Policy

Title:	Use of University Electronic Resources
Effective Date:	January 20, 2023
Approved By:	President's Council
Responsible Party:	Vice President of Technology & Learning Resources
History:	11/30/2022
Related Documents: Confidentiality of University Records & Information Policy; HIPAA;	

I. PURPOSE

In an effort to achieve its mission, Salus University ("Salus") provides electronic resources to faculty, students and employees to aid them in the effective performance of their job duties and/ or studies.

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 the Salus electronic communications systems, computer files and other stored communications and resources

E-Resources: is all electronic resources provided to university students, faculty and staff, authorized university guests, and all persons authorized for access or use privileges by the university, hereafter referred to as users. Examples of electronic resources include e-mail, Blackboard, Jenzabar, ADP, etc.

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

Within the university community, each person will have differing purposes for accessing E-resources; however, each person also has a shared responsibility to utilize those E-resources in a manner consistent with the university's policies, procedures and codes of conduct, including, as applicable, those found in the Student Handbook and the Employee Handbook. In addition, users are bound by the requirements of local, state, federal and international laws and contractual commitments.

By striving for compliance within our community, the university can assure its ability to provide, maintain and protect the confidentiality, integrity and availability of the university's data, systems, services and facilities.

This policy applies to all persons accessing or using university E-resources. This includes university students, faculty and staff, authorized university guests, and all persons authorized for access or use privileges by the university, hereafter referred to as users.

IV. PROCEDURE:

Resources Covered
E-resources covered by this policy include, without limitation:

- all university owned, operated, leased or contracted computing, networking, telephone and information resources, whether they are individually controlled, shared, standalone or networked,

- all information maintained in any form and in any medium within the university's computer resources, and

- all university voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, and storage media.

Additionally, all creation, processing, communication, distribution, storage and disposal of information by any combination of university E-resources and non-university resources are covered by this policy.

Authorized Use
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.

Authorization to users is given via issuance of a username and password from the Technology and Library Resources (TLS) department for faculty and staff network, VoIP phone, desktop, classroom technology, databases, wireless and all university provided software and technical resources.

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 180 days.

No Salus employee may access another Salus 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.

University Rights
The university reserves the right to access, monitor and disclose the contents and activity of an individual user's account(s) and to access any university-owned E-resources and any non-university-owned E-resources, on university property, connected to university networks. This action may be taken to maintain the network's integrity and the rights of others authorized to access the network. Additionally, this action may be taken if the security of a computer or network system is threatened, other misuse of university resources is suspected or the university has a legitimate business need to review such files (e.g., due to sudden death or incapacity of the employee). This action will be taken only after obtaining approval from the area vice president/dean appropriate to the circumstances, the president/provost/general counsel, when compelled by court order, or when there is deemed to be an urgent and compelling need to do so.

Users should be aware that electronic data, software and communications files are backed-up and stored. Items that were deleted may be preserved on backup tapes and retrieved if necessary. All activity on systems and networks may be monitored, logged and reviewed by system administrators or discovered in legal proceedings. In addition, all documents created, stored, transmitted or received on university computers and networks may be subject to monitoring by systems administrators.

User Responsibilities
Each user shall:
Be responsible for the security and integrity of information stored on his or her personal desktop system.

This includes:

- controlling and securing physical and network access to E-resources and data;
- properly logging out of sessions;
- monitoring access to their accounts, if a user suspects that their access codes have been compromised or that there has been unauthorized activity on their accounts, they are to report it to IT Security via the Help Desk and change access codes immediately;
- Choosing appropriate password(s) and guard the security of that password;
- Using only the access codes and privileges associated with their computer account(s) and utilize those account(s) for the purposes for which they were authorized; and
- Respecting and honoring the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement and use of E-resources.

Restrictions
Users may not do the following: (this list is not all-inclusive)

- Provide access codes to any non-user;
- Make use of accounts, access codes, privileges or E-resources to which they are no longer authorized;
- Tamper with, modify or alter restrictions or protection placed on their accounts, the university system or network facilities;
- Extend the network by introducing a hub, switch, router, wireless access point or any other service or device that provides more than one device to the university network;
- Use the university's internet access in a malicious manner to alter or destroy any information

available on the internet or on any network accessible through the internet for which he or she does not own or have explicit permission to alter or destroy;
- Introduce, create or propagate computer viruses, worms, Trojan Horses or other malicious code to university E-resources;
- Use knowledge of security or access controls to damage computer and network systems, obtain extra E-resources or gain access to accounts for which they are not authorized;
- Eavesdrop or intercept transmissions not intended for them;
- Physically damage or vandalize E-resources;
- Attempt to degrade the performance of the system or to deprive authorized users of E-resources or access to any university E-resources;
- Alter the source address of messages or otherwise forging email messages;
- Send email chain letters or mass mailings for purposes other than official university business;
- Use Salus University systems to relay mail between two non-university email systems;
- Engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with or threaten others;
- Comment or act on behalf of the university over the internet unless you have the authority to do so.
- Engaging in any activity that is illegal under local, state, federal or international law while utilizing Salus owned-resources or resources access through the Salus infrastructure.
- Engaging in any activity that can reasonably be deemed harmful to Salus University

Non-Organizational Use

Users may not use E-resources for:

- Compensated work outside of the university, except as authorized by the executive director of the Office of Research and Sponsored Programs (ORSP) pursuant to an approved grant or sponsorship agreement;
- The benefit of organizations not related to the university, except those authorized by a university dean or the director of an administrative unit, for appropriate university-related service;
- Personal gain or benefit;
- Political or lobbying activities not approved by the university's Office of Public Affairs;
- Private business or commercial enterprise;
- Commercial purposes, except as specifically permitted under other written policies of the university or with the written approval of Vice President for Technology & Learning Services.

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.

Copyright Compliance

In accordance with U.S. Copyright laws, the downloading, installation, configuration and operation of any 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 unauthorized 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

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, 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. The recipient's name and email address should be verified before the message is sent.

For Employees and Third Parties:

E-mail accounts will be created for employees 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.

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

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

Student E-Mail and other Electronic Resources

1. Upon Matriculation: into the Salus University academic program(s) student(s) and resident(s) are provided access to Salus University electronic resources. Every matriculated student and/or resident will be entitled to **one (1)** account and **one (1)** email address. This policy establishes the length of time extended access is provided for the following:

2. **Upon Graduation:** Each student or resident will be provided continued access to Salus Electronic resources for **one (1)** full year from their official date of graduation. Upon completion of the **one (1)** year extended access the student or resident account will be disabled and deleted. The student or resident must take individual responsibility to download and retain copies of their own electronic resources prior that time. These resources include but are not limited to the following services:

    - Electronic Mail
    - Blackboard
    - My Salus
    - Library Electronic Holdings

3. **Withdrawal or dismissal:** The student and/or resident account in question will be disabled immediately and deleted from the system.

4. **Administrative Action:** In certain circumstances Salus University administrative action(s) may require student and/or resident account(s) be disabled for a specific period of time. During such a

time Salus University will ensure and maintain its compliance with all Federal and State HIPAA and FERPA regulations.

Enforcement

Salus University 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.

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.