Northwestern
INFORMATION TECHNOLOGY

Approving University Official(s): Vice President for Information Technology/Chief Information Officer
Responsible Office: Information Security
Effective date: November 30, 2022

Electronic Communications Standard

1. Summary

This Electronic Communications Standard (hereinafter referred to as the "EC Standard") outlines the necessary actions each person or organization with access to Northwestern University electronic communications is responsible for taking to ensure the integrity of the systems and data for which Northwestern is responsible.

Electronic Communication (such as electronic mail, instant messaging, and audio/video conferencing) is a primary means of communication both within Northwestern University and externally. It allows quick and efficient conduct of University Business. Compliance with this Standard ensures that Institutional Data are appropriately managed and secured, and ensures recipients of Electronic Communications can feel confident of the integrity and authenticity of the source, further safeguarding the reputation of the University.

Departments and units may impose more, but not less, stringent procedures as they deem appropriate or necessary to preserve the University's information assets.

2. Authority

The authority for implementation and enforcement of this EC Standard is based on the Information Security Policy, effective January 1, 2022.

The implementation of this EC Standard will adhere to the Appropriate Use of Electronic Resources Policy, including provisions on the privacy and confidentiality of Electronic Communications.

3. Purpose Statement

This EC Standard standardizes platforms used for Electronic Communications of University Business to ensure Institutional Data (including verbal communications via electronic means) are appropriately managed and secured, thereby providing users of Electronic Communications confidence that the communications and data is authenticated, and protected, further safeguarding the reputation of the University.

Per this EC Standard, only an approved Northwestern-provided or Northwestern-affiliated Electronic Communications Platform may be used whenever University Business is conducted, or Institutional Data is exchanged via Electronic Communications. Specifically, all email, instant messaging, and videoconferencing for University Business must be conducted on a platform provided by and/or approved by Northwestern Information Technology ("Northwestern IT") for that purpose.

4. Scope and Audience

The scope of this EC Standard applies to all information and communication technology ("ICT") that can be used to transmit or receive Electronic Communications (such as email, instant messaging, or videoconferencing). The audience of this EC Standard is everyone – faculty, staff, students, affiliates, suppliers, and anyone else – who performs University Business on behalf of the University.

5. Control Requirements

The following are foundational and fundamental control requirements that all schools and business units must follow. University schools or business units that have additional regulatory or contractual requirements may require specific control requirements or capabilities in addition to what is defined below.

1. An Electronic Communications Platform approved by Northwestern IT must be used whenever University Business is conducted. Everyone who performs University Business on behalf of the University (e.g., faculty, staff, students employed by the University, etc.) shall not use any unapproved communication platforms to send or receive Electronic Communications in the course of performing University Business.

2. Any Electronic Communications Platform not approved by Northwestern IT may be submitted to the Information Security Office (ISO) for consideration of approval or exception. The Information Security Office, in consultation with the Information Security Advisory Committee (ISAC), will ensure communications platforms comply with applicable policies, standards, laws, and regulations to minimize the risk of Institutional Data being inadvertently sent or disclosed to unauthorized individuals or entities.

3. Electronic Communications records (e.g., emails, instant messages, videoconference recordings) that contain Level 2 or Level 3 (defined in the Data Classification Policy) may not be copied or downloaded to any devices or data storage platform that is not approved and secured according to Level 2, Level 3, or Level 4 Framework Controls (as defined in the Data Classification Policy). Northwestern IT-approved Electronic Communication Platforms may be used on personally owned mobile devices such as mobile phones, tablets, watches, etc., for Level 2 or Level 3 data, if those devices are appropriately secured following University policies and standards for protection of endpoint devices. **Level 4 data is not permitted on any University System, including personal devices.**

4. Northwestern shall provide, upon request to the Information Security Office, appropriate endpoint protection to any person who is required to conduct University Business on their personal computer or device. Members of the University Community are advised, however, the use of personal devices (including mobile phones/devices) for University Business may result in such devices being subject to subpoenas or other legal discovery actions as personal devices may not be protected by Northwestern legal processes. Additionally, personal devices (including mobile phones/devices) for University Business may be subject to sequestration by the University pursuant to federal regulation and/or University policy.

5. Emails (including calendar entries and invitations), file attachments, and other Institutional Data shall not be automatically forwarded through any means to a non-approved third-party or affiliated Electronic Communications Platform or email domain.

6. Emails (including calendar entries and invitations) and file attachments may be manually forwarded by a University user to a non-approved third-party or affiliated email domain or Electronic Communications Platform as long as such forwarding is in furtherance of University Business, and/or and will not result in the inappropriate disclosure or loss of Institutional Data.

7. Requests for approval of email domains or Electronic Communications Platform not listed in this EC Standard may be submitted to the Information Security Office for review and approval. A list of platforms and/or domains approved for use by specific Schools or business units is available by request from the Information Security Office.

6. Standard Implementation

The following are foundational elements for ensuring compliance with the requirements outlined in this EC Standard. Additional requirements may be imposed for members of the University community with access to Confidential Data or Contractually/Legally Restricted Data.

Electronic Mail (Email):
All faculty, staff, students and other approved members of the University community doing University Business will be assigned an Official set of unique logon credentials and Email Address, which is the address that University Business is to be sent and received. The Official Email Address will be the address to which all official University correspondence is sent. Each Official Email Address will include a mailbox assigned to one of the Northwestern-approved email systems:

- Microsoft Exchange 365 (@northwestern.edu addresses)
- Google Workspace (@u.northwestern.edu addresses), primarily for undergraduate students

Official Email Addresses may be provisioned with other email domains listed below depending on an individual’s university affiliation(s)

Individuals may be provided multiple mailboxes to accommodate multiple types of University Business. For example, students may be assigned a Microsoft 365 mailbox for the purposes of teaching or research, or faculty may be assigned a Google Workspace mailbox for the purpose of collaboration with students. Individuals with multiple mailboxes should use their Official Email Address for all University Business except that for which another mailbox was specifically assigned.

Personal use of an Official Email Address is allowed, provided that such personal use:

a. Does not materially interfere with performance of University Business;
b. Does not interfere with the performance of a University Network; and
c. Is in compliance with this and other University policies and standards.

NOTE: Personal communications through an Official Email Address may fall under the Appropriate Use of Electronic Resources Policy and may be viewed by the University, for purposes outlined in that Policy.

Instant Messaging:
Employees, students, and approved contractors/affiliates are permitted to conduct University Business over instant messaging platforms approved by Northwestern IT. The current approved instant messaging platforms are:

- Microsoft Teams (when accessed through a user’s University-assigned Microsoft 365 account)
- US or Qatar-based mobile communication provider SMS, MMS, RCS, or iMessage platforms.
- Chat capabilities within approved Northwestern Business Applications, such as Canvas or Zoom.

Video or Audio Conferencing:
Employees, students, and approved contractors/affiliates are permitted to conduct University Business over Northwestern-provided or Northwestern-approved video or audio conferencing. The current Northwestern-provided video/audio conferencing platforms are:

- Zoom (when accessed through a Northwestern license)
- Microsoft Teams (when accessed through a user's University-assigned Microsoft 365 account)
- PGI GlobalMeet (audio conferencing only)

Individuals should exercise caution when attending meetings hosted by platforms from outside Northwestern, as Northwestern cannot verify the security or integrity of the communication.

Other platforms for electronic communications, including, but not limited to, WebEx, GoTo Meeting, WhatsApp, or Google Chat (even if provided through Northwestern) are not approved business communication platforms and should be avoided when possible. When conducting University Business with external parties using these and other, unapproved platforms, members of the University community should exercise caution as the security and privacy of Intuitional Data is unknown.

Additional platforms may be approved as an exception by the Information Security Office for electronic communications at the individual school/unit level. If you have any questions about whether a specific platform can be used for University Business, please contact the Information Security Office.

7. Remedies and Compliance

Requests for any exceptions to this Standard should be submitted to the Information Security Office and will be reviewed in consultation with the Information Security Advisory Committee.

Lack of compliance to this Standard could result in sanctions relating to the individual's use of ICT resources at Northwestern, or other appropriate remedies as authorized by the Appropriate Use of Electronic Resources Policy, Faculty Handbook, Staff Handbook, or Student Handbook. Civil or criminal penalties may also apply if non-compliance results in the loss or disclosure of confidential, restricted, or regulated information.

8. Definitions

Electronic Communications or Electronic Communications Platform: For the purposes of this Standard, Electronic Communications are any method of exchanging or transmitting Institutional Data or conducting University Business over electronic mail (email), instant messaging (including chat or text message functionality), video conferencing, or audio conferencing. File sharing via any platform previously listed is covered as part of this Standard, however, other methods of file sharing are covered by a separate Standard with discrete control requirements.

Information Security Advisory Committee (ISAC): A University-wide technology governance group that is responsible for monitoring the security maturity and controls of the University, and providing approval for all security vulnerability exceptions that pose a significant or high risk to the University.

Institutional Data: All data that the University is responsible and accountable for protecting. This data includes, but is not limited to, data the University owns, collects, intellectual property owned by faculty or others, staff data, student data, faculty data, research data, personal information, alumni data, vendor and contractor data, and data that the university shares or provides to third parties for storage, processing, and analysis.

Northwestern- or University-owned Systems or Devices: ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are the responsibility of the University to account for and provide appropriate safeguards. This includes ICT purchased (either directly or by reimbursement) from a University chart of accounts, or devices with documented ownership or responsibility transferred to the University from another institution or organization (such as ICT loaned to a laboratory or department).

Northwestern University Email Domains: The following email domains are approved and provided by Northwestern University for the purposes of Electronic Communications:

northwestern.edu
kellogg.northwestern.edu
law.northwestern.edu
qatar.northwestern.edu
ads.northwestern.edu
chem.northwestern.edu
ci.northwestern.edu
comm.northwestern.edu
e.northwestern.edu
earth.northwestern.edu
ece.northwestern.edu
icair.org
ilcancer.org
ilcancercollab.org
itcs.northwestern.edu
lotus.phys.northwestern.edu
mail.it.northwestern.edu
mses.northwestern.edu
nuwildcat.mail.onmicrosoft.com
pim.northwestern.edu
relay.kellogg.northwestern.edu
thirdpartyemail.northwestern.edu
u.northwestern.edu
wcas.northwestern.edu
wnur.org

Northwestern University Affiliate Email Domains: The following email domains are approved as affiliates to Northwestern University for the purposes of Electronic Communications:

nm.org
nmh.org
northwesternmedicine.org
nmff.org
cadencehealth.org
cdh.org
childrensmemorial.org
lfh.org
livingwellcrc.org
luriechildrens.org
sralab.org
ric.org

Personal or Personally-owned Devices: ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are wholly owned by an employee, student, or affiliate of the University. This includes devices for which a user receives a stipend or subsidy, such as a mobile communication allowance.

University Business Any activity carried out under the auspices of Northwestern University and in furtherance of the University’s mission.

University Network: The University Network is the infrastructure and equipment that connects information and communication technology (ICT) to enable the exchange of data and information at Northwestern. This includes connections that are limited to within the university as well as the broader Internet. The University Network includes both physical wired (wall jacks, wiring, routers, switches, etc.) and wireless network components, including ad-hoc wireless networks. The University Network also includes connections provided by a third-party telecommunications provider but managed by Northwestern IT, or network paths over hardware or software (such as VPN, site-to-site tunnel, etc.) by which a user or ICT device receives a Northwestern-managed IP address, telephone number, or other Northwestern-owned network descriptor.

9. Related Policies, Standards, Guidelines or Procedures

Information Security Policy
Appropriate Use of Electronic Resources
Data Classification Policy

10. Contact Information

The following office can address questions regarding this Standard:

Northwestern Information Technology, Information Security Office
phone: (847) 491-HELP
email: security@northwestern.edu

11. Revision History

Date	Version	Modified By	Comments
October, 2022	1.0	Northwestern IT/ISO	New

12.Standard URL:

https://www.it.northwestern.edu/policies/electronic-communications.html