Title:	Use of University Email
Effective Date:	August 11, 2016
Approved By:	President's Council
Responsible Party:	Chief Information Officer
History:	
Related Documents: Confidentiality of University Records & Information Policy; HIPAA; Use of Electronic Communications Policy;	

I. PURPOSE

Electronic mail (email) is a primary means of communications within Salus University and externally. It allows quick and efficient conduct of business, but if used carelessly or illegally, it carries the risk of harm to the University and members of the University community.

The purpose of this email policy is to describe the permitted uses of University email and to ensure that users are aware of the acceptable and unacceptable use of the University email system. Compliance with this policy helps the University to achieve two goals:

1. Improve the successful delivery of University communications to all faculty, staff, students, and external parties, and
2. Reduce the risk of University data classified as legally restricted or confidential going through email systems that are not managed by the University.

II. DEFINITIONS:

***Encryption*:** is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

Sensitive Data: Protected Health Information, Social Security Numbers, Credit Card Numbers, Financial Account Numbers, and other information protected by HIPAA, FERPA, and other laws and regulations.

Protected Health Information: Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing health care services.

***Personally Identifiable Information (PII)*:** PII is information that can be used to distinguish or trace an individual's identify, such as their name, social security number, biometric record, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

III. POLICY

Email services are provided to University employees, students, and others to conduct University business. The University community will use email in an ethical and considerate manner in compliance with applicable Federal and State laws, as well as policies and guidelines established by the University.

IV. PROCEDURE:

A. Account Creation/Retention:

E-mail accounts will be created for employees and students prior to arrival at the University. E-mail accounts may be granted to third-party non-employees providing services for the University on a case-by-case basis.

For students in good standing with the University, their e-mail account will remain active for one year following the date of graduation.

E-mail access will be closed the date that an employee or third party terminates their association with the University unless other arrangement are made with and approved by the Office of Human Resources.

Emeritus professors are entitled to maintain an active University e-mail account.

B. University Rights and Responsibilities:

1. Ownership of e-mail: The primary purpose of email service is for University business. Therefore, the University owns any accounts provided by the University. All messages originating in or received by the email system are the property of Salus University.

2. Right of University Access: Under certain circumstances, it may be necessary for the technology staff or other appropriate University officials to access University email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating network security or abuse incidents, or investigating violations of this or other University policies. Technology staff or University officials may also require access to a University email account in order to continue University business where the University email account holder will not or can no longer access the University email account for any reason. Such access will be on an as-needed basis and any email accessed will only be disclosed to those individuals with a need to know or as may be required by law.

3. Privacy: Privacy of content in email messages sent through a University email account cannot be completely guaranteed. Privacy is not guaranteed when required by law, when authorized and necessary for University business, for service quality purposes, and/or when there is reason to believe an individual has violated law and/or University policy.

4. Confidentiality: The confidentiality of email cannot be assured. Confidentiality may be compromised by access consistent with applicable law or policy, including this policy; by unintended redistribution; or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters. Users may not send restricted or confidential data to entities outside the University without a business purpose or without appropriate authorization. When sending email to non-Salus addresses, precautions must be taken to protect the confidentiality of this type of information. Minimally, you must:
    - Verify the recipient's address (for example, from a directory or a previous email) and check that you have entered the address correctly;
    - Encrypt using the University Email Encryption Standard – Virtru.
    - Technology personnel instructions provided for using the University's encryption software must be followed completely.

A. Proper Use and User Responsibility:

1. Taglines and University Identifications: Acceptable signatures on emails contain information that would be considered acceptable on University business cards: the sender's full name, titles, roles, contact/department information, certifications, and other information related to one's position at the University. Personal statements/"taglines/quotes are not permissible, as the primary purpose of the email service is for University business use. The use of images, italics, bold type, color, letter and backgrounds in email is not allowed for accessibility reasons.

2. Email Etiquette: When using a University email account, members of the University community are representing the University. As such, users must be professional in their email communications. Communicate with a respectful tone; avoid overly long messages, and use descriptive subject lines. Checking for proper spelling and grammar usage and re-reading for context before sending is highly recommended.

3. Use of Personal Email Accounts for University Business: University email is provided to employees for work purposes, and employees must strive to maintain the integrity of University data. For security and confidentiality reasons, automatic forwarding of University email to personal or other non-Salus email accounts is prohibited. In addition, all Salus business must be conducted with Salus email. Do not use a personal email account for University business unless authorized.

4. Personal Use: University email services may be used for incidental personal purposes if such use does not:
    - Directly, or indirectly interfere with the University business,
    - Interfere with the email user's employment or other obligations to the University

- Violate this policy, or any applicable policy or law.

Email arising from such personal use **will be subject to access consistent** with this policy or applicable law.

5. Transmission of PHI, PII, and other Sensitive data: All University users must take precautions and reasonable safeguards to limit access to PHI, PII, and sensitive data to only authorized individuals and to protect against unauthorized disclosures.
    - Email communication of PHI, PII, or sensitive data from a Salus.edu address to another Salus.edu address is secure;, however, encrypting these communications is encouraged as a matter of good practice. Content should be limited to the minimum necessary or a limited data set.
    - Sending email containing PHI, PII, and sensitive data to a third party outside of the Salus.edu domain must be encrypted. Content should be limited to the minimum necessary or a limited data set. The recipient's name and email address should be verified before the message is sent.

6. Occasionally email users incorrectly address confidential electronic communications that result in email being delivered to an unintended recipient. An unintended recipient will generally inform the sender and delete the message. When the sender is made aware that confidential information has been received by an unintended recipient, the event must be treated as a privacy/security incident and promptly reported to the Director of Network Security.

B. **Inappropriate Use of email:** Inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Inappropriate use includes using the email service in any way that:
    - Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections; see Intellectual Property Policy.
    - Violates, or encourages the violation of, the legal rights of others or federal and state laws;
    - Is unlawful, invasive, infringing, defamatory, malicious, or has a fraudulent purpose;
    - Contains profanity or obscenities, or is legally harassing to another individual
    - Uses or attempts to use the accounts of others without their permission, or misrepresents the identity of the sender of an email;
    - Collects or uses email addresses, screen names, or other identifiers without the consent of the person identified (including, without limitation, phishing, internet scamming, or password theft)

- Uses email user identifications for commercial purposes, including the loaning or selling of user identifications;
- Improperly exposes confidential or proprietary information of another person;
- Generates or facilitates unsolicited bulk commercial email that is prohibited by law;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Alters, disables, interferes with or circumvents any aspect of the email services, including testing or reverse-engineering email services in order to find limitations, vulnerabilities or evade filtering capabilities. ;
- Constitutes, fosters, or promotes pornography;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, incites violence, compromises national security, or interferes with an investigation by law enforcement.