Northeastern University

INFORMATION TECHNOLOGY SERVICES

Effective Date: March 5, 2014

Date Revised: May 2, 2016

Supersedes: N/A

Related Policies:

- **Policy on Confidentiality of University Records and Information**
- **Policy on Enterprise Passwords**
- **Policy on Professional Standards and Business Conduct**

Responsible Office/Department: Office of Information Security

Keywords: Security, violation, appropriate, hacking, misuse

Policy On Appropriate Use Of Computer And Network Resources

I. Purpose and Scope

The information systems of Northeastern University are intended for the use of authorized members of the community in the conduct of their academic and administrative work. Northeastern's information systems consist of all networking, computing and telecommunications wiring, equipment, networks, security devices, passwords, servers, computer systems, computers, computer laboratory equipment, workstations, Internet connection(s), cable television plant, University-owned mobile communications devices and all other intermediary equipment, services and facilities. These assets are the property of the University. This Policy describes the terms and conditions of use for Northeastern information systems.

This policy applies to any and all users of these resources both authorized and unauthorized.

II. Definitions

PII: Personally Identifiable Information, Certain data defined in applicable laws of a state or country which can, separately or in combination, identify an individual. "PII" also can be defined by university policy.

PHI: Personal Health Information. Information protected under HIPAA.

HIPAA: Heath Insurance Portability and Accountability Act. Federal law protecting and defining the appropriate use of PHI

and medical records. For purposes of this Policy, "HIPAA" includes the HITECH Act amendments to HIPAA.

VPN: Virtual Private Network. Technology used for secure communication from a remote location to a network resource.

RESNet: The residential student network of Northeastern University.

NUNet: The administrative network of Northeastern University.

NUWave: The Wireless network of Northeastern University.

III. Policy

User Rights and Responsibilities Sections – GENERAL

Part 1

Assent to Terms of the Appropriate Use Policy
By accessing and/or using University information systems, and/or by "clicking through" a usage agreement during sign-on to any University system, registration onto ResNet or any other equipment registration procedure, users assent to the Terms and Conditions of the Appropriate Use Policy.

Part 2

Access To and Use of Systems/Normal Duration of Service
Access to and use of Northeastern information systems are privileges granted by the University to faculty, staff, students and authorized third parties. Additional electronic experiences as may be offered to parents and extended populations are included under the provisions of this paragraph. Access for up to one (1) academic year for others including "sponsored" individuals whose relationship with Northeastern is a result of a University-recognized affiliation or relationship must be approved by the authorizing unit. The University retains sole discretion over the extent to which access privileges are granted, extended and/or revoked.

Part 3

Use of Computer Accounts and Facilities
Members of the Northeastern community may use only the computer accounts and facilities authorized by the University for their use. Use of another person's account,

identity, security devices/tokens, or presentment of false or misleading information or credentials, or unauthorized use of information systems/services is prohibited.

Part 4

Users Responsible for Actions Conducted Under their User ID(s)

Users are responsible for all use of information systems conducted under their user ID(s), and are expected to take all precautions including password security and file protection measures to prevent use of their accounts and files by unauthorized persons/entities. Sharing of passwords or other access tokens with others is prohibited. Users who disclose their passwords to third parties are solely responsible for all consequences arising from such disclosure.

Part 5

Duties When Speaking in Electronic Communications

Speakers are expected to make clear when they are not representing the University in their electronic communications.

Part 6

Posting of Personal Information/Web Pages/Other Electronic Writings

Users are responsible for the timeliness, accuracy and content/consequences of their personal information, web pages and other electronic writings. Personal information of members of the Northeastern community, including but not limited to students, faculty and staff, may not be posted or maintained on public networks or sites, unless the user fully complies with applicable laws and regulations governing handling of personal information.

Part 7

Use of University-Recognized Messaging Systems

Electronic messages pertaining to the official business of the University, including all academic and administrative matters shall be sent from University-owned or University-recognized messaging systems. For example, inquiries about students must be sent from an account associated with a University-recognized e-mail system. Replies from faculty or staff must be sent using the same University-recognized accounts. In cases where unrecognized third-party messaging systems are used to originate a message, and/or where a party chooses to forward messages

from a University-owned or University-recognized system to a third-party unrecognized system, individuals using these systems shall be solely responsible for all consequences arising from such use.

Part 8

Use of University Systems to Host Non-University Activities
Use of University information systems for hosting non-University activities must have the explicit written authorization of the Office of the Provost or its designee.

Part 9

Commercial Use
University information systems may not be used for commercial purposes except only as permitted with the explicit prior written approval of the Offices of the Provost and General Counsel.

Part 10

Offering, Providing, Lending or Renting Access to University Systems
Users may not offer, provide, lend, rent or sell access to University information systems or networks. Users may not provide access to individuals outside the University community. Expansion or redistribution of Northeastern's cable television services is not permitted. Expansion of centrally-managed administrative network segments and connection of personal, private or departmental switches, routers, wireless access points or DHCP-serving devices is prohibited, except only as may be agreed to in writing between the device owner and Information Technology Services.

Connection of personal or privately-owned routers and/or wireless access points to the ResNet wired networks is prohibited.

Northeastern reserves the right to reconfigure or disable the network port(s) of any user whose activity interferes with NUNet, ResNet, NUwave or any other University-provided system or service, for example, to address a misconfigured device or a computer infected with virus/malware.

In order to receive ITS support to resolve a problem reported by a student using a privately-owned router and/or wireless access point, such problem must be recreated while connected to the ResNet port in question, with privately-owned device(s) out of the connection path.

For security reasons, dial-up modems shall not be used on computers while they are connected to the University network. The VPN (Virtual Private Network) shall instead be used.

Part 11

Compliance with Internet Service Provider Terms of Use

Internet use must comply with the Terms of Service stipulated by our Internet service provider(s). In addition, the Acceptable Use, Terms of Service and/or other policies of systems and/or electronic resources accessed through University Internet connection(s) also bind users of University Internet connections. Failure of users to comply with these Terms of Service may result in sanctions, up to and including separation from the University.

Links to the terms of service for the University's Internet service providers are found in Appendix A.

Part 12

Use of Remote Resources

Users may not connect to remote resources such as printer, file systems, or any other remote resource, regardless of location on or off the Northeastern network, unless the administrator of the remote resource has first granted permission to do so.

All access to University electronic resources shall occur through reasonable and customary means. For example, all electronic resources offered through a web-based experience shall be accessed using a web browser only.

Electronic resources are available to faculty and staff only when using "remote access", also known the Virtual Private Network (VPN). The University reserves and intends to exercise its right to determine:

- *who may use the VPN,*
- *from what locations the VPN may be accessed,*
- *what services and experiences are offered through the VPN,*
- *the extent of individual access rights when using the VPN,*

- *to limit or block connections not originating from the VPN, and*

- *to assess and approve other secure connection methods.*

Exclusions to this policy provision may be made to vendors and affiliates who maintain private connections to the University network.

All users establishing a connection to the University network through the VPN or by any other means are responsible to ensure antivirus software is present on their computer, and that its protection signatures are up to date. For more information on use of the VPN or antivirus software, please refer to the Information Services website.

Part 13
Irresponsible/Wasteful Use
Users may not use information systems irresponsibly, wastefully, or in a manner that adversely affects the work or equipment of others at Northeastern or on the Internet.

Part 14

Specific Prohibitions on Use of Information Systems

In addition to all of the requirements of this Policy, it is specifically prohibited to use Northeastern University information systems to:

- *Harass, threaten, defame, slander or intimidate any individual or group;*

- *Generate and/or spread intolerant or hateful material, which in the sole judgment of the University is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, marital status, sexual orientation, veteran status, genetic makeup, or disability;*

- *Transmit or make accessible material, which in the sole judgment of the University is offensive, violent, pornographic, annoying or harassing, including use of Northeastern information systems to access and/or distribute obscene or sexually explicit material unrelated to University sanctioned work or bona fide scholarship;*

- *Generate unsolicited electronic mail such as chain messages, unsolicited job applications or commercial announcements;*

• *Generate falsely -identified messages or content, including use of forged content of any description;*

• *Transmit or make accessible password information;*

• *Attempt to access and/or access information systems and/or resources for which authority has not been explicitly granted by the system owner(s);*

• *Capture, decipher or record user IDs, passwords, or keystrokes;*

• *Manipulate or tamper with uniform resource locators (URLs);*

• *Intercept electronic communications of any kind;*

• *Probe by any means the security mechanisms of any resource on the Northeastern network, or on any other network through a connection to the Northeastern network;*

• *Disclose or publish by any means the means to defeat or disable the security mechanisms of any component of a Northeastern University Information System or network;*

• *Alter, degrade, damage or destroy data;*

• *Transmit computer viruses or malicious/destructive code of any description;*

• *Conduct illegal, deceptive or fraudulent activity;*

• *Obtain, use or retransmit copyrighted information without permission of the copyright holder;*

• *Place bets, wagers or operate games of chance; or*

• *Tax, overload, impede, interfere with, damage or degrade the normal functionality, performance or integrity of any device, service or function of Northeastern information systems, content, components, or the resources of any other electronic system, network, service or property of another party, corporation, institution or organization.*

The above enumeration is not all-inclusive. If there is a question as to whether a specific use is appropriate or acceptable under this policy, the University's sole determination shall prevail.

UNIVERSITY RIGHTS AND RESPONSIBILITIES SECTIONS

Part 15

General Rights of the University

To protect Northeastern information systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the University reserves the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The University may also monitor, record, inspect, copy, remove or otherwise alter any data, file, or system resources in its sole discretion. The University further reserves the right to periodically inspect systems and take any other actions necessary to protect its information systems. The University also retains access rights to all files and electronic mail on its information systems. Anyone using these systems expressly consents to such monitoring.

Part 16

Right to Seize/Inspect University-Owned Computing Devices

The University reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other University-owned computing device, to seize such device and/or copy or have copied, any and all information from the data storage mechanisms of such device as may be required in the sole discretion of the University in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the University network are also subject to inspection by authorized University personnel.

Part 17

Right to Block Content

The University reserves the right to reject from the network or block electronic communications and content deemed not to be in compliance with policies governing use of University information systems.

Part 18

Right to Disclosure Information

The University may disclose information, including pursuant to an internal or external investigation of alleged misconduct or wrongdoing, and may provide information to third parties, including law enforcement. By accessing Northeastern

information systems, users give Northeastern permission to conduct each of the operations described above.

Part 19

Detection of Plagiarism/Academic Dishonesty

The University reserves the right to use, and intends to use manual and/or automated means to assess materials submitted as academic work submitted electronically for indications of plagiarism or other form(s) of academic dishonesty.

Part 20

Actions to be Taken When a Policy Violation is Identified

When a potential violation is identified, the appropriate system manager or unit head, the Information Security Office, and any other University employees or agents as are deemed appropriate, are authorized to investigate and initiate action in accordance with University policy. Repeated violations may result in suspension or termination of service(s). In addition, the University may require restitution for any use of information systems that violates this policy. The University may also provide evidence of possible illegal or criminal activity to law enforcement authorities.

Part 21

Consequences of Policy Violation

Any unauthorized, inappropriate, illegal or illegitimate use of the University's information systems, or failure to comply with this policy shall constitute a violation of University policy and will subject the violator to disciplinary action by the University up to and including separation of employment or relationship, and may result in legal action.

Part 22

Termination of Access to University Systems and Services

Notwithstanding any other provision of this policy, authorization to access the information systems and resources of Northeastern University ends at the termination of employment, end of a recognized role or relationship, or loss of sponsorship.

Students may continue to use their Northeastern electronic mail account for up to one (1) year after completion of requirements.

CONFIDENTIALITY / PRIVACY SECTIONS

Part 23

Electronic Content Property of the University

Right of University to Monitor Content

University information systems and the messages, e-mail, files, attachments, graphics and Internet traffic generated through or within these systems are the property of the University. They are not the private property of any University employee, faculty, staff, contractor, student or any other person. No user of University systems should have an expectation of privacy in their electronic communications. All electronic communications, files and content presented to and/or passed on the Northeastern network, including those to, from or through Internet connection(s), may be monitored, examined, saved, read, transcribed, stored or re-transmitted by an authorized employee or agent of the University, in its sole discretion, with or without prior notice to the user. The University reserves and intends to exercise the right to do so. Electronic communications and content may also be examined by automated means.

Part 24

Confidentiality of Content

The confidentiality of any content shall not be assumed. Even when a message or material is deleted, it may still be possible to retrieve and read the message or material. Further, use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Aside from the right of the University to retrieve and read any electronic communications or content, such messages or materials must be treated as confidential by other students or employees and accessed only by the intended recipient. Without prior authorization, no person is permitted to retrieve or read electronic mail messages not sent to them.

Part 25

Responsibility to Maintain Confidentiality

Notwithstanding the University's right to audit or monitor its information systems, all users are required to observe the confidentiality and privacy of others'

information accessed through Northeastern information systems and records of every description, including information pertaining to University programs, students, faculty, staff and affiliates. Without proper authorization, users are not permitted to retrieve or read content not intentionally addressed to them. With proper authorization, the contents of electronic mail or Internet messages or materials may be accessed, monitored, read or disclosed to others within the University or otherwise.

Part 26

Electronic Privacy Rights

The electronic privacy rights of others shall be respected at all times. Use of audio, video, cell phone, "web cam" or related technologies, for the purpose of capturing images and/or recording speech in locations or circumstances where a reasonable expectation of privacy exists is prohibited without the consent of the subject(s) depicted and/or recorded. This provision shall not apply to lawful surveillance conducted by law enforcement agencies. The University reserves the right to impose additional restrictions on use of electronic recording devices, in its sole discretion. Questions about the applicability of this provision to a particular situation shall be referred to the Office of General Counsel or the Director of Information Security.

Part 27
Handling of Sensitive Information
Disposal of Equipment and Storage Media

Printed materials, computer equipment and storage media containing sensitive and/or protected information shall be handled in accordance with Information Disposal Requirements, Asset Disposition procedures, and hazardous materials regulations. Additional information on these topics is available from the Information Services website (northeastern.neu.edu/secureNU, and ehs.neu.edu).

Part 28
No Guarantee of Protection Against Unauthorized Access
Prohibition on Accessing/Moving Data Belonging to Another Accountholder

While the University attempts to protect electronic communication and files from unauthorized access, this cannot be guaranteed. Users may not access, copy or move files including, but not limited to programs, data and electronic mail belonging to another account, without prior authorization from the accountholder. Files may not

be moved to other computer sites without permission from the accountholder whose account under which the files reside.

COMPLIANCE WITH LAWS SECTIONS

Part 29
Requirement to Comply with Applicable Local, State and Federal Laws Concerning Use, Dissemination and Disclosures of Information

The University strives to maintain the security and privacy of electronic communications. Use of Northeastern University information systems or resources, dissemination, and disclosures of information, must comply with the provisions of applicable local, state and federal laws, regulation and University policy. Applicable laws and policies may be found in Appendix B. That list is not exhaustive.

Part 30
Lawful Use

Northeastern information systems may be used for lawful purposes only. It is prohibited to use Northeastern information systems for unlawful purposes, including, but not limited to the installation of fraudulently or illegally obtained software, harmful software, illegal dissemination of licensed software, sharing of content where the disseminator does not hold lawful intellectual property rights, propagating chain messages, pyramid, ponzi, other unlawful or deceptive schemes, or for any purpose contrary to local, state, federal law or University policy.

Part 31
Compliance with Copyright Law

Use of University information systems must comply with provisions of copyright law and fair use. Copyright law limits the rights of a user to decrypt, copy, edit, transmit or retransmit another's intellectual property, including written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is in compliance with Fair Use or TEACH Act provisions.

Part 32
Compliance with Export Control Regulations

Exports of computing equipment and information technologies from the University must be in compliance with US Export Control Regulations.

Part 33

NOTICE OF RIGHT TO CHANGE APPROPRIATE USE POLICY

The University reserves the right to change this policy or any portion of the policy, at any time, with or without prior notice. Changes to this policy are effective upon posting at http://www.northeastern.edu/policies/, where the most current version resides. The AUP was last revised on May 2, 2016.

Appendix A

Handling of this type of information	Must be in compliance with this law, regulation or policy…	Which can be reviewed at this location…
Student information	Family Educational Rights and Privacy Act (FERPA) of 1974	http://www.northeastern.edu/registrar/ferpa.html
Protected Health Information (PHI)	Health Insurance Portability and Accountability Act (HIPAA) of 1996	http://www.northeastern.edu/drc/pdf/HIPAA%20privacy%20practice.pdf
Social Security Number (SSN) and Personal Information	NU Policy on Collection, Handling and Use of the Social Security Number and Personal Information	http://www.northeastern.edu/policies/pdfs/Policy_on_Confidentiality_of_University_Records_and_Information.pdf
Personal Identifying Information (Pii)	Massachusetts Data Protection Laws (MA201 CMR 17.00)	http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Note: *If clicking on the links above fails to render a readable page, it is suggested to paste the link into a web browser URL bar.*

APPENDIX B

Mass. 201 CMR 17.00, which are the Massachusetts regulations for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts.

Massachusetts General Laws Chapter 266, Sections 33(a) and 120(f), which impose sanctions for, among other acts, destroying electronically processed and stored data or gaining unauthorized access to a database or computer system.

Massachusetts General Laws Chapter 272, Section 99, which regulates and prohibits recording of communications without permission of participants, including but not limited to telephone conversations. The law also includes prohibitions on possession, editing, and disclosure of recordings.

United States Code, Title 18, Section 1030 et seq., ***Computer Fraud and Abuse Act*****,** which imposes sanctions for, among other acts, knowingly accessing a computer without authorization or in excess of authorized access, knowingly causing damage to protected computers, or trafficking in password information.

United States Code, Title 18, Section 2510 et seq., ***Electronic Communications Privacy Act***, which imposes sanctions for, among other acts, interception of wire, oral or electronic communications.

United States Code, Title 18, Sections 2701 et seq., ***Stored Wire and Electronic Communications and Transactional Records Act***, which imposes sanctions for, among other acts, intentionally accessing without authorization, a facility through which electronic communication service is provided, or intentionally exceeding authorization to access a facility, thereby obtaining, and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage.

United States Code, Title 47, Section 223 (H)(1) et seq., Communications Act of 1934 (as amended), which imposes sanctions for, among other acts, use of any device or software that can be used to originate telecommunications or other types of communications that are transmitted in whole or in part by the internet, without disclosing the sender's identity, and with intent to annoy, abuse, threaten, or harass any person who receives the communications.