Northeastern Illinois University's (the "University") Information Technology Resources (ITR) exists to support the mission of the University and are to be used appropriately and in accordance with this policy, related policies, as well as local, state and federal laws.

This Policy sets out the direction, expectation, and guidelines for use of the University's ITR including, its network and network resources, hardware and software (including applications), remote technology, communications facilities, and data.

- All users of University Information Technology Resources (ITR)
- All users who conduct University business using its ITR either from the University's networks or external networks.

Information Technology Resources (ITR) - all electronic and technology facilities, services, devices and data used for information processing, transfer, storage, display, printing, and communications by NEIU. These include, but are not limited to, networks, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, computing and electronic communications devices and services, modems, email, faxes, telephones, voicemail, video, multi-function printing devices, mobile devices, multimedia and instructional materials, and third-party hosted services used to conduct NEIU business.

User - An individual or entity authorized to use NEIU Information Technology Resources (ITR).

Illinois Criminal Code of 2012 (720 ILCS 5/16D-3, 720 ILCS 5/26.5-2)

University Information Technology Resources are to be used to advance the University's mission.

Acceptable Use of Information Technology Resources
I1.01.1
Effective date: 01/02/2007
Last revised: 07/29/2022

Responsible Officer: Chief Information Officer

Responsible Office: University Technology Services

Acceptable Use of Information Technology Resources
I1.01.1
Effective date: 01/02/2007
Last revised: 07/29/2022

Responsible Officer: Chief Information Officer

Responsible Office: University Technology Services

or electronic device at any time. Any monitoring of a specific individual's voice mails, email exchanges, internet use, or personal computer files, shall be done only with reasonable suspicion of improper conduct and with written notice, when necessary. The Chief Information Officer or designee must approve any request to monitor, inspect or examine electronic content on any University-owned