



Email Transmission and Use Policy

Policy ID:	8.2.1.13
Version:	2.1
Policy Owner:	Chief Information Officer (CIO)
Policy Approver:	President, University of Oklahoma

PURPOSE

This Email Transmission and Use policy establishes the rules for using email to send, receive, or store electronic mail and informs email users of their responsibilities associated with such use.

SCOPE

This policy applies to all staff, faculty, students, contractors, and their associated contractors, as well as temporary workers and those who are provided email services managed by or for the University.

POLICY STATEMENTS

University Business¹

All University Business that is conducted on email is to be done only through the OU-provided email system, which may include a University-approved patient portal and/or an OU-assigned email account. University Personnel (faculty, staff, student employees, residents, trainees, volunteers) and affiliates who have OU email accounts shall not use personal email accounts or non-University email systems to conduct OU Business.

Auto-forwarding or Auto-redirecting Email Messages

University Personnel must not auto-forward or auto-redirect their OU email to non-University provided systems. Examples of non-University provided email systems include, but are not limited to, OMRF, VA, Gmail, Outlook/Hotmail, Yahoo, AOL, and email provided by other Internet Service Providers (ISP) such as Cox or ATT.

University Personnel may send OU email to authorized internal and external (subject to encryption requirements) recipients for authorized purposes. For example, PHI may be sent only to authorized recipients and only for treatment, payment, or health care operations purposes. Users may send ePHI to third parties with whom the University has a Business Associate agreement in place (contact Purchasing or the Office of Research Administration to confirm Business Associate status of a particular vendor or sponsor).

Student records subject to FERPA may be sent only to University officials who have a legitimate educational purpose and others authorized by law.

Encrypted Transmission of Confidential or Regulated Email Outside OU

If confidential or regulated University information, such as PHI, FERPA, GLBA, PII, CUI, ITAR or

¹ University Business: Work performed as part of an employee's job responsibilities, or work performed on behalf of the University by faculty, staff, volunteers, students, other trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. University business includes the use of a Portable Computing Device to access OU email, non-public University systems, networks, or data in the performance of work for the University.

confidential research data, must be transmitted over an external network (e.g., the Internet), the email communication channel and/or the email message must be encrypted. Message encryption options include typing [secure] or [ouencrypt] in the email subject line, using the Secure Email plugin, or using a University-approved Patient Portal. (For additional policy regarding sending PHI via email, refer to HIPAA Privacy Safeguards policy.)

Third-Party Email Services

Third-party solutions that contain their own email delivery systems are outside of the University's control; however, those that attempt to impersonate an official University email account or address to send directly on behalf of the University must submit a request using the [General Help Request](#) form that includes: a) email address of the account, b) systems impacted, c) IP (internal and external) addresses of the connecting services, and the service owner.

Portable Computing Devices

To protect confidential and regulated University information that resides within the OU email system, University-owned Portable Computing Devices that connect to the OU Email environment, including webmail, are required to be encrypted and to have baseline security settings applied. See the OU Cybersecurity and End User Device security policies for these requirements.

Confidentiality Notice

Emails that contain confidential University information, such as PHI, or regulated data must include a confidentiality notice in the signature block, such as: *Confidentiality Notice: The information contained in this message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, distribution, or retention is strictly prohibited. If you are not the intended recipient or believe that you have received this message in error, please notify the sender immediately by reply email and permanently delete the original message.*

Acceptable Email Use

The following activities are prohibited when using OU electronic messaging and communication services:

- Sending unsolicited email or other electronic messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material.
- Engaging in any form of harassment via email, telephone, or text messaging, whether through the content, frequency, or size of the messages.
- Including any misrepresentations or misleading information in email header information.
- Creating or forwarding chain letters or communications relating to Ponzi, pyramid, or other fraudulent or misleading schemes of any type.
- Using unsolicited electronic messages, originating from within OU's networks to advertise any service hosted by an Information Systems, unless specifically authorized in writing by the Office of Legal Counsel.
- Posting the same or similar non-business-related messages to large numbers of Individual Users or other individuals.

Email Privacy

All OU email content and systems are owned by the University; as such, all user activity is subject to logging and review. OU email may be subject to release under the applicable law. OU email is subject to open records requests. Refer to the OU Acceptable Use policy for additional information.

Phishing Preparedness

Phishing emails look sophisticated and can be hard to separate from authentic messages. Follow these best practices to be prepared to spot and prevent a phishing attack:

- Don't send passwords or any personal sensitive information over email, instead contact any institution requesting this information directly.
- Don't reply to, click on links, or open attachments from senders you don't know.
- Don't call the number in an unsolicited email or give sensitive information to a caller you don't know personally.
- Report impersonated or suspect email to OU IT Security by using the Report Phish button made available at <https://portal.office.com>.
- Be cautious about opening attachments, even from trusted senders.

REFERENCES

- National Institute of Standards and Technology Cybersecurity Framework (CSF), PR.DS-2
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information
- HIPAA Standards for Safeguarding Customer Information, 164.308 (a)(ii)(B), 164.308 (a)(4)(i), 164.308 (a)(4)(ii)(C), 164.308 (b)(1), 164.312 (e)(1), 164.312 (e)(2).
- Gramm-Leach-Bliley Act (“G–L–B Act”), Section 501(b)
- Payment Card Industry Data Security Standard (PCI DSS)
- Family Educational Rights and Privacy Act (FERPA): 20 U.S.C. §1232g; 34 CFR Part 99
- NIST Special Publication 800-53 rev 4, SC-8 Transmission Confidentiality and Integrity
- NIST Special Publication 800-53 rev 4, SC-13 Cryptographic Protection
- NIST Special Publication 800-53 rev 4, AC-4 Information Flow Enforcement
- NIST Special Publication 800-53 rev 4, AC-20 Use of External Information Systems

ENFORCEMENT AND COMPLIANCE

Failure to comply with this Policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This standard is approved and enforced by the OU Chief Information Officer (CIO). Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this Policy. Such instances must be documented following the IT Policy and Standards exception process, and may require the approval of the Chief Information Officer, Chief Information Security Officer, and/or the Data Owner depending upon the level or risk introduced with the exception.

Figure 1 - Revision History

Revision Date	Version	Revised By	Changes Made
0.1	02/24/2017	OUHSC IT	Baseline Version
0.2	02/24/2017	OUHSC IT	Updated Regulatory References
0.3	02/24/2017	OUHSC IT CIO	Minor changes: See SharePoint track changes
0.4	03/02/2017	OUHSC Legal Counsel (Jill Raines)	See SharePoint track changes.
.05	04/17/2017	OUHSC Legal Counsel (Jill Raines)	See SharePoint track changes.
.06	04/19/2017	OUHSC CTO	See SharePoint track changes.
.07	05/09/2017	OUHSC Information Security Review Board (ISRB)	See SharePoint track changes.
.08	05/10/2017	OUHSC IT Managers	See SharePoint track changes.
.09	05/17/2017	ISRB	See SharePoint track changes.
1.0	05/25/2017	OUHSC Deans' Council and Senior Vice President and Provost	Change "redirect" to "auto-redirect"
2.0	01/17/2021	OU IT GRC	Expanded the scope to include all OU campuses. Applied OU IT Security Policy style sheet.

Figure 2 - Approval History

Version	Approval Date	Approved by:
1.0	05/25/2017	OUHSC Deans' Council and Senior Vice President and Provost
2.1	06/29/2022	Cybersecurity and Infrastructure Advisory Committee (CIAC)
2.1	07/11/2022	University President

Figure 3 - Review History

Version	Review Date	Reviewed by:
.05	04/17/2017	OUHSC Legal Counsel
.06	04/19/2017	OUHSC IT
.07	05/09/2017	OUHSC Information Security Review Board
2.0	05/07/2022	Refer to OU IT PSP Program Page
2.1	06/29/2022	Cybersecurity and Infrastructure Advisory Committee (CIAC)