THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: GP-006-Email	
Version 5	**Effective Date: 11/02/2023**

Responsible Office: Office of Cybersecurity	Last Review: 11/02/2023 Next Review: 11/02/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The University of Tennessee Health Science Center (UTHSC) email services are provided to facilitate communication in the pursuit of academic and business endeavors. The purpose of this standard is to describe the availability and permitted use of this critical service for purposes appropriate to the University's mission.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This standard applies to all members of the UTHSC community entitled to email services.

Definitions

C-3 Data - Defined by UTHSC Standards, data whose unauthorized disclosure could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory, and contract obligations are major drivers for this risk level. Other drivers include but are not limited to, the risk of significant harm or impairment to UTHSC students, patients, research subjects, employees, guests/program participants, UTHSC's reputation, or the overall operation of the Location or essential services. This classification level also includes lower-risk items that, when combined, represent increased risk per GP-002 Data & System Classification.

Email - electronically delivered messages addressed to specific email account holders

Email Account - a NetID and password assigned to a user that allows access to email services

Sponsored NetID - a NetID not automatically generated for an active faculty, staff or student, but for someone affiliated with the University that needs access to specific systems. This type of NetID must be requested by a supervisor, business manager or

department head.

UTHSC Business - any activity or communication supporting the mission of UTHSC. This includes communication between internal and external individuals while representing the interests of UTHSC for any UTHSC-related purposes.

UTHSC Information Technology (IT) Resource - Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems), and information.

Responsibilities

Information Technology Services (ITS) is responsible for creating and maintaining UTHSC email accounts.

ITS Leadership is responsible for setting standards for the use of the UTHSC email system.

System Custodian is responsible for configuring the appropriate controls for the UTHSC email system.

UTHSC User is responsible for adhering to this standard and the security controls set forth in it.

Standard

UTHSC Email Address and Accounts

Faculty and Staff

Faculty and staff must use UTHSC email services to conduct and communicate University business. Incidental personal use of email is allowed, with the understanding that the primary objective of this email service is UTHSC-related and that occasional personal use does not adversely impact work responsibilities or the performance of the network.

Email services are provided only while a user is employed by the University, or 30 days after separation if the user has left on good terms. Once a user's electronic services are terminated, employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure. Upon separation, emails contained in the account remain the property of the UTHSC. Retirees wishing to continue using a UTHSC email address must have a sponsored account. See Sponsored Accounts below.

Faculty and staff email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed by authorized University officials for purposes related to University business per GP-003 Expectation of Privacy. UTHSC has the authority to access and inspect the contents of any equipment, files, or email on ITS resources.

Students

Email services are available for students to support learning and for communication by and between the University and themselves. The services are provided only while a student is enrolled in the University, or up to one year after the end date of the last term the student attended UTHSC classes. Once a student's electronic services are terminated, students may no longer access the contents of their mailboxes. Upon separation, emails contained in the account remain the property of the UTHSC.

Student email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed per GP-003 Expectation of Privacy. UTHSC has the authority to access and inspect the contents of any equipment, files, or email on ITS resources.

Sponsored Accounts

Individuals with special relationships with UTHSC who are neither employed nor enrolled at UTHSC, are granted limited email privileges, including an email address, commensurate with the nature of their relationship with the University with a sponsored NetID account. This type of account must be requested by a supervisor, business manager, or department head. UTHSC is free to discontinue these privileges at any time. The management of these types of accounts is described in AC-002.04-NetID Account Management.

Acceptable Use under University Policies

Email users have a responsibility to learn about and comply with UTSA Policy IT0110, Acceptable Use of Information Technology Resources and GP-004-Acceptable Use of IT Resources. Violation of UTHSC standards and practices (including this one) may result in disciplinary action dependent upon the nature of the violation. Examples of prohibited uses of email include, but are not limited to:

- Intentional and unauthorized access to other people's email

- Sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail
- Use of email for commercial activities or personal gain (except as specifically authorized by University policy and in accordance with University procedures)
- Use of email for partisan political or lobbying activities
- Sending of messages that constitute violations of the University of Tennessee's HR-0580-Code of Conduct
- Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications
- Use of email to transmit materials in a manner that violates copyright laws. Abuses of UTHSC's email services should be directed to the Office of Cybersecurity at abuse@uthsc.edu.

Security and Privacy of Emails

UTHSC attempts to provide secure, private, and reliable email services by following sound information technology practices. However, there are always emerging risks that allow attackers to compromise the confidentiality, integrity, and availability of our emails. Therefore, email users should exercise extreme caution in using UTHSC email to communicate sensitive matters. All data contained within an email message, or an attachment, must be secured commensurate with the criticality of the information per GP-002-Data & System Classification.

Email is a business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email. In that case, the email must be retained according to pertinent University of Tennessee and/or State retention requirements. Users of UTHSC email services also should be aware that the Tennessee Public Records Act & Tennessee Sunshine Law (Open Meetings Act) and other similar laws jeopardize the ability of UTHSC to guarantee complete protection of email.

Best Practices in the Use of Email

C-3 Data or Information

When sending information categorized as C-3, per GP-002-Data & System Classification (such as data covered by HIPAA and FERPA), the user must encrypt the message if sent via email. To encrypt an email, add the word **encrypt** anywhere in the subject line of an email sent from the sender's UTHSC account. More

information about encrypted email is found at https://uthsc.edu/its/cybersecurity/encrypt-your-email.php. The University of Tennessee UT Vault can also be used to send encrypted messages. Students, staff, and faculty members from any UT institution can send and receive encrypted emails, including emails from non-UT entities. More information on UT Vault is found at vault.utk.edu.

Phishing

Phishing attacks use email to collect personal and financial information or infect devices with malware and viruses. UTHSC email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Clicking a link in an email message or opening an attachment may allow bad actors to install malicious programs on the workstation.

Identity Theft

Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.

Password Protection

UTHSC requires the use of strong passwords for the protection of our NetID and email. Requirements for a UTHSC password is given in AC-002.02-Password Management and Complexity.

Departmental Email Boxes

Departments that provide services in response to email requests should have a shared mailbox created to help support departmental functional continuity for managing requests sent via email. These accounts should have one owner accepting responsibility for the account and must be monitored.

Forwarding Email

UTHSC email users may not forward emails to a non-UTHSC email address, except to domains that have been approved for forwarding. Staff email users on an extended absence should create an Out of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.

Compromised Accounts

An email account that has been compromised, whether through password cracking, social engineering, or any other means, must be promptly remediated with the appropriate means. Such appropriate means will include a password reset, review of account settings, computer scans, and malware disinfection to prevent possible leakage of PII, spamming, potentially infecting others, and degradations of network service. If the account is being used to harm UTHSC, the Chief Information Security Officer (CISO) or designee will direct the ITS Infrastructure Team to disable the account until remediations can occur.

Representation

Email users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of UTHSC or any unit of UTHSC unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing UTHSC. Refer to SC-002.01-Offical Communications Use & Protections for guidance.

Alternative Means of Communication

Users should be aware that there are alternative means of communication that may be more efficient than email. For example, the use of Microsoft Teams for individual or group conversations and meetings is an approved and appropriate alternative that allows for flexibility during collaborations.

Exceptions to this Standard

Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. UTSA IT Policy 0110 – Acceptable Use of Information Technology Resources
2. UTSA HR-0580-Code of Conduct
3. AC-002.04-NetID Account Management
4. GP-001.02-Security Exceptions and Exemptions to ITS Standards and Practices
5. GP-002-Data & System Classification
6. GP-003 Expectation of Privacy

7. GP-004-Acceptable Use of IT Resources
8. SC-002.01-Offical Communications Use & Protections