Name of Policy: Electronic communication policy **Policy Number**: 3364-65-07 **Approving Officer**: President **Responsible Agent**: Vice President, CIO/CTO **Scope**: All University organizational units			**Revision date:** January 12, 2017 **Original Effective Date**: January 29, 2009
☐	New policy proposal	☐	Minor/technical revision of existing policy
☒	Major revision of existing policy	☐	Reaffirmation of existing policy

(A) Policy statement

The University of Toledo provides electronic mail ("e-mail"), communication, and collaboration services to support academic, research, medical, and administrative functions of the institution. University electronic communication services are to be used responsibly within the normal standards of professional and personal courtesy and conduct. The use of electronic communication services is a privilege, not a right, and it should be treated as such by all users.

(B) Purpose

This policy establishes guidelines for the responsible and efficient use of University of Toledo ("University") electronic communication services, and to clearly set forth the rights and responsibilities of the university's authorized users regarding these services, including e-mail.

(C) Scope

Electronic communications and associated attachments transmitted or received over the university network are subject to the provisions of this policy. According to Ohio law, electronic communications such as e-mail are generally considered to be public records to an equal degree of an equivalent communication in physical form. E-mail communications written and sent in the course of university business are subject to

applicable provisions of this policy, regardless of whether the communication was sent or received on a public or privately owned personal computer or messaging system.

(D) Definitions

(1) E-mail. E-Mail means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval**.**

(2) Payment card information ("PCI"). PCI is information associated with payment cards such as credit card numbers and associated personal identification numbers.

(3) Personally identifiable information ("PII"). PII is information that can be used to distinguish or trace an individual's identity. Examples of PII include social security numbers or information that, when combined or used with other identifying information, is linked or linkable to a specific individual.

(4) Protected health information ("PHI"). PHI is healthcare information that could reasonably lead to the identification of an individual, either by itself or in combination with other reasonably available information. Consult the university Office of Legal Affairs for guidance about whether a particular University organizational unit is a "covered entity" for purposes of HIPAA.

(5) Public records. Public records means all writings made, maintained, or kept by the state, or any agency, institution, or subdivision thereof, for use in the exercise of functions required or authorized by law or administrative rule, or involving the receipt or expenditure of public funds.

(6) Student educational records. Student educational records include all records maintained by the university concerning a student, including admissions, academic, financial, and placement records. The university's rule 3364-71-15 of the Administrative Code, "Confidentiality of Student Records (FERPA)," further defines student educational records and our responsibilities to protect them under the

Family Educational Rights and Privacy Act (FERPA) of 1974.

(7) Sensitive data. Sensitive data is data for which the university has an obligation to maintain confidentiality, integrity, or availability.

(E) Policy

Electronic communications must comply with these general principles and rules:

(1) Authorized users.

Authorized users of the campus electronic communications or electronic mail systems may include the following based upon need and available resources:

(a) Employees, agents, and affiliates of the university.

(b) Students designated as active by the registrar's office.

(c) Other users as approved by the vice president, CIO/CTO or designee.

(2) Management of electronic communications.

Access to university e-mail, when provided, is a privilege that may be wholly or partially restricted by the university without prior notice and without the consent of the user. Individual e-mail privileges may be suspended or revoked as conditions warrant to ensure the overall health and security of the university's messaging system.

(a) E-mail accounts assigned to employees, affiliates, and other authorized users who elect to leave the university are deleted after the user departs. Those employees who have been terminated or who have received notification of termination may be immediately restricted from access to their account, unless expressly permitted by the vice president, Human Resources or designee.

(b) Students not currently enrolled at the university may retain their assigned e-mail accounts.

(3) Authorized access and disclosure.

The university reserves the right to monitor, inspect, and disclose usage of electronic communications without prior notice in accordance with state and federal law. The university information security office may institute scanning, sandboxing, and/or blocking technologies for the protection of the university and university owned information technology assets.

E-mail and other documents needed by a departing employee's department may be identified and archived by the department on request to the departing employee. Access to a terminated employee's e-mail after the terminated employee's departure may be granted to another individual upon approval of the vice president, Human Resources, or designee.

(4) Privacy and confidentiality.

The confidentiality and privacy of e-mail messages cannot be guaranteed. Disclosure of electronic messages may be made at any time due to legal discovery, public record request, or other legal request. Authorized users should review the content and attachments of e-mail to ensure that the message would not be a source of embarrassment to the sender, to the recipient, or to the university.

Authorized users should exercise extreme caution when using e-mail services to communicate confidential or sensitive matters. Users should employ protections including password protecting files, encrypting messages, or hand delivery of electronic files. Users that are unsure how to protect content should contact the information technology help desk for guidance.

(5) Application of Ohio public records law to email.

E-mail and other electronic messages are subject to the same legal requirements as most other forms of communication. The Ohio Public Records Act, Ohio Revised Code §149.43 governs

availability of public records. The Ohio Public Records Act treats electronic records in the same manner as an equivalent paper record.

Email and other electronic messages that document the functions, policies, and procedures of the university are public records that must be retained in either paper or electronic format. Disposition decisions regarding individual documents should be made in accordance with the definition of public records and in accordance with university record retention policy.

(6) Retention.

University records in electronic form including documents, email, and backup copies should be retained in accordance with the university's record retention schedules that apply to non-electronic records of similar subject and content. If necessary, specific departmental retention schedules for unique records in electronic form can be established. The university archivist is responsible for establishing records retention schedules. Further guidance on the university's public records responsibilities may be found at:

http://www.utoledo.edu/policies/retention.html

(7) Sensitive data.

Electronic communications may contain sensitive data, including health information (PHI), personally identifiable information (PII), payment card information (PCI), and student educational records. In the event that sensitive data is sent in an e-mail message, it should be protected appropriately and sent to only those individuals with a need to know. Sensitive information shall not be transmitted to any external, e-mail addresses unless it has been encrypted through the university's encrypted e-mail gateway. Authorized users can contact the information technology help desk for further guidance on the university's encrypted e-mail gateway.

(8) Institutional communication.

Communications by e-mail to the entire university address book or to large portions of the address book must be approved and distributed by the office of marketing and communications. The office of marketing and communications will work with the departments to select and utilize the most appropriate means to disseminate information to the entire university community. The information should be sent in a manner that prevents identification of individual's protected information including e-mail addresses and does not allow replies to the entire group.

This requirement does not apply to critical communications sent by pre-approved senders, such as electronic infrastructure outage notices, health, security, and safety alerts and messages from the university president.

(9) Personal use by employees.

University equipment and e-mail service may be used by employees for incidental personal purposes so long as the personal use does not harm:

(a) the performance of his or her job responsibilities;

(b) the business use of e-mail by other authorized users;

(c) the university's technology budget or cost(s);

(d) the user's employment or other obligations to the university.

(10) Responsible use of electronic communications.

In order to ensure responsible use of email, authorized users should ensure that:

(a) Incoming messages or attachments from unknown or untrusted senders are not opened by the recipient user;

(b) Addresses on outgoing messages are those of the correct intended recipients of the information transmitted;

(c) Virus checking is performed on all attachments before opening them on the university network;

(d) Broadcast e-mails sent to large groups (e.g. class groups or other distribution groups) protect the identity of list members and do not allow replies to the entire group;

Note: This can be accomplished by placing these addresses in the “Bcc” line of the e-mail being sent.

(e) Appropriate disclaimers are attached to applicable outgoing e-mail. Examples of such disclaimers include:

(i) “This e-mail and any files transmitted are confidential. They are intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, be advised that you have received this e-mail in error, and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.”

(ii) “This message and any response to it may constitute a public record and therefore may be available upon request in accordance with Ohio public records law.”

(11) Prohibited activities.

The following practices are prohibited on university electronic communication systems:

(a) Auto-forwarding of e-mail messages to a system that is out of the university's custody or control;

(b) Harassment, intimidation, or threatening another person;

(c) Accessing or distributing obscene, sexually explicit, or abusive materials, including but not limited to racial slurs, insensitive gender-related comments or any comment or other material

that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, disability or other protected class;

(d) Illegally distributing copyrighted materials;

(e) Initiating or forwarding chain messages;

(f) Pursuing personal business interests not related to the university;

(g) Any purpose that is illegal, against policy, or against the university mission;

(h) Deliberately sending large volumes of mail or attachments to purposely waste resources;

(i) Selling or soliciting the purchase of personal items;

(j) Obtaining access to the electronic communications of others for the purpose of satisfying idle curiosity, with no substantial university purpose;

(k) Attempt unauthorized access to electronic communications or attempt to breach any security measures on any communications system, or attempt to intercept any e-mail or other electronic transmissions without proper authorization; and

(l) Employing false identities or unauthorized sending of electronic messages on behalf of others.

(12) Violations.

Violations of this policy will be subject to the university's disciplinary process and may result in disciplinary action up to and including termination. Minor violations will result in removal of the offending device from the university network at the discretion of information technology or administration. Criminal activity subject to applicable state and federal criminal penalties may be referred to law enforcement as appropriate.

Approved by: /s/ Dr. Sharon Gaber, PhD President January 12, 2017 Date Review/Revision completed by: Senior Leadership Team Vice President, CIO/CTO	**Policies Superseded by This Policy:** • *3364-65-01, effective date July 18, 2014* • *Policy number changed from 3364-65-01 to 3364-65-07 (effective date January 12, 2017)* • **Initial Effective Date:** January 29, 2009 • **Review/Revision Date:** August 1, 2012; July 18, 2014; January 12, 2017 • **Next review date:** January 12, 2020