Sanctions: Hearing Officers and the Student Conduct Board have discretion to impose sanctions for a Responsible finding of an Academic Integrity violation that range in severity from a written warning to expulsion, and include an action taken by the student to help rebuild trust within the community.

Hearing officers will take the following into consideration when determining appropriate sanctions for violations of the Academic Integrity policy:

1. Nature of the violation(s)

2. Severity of the damage, injury, or harm resulting therefrom

3. Student's past disciplinary record

4. Mitigating circumstances

5. Aggravating circumstances

Appeals: Students may appeal the disciplinary actions of an Academic Integrity violation on the three grounds identified in the Code of Student Conduct.

The Appeals Process outlined in the Code of Student Conduct will be used for such appeals. Please refer to the Code of Student Conduct for a complete description and explanation of the Appeals Process.

Grading Authority: OSCCR does not have authority over assignment or course grades. Therefore, a student who violates Northeastern University's Academic Integrity Policy may also be subject to academic penalties at the discretion of the instructor in the course. This can result in, but is not restricted to, the student failing the course. A student with questions about the Academic Appeals process should contact the academic advisor to review that process.

Appropriate Use of Computer and Network Resources Policies

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 Communicating Electronically

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.