish a technology's useful life in terms of the number of years it may be productively used by an institution. All campuses, departments, and offices should consider the useful life of their information technology equipment during the reviews of their respective annual budgets and plan accordingly for the timely substitution of their computers and devices when they reach the end of their useful life; provided that adequate funding is available. In this endeavor, ISO may provide assistance to identify particular equipment model's age, technical specifications, and estimated replacement cost.

The ultimate determinants as to how long information technology equipment lasts are the care and preventive maintenance provided to it and the support available from the technology

industry. The decision to acquire new technology rather than repair existing technology should be based on which is the lesser cost. Acquisition of new equipment, rather than repairing the existing equipment should be authorized by the office or laboratory director.

All information technology equipment and software purchased through the University is considered the sole property of the University. Acquisitions of Information Technology equipment will be done in compliance with the IT Policy and the Board of Trustee's Certificate # 62, Series 1994-1995, *Regulation for Control of Fixed Assets in the University of Puerto Rico.*

Software acquisitions will be acquired in compliance with the IT Policy. Non-standard software will be acquired following the IT Policy and the applicable regulations and procedures regarding the acquisition of non-personal equipment, supplies, and services at the University of Puerto Rico.

In order to make the best possible use of available technology resources, offices, campuses, and faculties may transfer productive equipments following appropriate control procedures. Damaged equipment may be repaired as long as it is economically feasible for the University. Otherwise, it will be disposed in compliance with the applicable regulations regarding the control of fixed assets in the University of Puerto Rico.

USING HARDWARE AND SOFTWARE RESOURCES

University computers, networks, systems, applications and data are to be used only for legitimate, authorized purposes. User and technology administrators will utilize only the hardware and software legally made available to them. No user and technology administrator must ever engage in, promote, cause, abet, or allow any activity that might be harmful to any University equipment, network, system, application or data; since this would inhibit other user and technology administrators from conducting their own legitimate work for the University.

Avoid unapproved changes to a computer's configuration, as this may hamper the computer´s connectivity to network services.

A user and technology administrator should either lock or logoff from a computer being used whenever he or she steps away; to avoid unauthorized use of his or her work session.

SECURING INFORMATION TECHNOLOGY RESOURCES

In an endeavor to secure University IT resources, user and technology administrators should take all reasonable precautions to protect University computers (including servers), networks, applications, and data. Such measures should include special arrangements for housing the IT equipment (temperature and humidity control, physically controlled access, fire suppression, etc.) in line with the equipment's criticality; as well as using specialized hardware and software to protect these IT resources and the data contained therein. Third parties who connect their equipment to the University network must also provide similar protection for their computers.

Malicious software represents a substantial risk to the University community in terms of time, money, and potential loss of computer software and/or data. As part of the endeavor to secure and protect all equipment that accesses University data, every computer and server connected to the University network is required to maintain and use up-to-date versions of protective software such as anti-virus, anti-spyware, or intrusion detection software configured according to relevant IT system-wide procedures. User and ISO's will regularly apply vendor-issued critical security updates and patches to installed software to protect University computers (including servers), networks, systems, applications, and data. Administrators of servers and network equipment will take steps to apply security and firmware updates with minimal to no impact or interruption to system availability by users.

Furthermore, University users and technology administrators should periodically backup critical applications and data to allow continuity in the event of emergencies.

USING ID AND PASSWORD

The combination of username (user ID) and password is uniquely assigned to each user and technology administrator as a mechanism to ensure that only an authorized person may access University data and systems over the network. User and technology administrators will take the necessary steps to protect these, whether accessing systems locally or remotely, in compliance with the IT Policy, these Standards, and subordinate system-wide procedures implemented throughout the University. Strong passwords should be used to minimize the probability of unauthorized access, following the techniques identified within *ISO Security Norms.*

ADMINISTRATING DOMAINS

The University and its Campuses have established a virtual presence over the Internet through the use of domains. The System ISO administers and operates the University DNS UPR.EDU and the Internet Protocol (IP) address space assigned to them. Anyone wishing to define additional domains to run on the University network or represent the University must coordinate and obtain approval from the System ISO.

Each Campus ISO administers and operates the Internet domain for their respective Campuses and the IP address space assigned to them. Anyone wishing to define additional domains to run on the Campus network or represent the Campus must coordinate and obtain approval from the Campus ISO.

SECURE ACCESS TO THE NETWORK

The University network consists of Campus Area Networks and many dependencies all connected to a high-speed, broadband backbone. The majority of the campus networks are run centrally by campus ISO but for those departments with certain specialized needs, non-ISO local networks are allowed to connect to the campus backbone network.

As a general rule, a non-ISO network is financed, administered, and maintained primarily by a department, faculty or facility. Nevertheless, although said network may be seen as a separate resource, relevant practices and procedures should be consistent with the IT Policy and these Standards.

To function, the elements of the network must have an implicit trust arrangement with each other. Thus, the entire network infrastructure (i.e. network equipment such as routers and switches), whether on ISO or non-ISO networks, must be secured to a high level. All efforts to connect to the campus network must be coordinated through the Campus ISO. Efforts to connect to the university network must be coordinated through the System ISO, given the system-wide impact that any change here may have. Furthermore, network administrators shall protect the network by implementing authentication to validate the legitimate access of authorized users.

Every user and technology administrator of University IT resources must make sure that all possible measures have been taken to secure the computers used to connect, whether locally or remotely, turned on or off, to the University network. Application resources over the network shall be provided, based upon user and technology administrator needs, but will be subject to protecting said resources against attacks and unauthorized access attempts. This Standard applies to remote access connections used to do work on behalf of the University, including but not limited to, reading or sending e-mail and viewing intranet Web resources. All remote access implementations at the University are covered by the IT Policy and this Standard.

ACCESSING WIRELESS NETWORKS

The University provides wireless networks (also called wireless local area networks, WLAN's or LAWN's) to allow flexible, mobile connectivity to the Campus and University networks, and the Internet. Wireless access should be implemented wherever feasible: i.e., wherever technical facilities are available and the applications' security and technical requirements permit their use. University administrators wishing to implement wireless access and user wishing to access WLAN's should coordinate the effort through the System or Campus ISO. System and Campus ISO are responsible for configuring the WLAN to guarantee secure access to Campus and University networks, applications, and data by implementing segmentation and authentication.

SECURING PRIVATE DATA

The University is responsible for maintaining high standards of security for private/non-public electronic information, as required by federal and Commonwealth laws. University data that is stored on or accessed by computers or other electronic devices must be secured against intentional or accidental loss of confidentiality, integrity, or availability regardless of location: whether on campus or off campus.

Information should be treated in accordance with its nature: confidential, private, or public. The University will treat all legally and contractually protected non-public University data as

confidential; whether it is research, clinical, educational, outreach, or administrative data. Furthermore, the University will hold any person who requires access to University information, whether or not said person is a user and technology administrator of University Information Technology, to comply with the IT Policy and these Standards.

User and technology administrators will take reasonable steps to secure all hardware through which private data may be accessed. University offices, campuses, faculties, and units shall conduct periodic reviews of information systems under their control that contain private or confidential data.

SECURELY DELETING DATA

Non-public data and licensed software remaining on computers, other electronic devices, and storage media at the time of transfer or disposal represent a substantial security risk that should be addressed through secure data deletion. Non-public information must be securely deleted from any and all devices which will be disposed of or transferred from a current User and technology administrator to an unknown destination or to another User and technology administrator who is not authorized to the data. The department or individual directly responsible for non-public data on a University computer or other electronic device is required to ensure that any non-public information on that device is securely removed before disposing of the device beyond their direct control. The department or individual directly responsible for non-public data on a University computer or other electronic device shall take the required steps to eradicate data contained on any form of electronic storage media in a manner that makes it totally impossible to recover the data, before said electronic storage media is transferred or otherwise disposed of. If necessary, said department or individual may request assistance from ISO to comply with this responsibility.

FILE SHARING THROUGH PEER-TO-PEER (P2P) PROGRAMS

User and technology administrators should coordinate with ISO before installing and using file sharing or peer-to-peer (P2P) programs. Although information sharing is an integral part of the University's philosophy, it should be done in a manner that complies with the IT Policy, these Standards, and relevant Procedures. The University does not explicitly prohibit the installation of these programs. Nevertheless, when a program of this type is installed, its file sharing functionality is activated by default. This is a serious security risk, since it represents a way in for programs whose intent is to exploit network vulnerabilities. Also, users and technology administrators open themselves – and the University – to possible violations and infringements of copyright law, even without their knowledge.

DESIGNING WEB SITES AND WEB APPLICATIONS

The University's mission of instruction, research, and service outreach applies to all individuals, regardless of whether an individual has a physical limitation. The University will promote that its

technologies and electronic sources of information, particularly web pages and web sites, comply with applicable federal and Commonwealth legislation and regulations; to allow individuals with disabilities have access to and use information and data in a manner that is comparable to that by individuals without disabilities.

As with written communication forms such as University stationary and promotional material, University web pages and web sites reflect a graphical image of the University to the outside world. The University and/or its Campuses may define and publish basic design frameworks (colors, headings, and logos, among other criteria) to align their web pages and sites with a desired institutional image. Within a framework, individual designers have ample leeway for designing web pages and applications. University researchers and academicians are exempt from having to comply with these frameworks, due to the specialized nature of their institutional work. Nevertheless, all web sites will include, as a minimum, a link to their Campus or institutional unit on the site's top page. This exemption does not preclude from the use of best practices for website design or application development. All web sites on the UPR domain must comply with UPR's legal and policy guidelines. Web pages should be designed to load fairly quickly; for the benefit of those users who do not have broadband access.

As a public corporation, the University must exercise care when placing notices on any form of communication which may be construed as an advertisement or endorsement of any external commercial or political entity. As a general rule, political or commercial advertisements in UPR websites are not allowed. Any advertisement through UPR websites that is justified in terms of its benefits to the University may be allowed after written approval from the corresponding University official – the President, the chancellors, or their designated representative - at the Institution or Campus level.

EDUCATING FOR THE CORRECT USE OF TECHNOLOGY

System and Campus ISO will promote the correct use of IT resources and compliance with the IT Policy, these Standards, and the applicable subordinate procedures, through a permanent campaign using such mechanisms as periodic seminars, workshops, conferences, and written and electronic forms of communications issued to the user and technology administrator communities throughout the University. This effort may be coordinated and conducted at the campus level as well as through Central Administration; and may be conducted using either University or non-University resources.

MAINTAINING IT STANDARDS & PROCEDURES

From time to time, it may be necessary to review these Standards, and their subordinate procedures, to adapt them to the University's changing needs. Said review may be required as a result of changes in legislation or University regulations, policies, and bylaws. Reviews may also be required to address emerging technologies, better ways to use current technologies, better ways to execute processes, or whenever new technology is implemented.

The Vice President for Research & Technology will work with the System and Campus ISO's to review these Standards and Procedures; in particular where issues of information technology adoption, use, security, privacy, and intellectual property are concerned. Any change to existing Standards and Procedures – as well as the incorporation of any new Standard or Procedure – must be consonant with the IT Policy and these Standards.

DEFINITIONS

The following definitions are provided as a convenience for the reader. The definitions include terms referred to throughout this document, which are endemic to the information technology industry.

- **ADWARE**

  Advertising-supported software (Adware) is software that automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while an application is being used. In a negative context, malicious adware may take the form of spyware (in which information about the user and technology administrator's activity is tracked, reported, and often re-sold, without the user and technology administrator's knowledge or consent) or malware, which may interfere with the function of other software applications, in order to force user and technology administrators to visit a particular web site.

- **ANTI-SPYWARE**

  Specialized software used to protect a server or user and technology administrator computer from the effects of spyware.

- **ANTI-VIRUS**

  Specialized software used to protect a server, user and technology administrator computer, network systems, applications, and data from malware such as viruses, Trojan horses, or worms.

- **BROADBAND**

  In telecommunications, broadband is a term which refers to a signaling method which handles a wide (broad) range of frequencies divided into channels. The wider the bandwidth, greater is the information carrying capacity.

- **DOMAIN NAME SYSTEM (DNS)**

  The Domain Name System is a distributed hierarchical database that stores information associated with Internet Domain names. Common uses include designating domain names to IP addresses and locating e-Mail servers under a designated domain.

- **HARDWARE**

  General term used to refer to physical artifacts of technology, such as computers or communications routers.

- **INTRUSION DETECTION SOFTWARE (IDS)**

  IDS alert computers to unknown, unauthorized access attempts. IDS let user and technology

administrators know that someone or something is trying to get into the system.

- **INFORMATION SYSTEMS OFFICE (ISO)**

  The office specifically empowered by the University with authority to protect information technology resources and data. The System ISO is located at the Central Administration, while each campus has its own Campus ISO, albeit under a different name.

- **INFORMATION TECHNOLOGY (IT)**

  Information Technology encompasses the study, design, development, implementation, support or management of computer-based information systems. IT includes computer hardware, network hardware, software applications, and data. IT deals with the use of hardware and software to store, convert, protect, process, transmit, retrieve, and report information, securely.

- **INTERNET DOMAIN**

  An Internet Domain is a base name that groups clusters of hardware devices. It allows designating names to identify this equipment which are easier to remember than numerical IP addresses. As with IP addresses, the Internet Domain identifies the equipment located within. As a general rule, the domain name identifies the institution to which it belongs.

- **INTERNET PROTOCOL (IP)**

  IP constitute the standard rules governing the syntax, semantics, and synchronization for communicating data across telecommunications networks.

- **LAWN**

  Local Area Wireless Network (also referred to as WLAN).

- **LOCAL AREA NETWORK (LAN)**

  A local area network is a computer network covering a small geographic area, such as an office, campus or a group of buildings.

- **MALICIOUS HACKING**

  Hacking refers to the modification of computer programs, systems or network security to exploit perceived weaknesses or achieve illegitimate access to IT or network resources.

- **MALICIOUS SOFTWARE (MALWARE)**

  Software designed to infiltrate or damage a computer's systems, application, or data without the owner's informed consent. It encompasses such programs as computer viruses, worms, Trojan horses, spyware, dishonest adware, and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant. Malware may have been purposely or accidentally installed on computers.

- **TELECOMMUNICATION NETWORK**

  A computer network is multiple computers connected together using a telecommunication system for the purpose of communicating and sharing resources.

- **NETWORK PORT ACCESS**

  A port refers to an access point into the network. It may range from a dial-in connection, to Ethernet connections, to a Wi-Fi (wireless) connection. Ports are designated as either standard or open.

- **OPEN PORT**

  An open port is a network port that may be used by more than one computer to connect to a network. Authentication is required on an open port before allowing traffic to pass, as a way to protect the network. Furthermore, an open port should be subject to re-authentication every pre-determined number of hours, for security purposes.

- **PRIVATE DATA**

  The term "private data" refers to legally or contractually protected non-public institutional data or data which the University is obliged to treat as confidential whether it is research, clinical, educational, outreach, or administrative data. Some examples of private/non-public data are:

  - Social security number
  - Ethnicity
  - Birth date
  - Linking library user and technology administrators with subjects about which information was requested
  - Citizen visa code or passport number
  - Citizenship
  - Trade secrets or intellectual property
  - Non-directory Student Information (not to be released except under prescribed conditions)

  Examples of non-releasable information include:

  - Grades
  - Courses taken
  - Schedule
  - Test scores
  - Advising records
  - Educational services received
  - Disciplinary actions

  Examples of contractually protected information:

  - Credit card numbers
  - Personal Identification Number (PIN)

- **SECURE DATA DELETION**

  Secure data deletion refers to a process of eradicating data on any electronic storage media in a manner that makes it totally impossible to recover the data. Secure deletion is achieved by an electronic wipe through a secure data deletion program for computers that writes random data in multiple passes; by replacing the current contents of a computer hard disk en masse with a base image of the computer disk (e.g. an image of the initial disk configuration, before the data was generated or stored on the disk); or by utterly destroying the physical media. Non-public information located on any storage media must be securely deleted or destroyed before disposing of the storage media beyond the custodian's direct control.

- **SOFTWARE**

  In contrast to hardware, software is the general term used to refer to the logical components of technology, such as the operating system, computer programs and the data accessed and maintained by the programs.

- **SPYWARE**

  Spyware is computer software that collects personal information about user and technology administrators without their informed consent. Purposes range from overtly criminal (theft of passwords and financial details) to the merely annoying (recording Internet search history for targeted advertising, while consuming computer resources). Spyware may collect different types of information. Some variants attempt to track the websites a user and technology administrator visits and then send this information to an advertising agency. More malicious variants attempt to intercept passwords or credit card numbers as a user and technology administrator enters them into a web form or other applications.

- **STANDARD PORT**

  A standard port is a network port that has a single machine continuously connected to it. It is generally more secure than an open port.

- **STORAGE MEDIA**

  Any device used to store or retrieve data or application files from a computer. Storage media may be fixed, such as a hard disk; or removable, such as floppy diskettes, magnetic tape cartridges, compact disks (CD's), digital video disks (DVD's), or pen drives (also known as USB drives).

- **TROJAN HORSE**

  A Trojan horse is a program that contains or installs a malicious program (sometimes called the payload or 'Trojan'). The program may be a legitimate program that has been hacked to insert malicious code.

- **VIOLATION**

  Any action contrary to the Acceptable Use IT Policy, these Standards, or the subordinate IT policies and procedures is considered a violation.

- **VIRUS**

  A virus is computer program that copies itself and infects a computer without permission or knowledge of the user and technology administrator. The original may modify the copies or the copies may modify themselves. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user and technology administrator sending it over a network or carrying it on a removable storage medium such as a diskette, CD, or pen drive. Viruses can also spread to other computers by infecting files over a network.

- **WIDE AREA NETWORK (WAN)**

  System-wide communications network that interconnects the different local area networks (LAN's); and also connects these local area networks to the commodity Internet and Internet2.

- **WIRELESS NETWORK**

  In traditional networks, computers are connected to telecommunications equipment via cables or 'wires'. As opposed to 'wired' networks, a wireless network provides this link through devices that use radio frequency to achieve the same link between computers. Wireless access is also known as 'Wi-Fi' (for wide fidelity) access.

- **WLAN**

  Wireless Local Area Network or Wireless LAN (also referred to as LAWN).

- **WORM**

  A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user and technology administrator intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

REVIEW HISTORY

Version	Date	Description
0	4-Abr-2008	Initial version of the ***Standards for the Acceptable Use of IT Resources***, in line with the *System-Wide Policy for the Acceptable Use of Information Technology Resources Throughout the University of Puerto Rico.*