POLICY

Title:	**Use of Electronic Communications**
Effective Date:	November 15, 2011
Approved By:	President's Council
Responsible Party:	Chief Information Officer
History:	April, 1999, August 2003

I. PURPOSE

Salus University ("Salus") encourages the use of electronic communications to share information and knowledge in support of the University's mission of education, research and public service and to conduct the University's business. To this end, the University supports and provides interactive electronic communications services and facilities for telecommunications, mail, publishing, and broadcasting.

Recognizing the convergence of technologies based on voice, video, and data networks, this policy establishes principles, rules, and procedures applying to all members of the University community to specifically address issues particular to the use of electronic communications. It clarifies the applicability of law to electronic communications and references other University guidelines to ensure consistent application of the Electronic Communications Policy on all University campuses/satellites.

II. DEFINITIONS

Authorized Users: Authorized users are Salus University faculty, staff, students and other persons who have received permission under the appropriate University authority to use SU's electronic communications systems, computer files and other stored communications and resources.

III. POLICY

The Salus University electronic communication systems includes: computers, communications networks, computer accounts, web pages, network access, central computing and telecommunications facilities, and related services. Users of University electronic communication systems must respect the rights of others, respect the integrity of the computers, networks, and related services, and observe all relevant laws, regulations, contractual obligations, and University policies and procedures. All users of the electronic communication systems must act responsibly and maintain the integrity of the systems.

Access to computers is a privilege based on the responsible use of computer and network resources. All policies included here are intended to insure a continued tradition of academic freedom, freedom of expression, and freedom to access information in a considerate and responsible manner. In keeping with the mission of

Salus University, all policies are intended to provide the widest possible academic and scholarly access to computer resources and information technology.

While Salus University's network administration desires to provide a reasonable level of privacy, users should be aware that all data created, read, and/or sent using the University's systems remain the property of the University. Because of the need to protect Salus's network, the University cannot guarantee the confidentiality of information stored, sent or received on any network device belonging to the University and employees should not have any expectations to privacy. Routine maintenance can result in the contents of files and messages being seen by system or network administrators; however, network and system administrators are expected to treat the contents of electronic files and communications as private and confidential. Any inspection of electronic files or messages, and any action based upon such inspection, will be governed by all applicable and relevant University policies. Note also that under the Freedom of Information Act, the files of University employees (paper or electronic) may be considered public documents, and may be subject to inspection under the FOIA, through formal University-administered procedures. The content of electronic files and communications may also be subject to subpoena in other legal proceedings.

IV. PROCEDURE

Authorized Use

Authorization is given by way of receipt of a username and password from the MIS department for computer use and activation of the voice mail system for voice mail capability.

Authorized users should keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed regularly; user level passwords should be changed every six months.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.

No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Salus official.

Authorized users should not reveal their account password(s) to others or allow use of their account by others. This includes family and other household members when work is being done at home.

Salus University's technical resources are to be used to further the University's mission, to provide effective education and services of the highest quality to the University's students, customers, patients and staff, and to support other direct job-related and/or administrative purposes.

Use of the University's name and logo is regulated by the State of Pennsylvania Education Code. Users of electronic communications resources must abide by this statute as well as by University and campus policies on the use of the University's name, logo, seals, and trademarks. Users of electronic communications resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so.

Personal Use

The University's computing and network resources exist to support the University's missions of teaching, research, patient care and public service. Incidental personal use of these resources by authorized users is permitted only to the extent that such use is lawful and ethical, does not conflict with the University's missions, does not interfere with other authorized users, and does not cause additional expense to the University. The University e-mail system may not be used to send hostile, aggressive, insulting, offensive, or derogatory statements about or against another individual.

Any personal use is expected to be on the user's own time, is not to interfere with the person's job responsibilities, and must not violate the parameters set forth in this policy. Personal use includes instant e-mail, messaging, chat rooms, Facebook, Twitter, My Space, and other such social media and personal sites.

Ethical Use

This policy should be read and interpreted in conjunction with all other University policies including but not limited to policies prohibiting harassment, discrimination, unprofessional or offensive conduct or inappropriate behavior. Within the broad context of free academic discussion and debate, all forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility.

Employee-users are prohibited from using Salus computers, network or internet resources for any unethical purposes, including pornography, violence, gambling, racism, sexism, threats, harassment, or otherwise objectionable or illegal activity/material. "Material" is defined as any visual, textual, or auditory item, file, page, graphic, or other entity.

Users are to refrain from using profanity or vulgarity when positing electronic mail via the Internet or posting to public forums (i.e., newsgroups).

Academic Freedom

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The freedom to learn depends upon appropriate opportunities and conditions not only in the classroom, but on the campus as a whole. The responsibility to secure and to respect general conditions conducive to the freedom to learn is shared by all members of the academic community -- faculty, staff, and students. System and network administrators are expected to respect the University's academic freedom policies.

No file stored on a University computer system should be removed by a system administrator without the file owner's permission unless the file's presence interferes with the operation of the system.

No posting to a University-sponsored electronic forum should be removed by a system administrator unless it violates US law, State law or University policy.

Intellectual Property
This Policy does not address the ownership of intellectual property stored on or transmitted through University electronic communications resources. Ownership of intellectual property is governed by law and the Salus University Policies on Intellectual Property and Copyright and Patents.

The contents of all electronic communications shall conform to laws and University policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. When the content and distribution of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976, users of University electronic communications resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.

Prohibited Uses of Electronic Communications
The following activities are, in general, prohibited. This list is not all-inclusive.

a. Engaging in any activity that is illegal under local, state, federal or international law utilizing Salus-owned resources.
b. Personal use that creates a direct cost for Salus University.
c. Use of Salus's electronic communications resources for personal monetary gain or for commercial use not directly related to University business.
d. Attempting unauthorized access to or disclosure of employee, student or patient care information, including all information regarding a patient's identity, treatment or diagnosis.
e. Writing, sending, reading, or receiving data that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.
f. Sending or receiving communications that contain sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, gender, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
g. Using electronic communication devices for political causes or activities, religious activities, or any sort of gambling;
h. Viewing or downloading of pornographic or other similarly inappropriate internet sites;
i. Constructing an electronic communication so it appears to be from someone else;
j. Sending or posting messages or material that could damage the University's image or reputation;

k. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
l. Using the University's Internet/Intranet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the University's networks or systems or those of any other individual or entity.

Interference

University electronic communications resources shall not be used for purposes that could reasonably be expected to cause excessive strain on any electronic communications resources, or to cause interference with others' use of electronic communications resources.

Users of electronic communications services shall not: (i) send or forward chain letters or their equivalents in other services; (ii) "spam," that is, exploit electronic communications systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic messages; (iii) "letter-bomb," that is, send an extremely large message or send multiple electronic messages to one or more recipients and so interfere with the recipients' use of electronic communications systems and services; or (iv) intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications services.

Intentionally destroying anything stored on the communication systems, including anything stored in primary or random access memory is prohibited. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer or peripheral.

Salus University faculty and staff are required to report any security incident that affects any SU information system or any SU data.

Copyright Compliance

In accordance with U.S. Copyright laws, the downloading, installation, configuration and operation of any peer-to-peer ("P2P") software or server on Salus computers facilities is illegal under state and federal laws and is in direct violation of this policy. Any individual who operates P2P software on Salus computer facilities will be subject to the disciplinary terms outlined in this policy. In addition, individual(s) will be held personally liable for any infraction, which results in criminal investigation and/or civil action resulting from non-compliance to this specific provision of this policy.

In compliance with the Digital Millennium Copyright Act, the University reserves the right to suspend or terminate use of University electronic communications systems and services by any user who repeatedly violates copyright law.

No user may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

Electronic Mail (E-Mail)
The campus electronic mail system exists primarily to facilitate business communications between individuals and specific groups. To the extent that there is excessive use of "Everyone Group" messages (or similar mass mailings) to numbers of individuals who, given a choice, would choose not to receive them, the effectiveness of the System is compromised. Such messages must be restricted to campus emergencies and urgent operational messages, notification of campus meetings and events, and notification of University-sponsored events or other events off-campus, which relate to the University's educational goals. Messages such as notice of lost and found articles, promotion of political causes, and listing of personal sale items should not be sent via the campus e-mail system.

Enforcement
SU reserves the right to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state or federal laws. The University reserves the right to deny, limit, revoke, or extend computing privileges and access to the computer system in its discretion. In addition, alleged violations of this policy or violation of other University policies in the course of using the communication systems may result in an immediate loss of computing privileges and may also result in the referral of the matter to the appropriate authority. Any user who violates this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Acknowledgement
All authorized users will acknowledge receipt of this policy by signing the Acknowledgement Page. Acknowledgement means that the user has reviewed and understood the policy and that the user agrees to be bound by the terms of the policy.

Authorized users are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements. The University will report any illegal or potentially activity to the proper authorities and cooperate fully with any investigation resulting from such a report.

Electronic Communications Policy Acknowledgement Form

I acknowledge that I have received the Policy on Electronic Communications. I understand the policy and agree to be bound by the terms of the policy.

_____

Name (Please Print)

_____ _____

Signature Date