Dear Members of the Northeastern Community,

This is the next in a series of periodic reminders about individual and institutional responsibilities around protecting sensitive information, and the requirement to read and comply with relevant university policies on use of information and information systems.

Spring 2014 Information Security Tips:

Spring Forward
It might not seem like it with the cold, but remember that Daylight Savings Time begins at 2 a.m. on Sunday, March 9, 2014. Set your clocks forward one hour as we start observing Daylight Savings Time. While most computer and electronic systems will automatically make the change, it is always a good idea to verify that it has occurred correctly to ensure proper functionality.

Appropriate Use
All users of Northeastern University computer resources are required to read and abide by the Appropriate Use Policy. This year’s policy has been updated and streamlined to highlight responsibilities. Look for the new format in upcoming publications of the Student Handbook as well as on the Information Technology Services website.

REMEMBER: Northeastern University WILL NEVER ASK FOR YOUR PASSWORD. Any email you receive claiming to need your login and password is spurious and should be deleted without replying. If you have given a password to another person, change that password immediately. Each of us is held responsible for all activity conducted under our user ID and password.

Something in the Air
While wireless connections make all our lives more simple and convenient, open and free access points are inherently insecure. Northeastern University provides two different wireless networks for our community: NUwave and NUwave-guest.

NUwave is the secured wireless network on campus and offers exclusive wireless access to internal systems for faculty, staff and sponsored accounts. NUwave can be accessed by using your myNEU username and password. Always connect to the authenticated wireless when you are on campus. NUwave-guest provides individuals without a myNEU login limited Internet access to most browser-based applications, email and VPN access. NUwave-guest is an open access (not secured) wireless network on campus, similar to a free wireless connection in a coffee shop or airport. You should never conduct any transactions on a guest or free wireless access system.

Playing on Heartstrings
As the 2014 Boston Marathon approaches and we recall the memories of last year’s tragic events, it is difficult for those of us in the City of Boston to not have a visceral reaction. Unfortunately, it is possible that unscrupulous individuals may take advantage of those emotions in the form of phishing emails. We advise everyone to have a heightened sensitivity to emails addressing the Boston Marathon bombings. There may be requests to click on links or donate funds and we strongly encourage you to verify the legitimacy of these messages.
Protection of Sensitive Information / Regulatory Compliance:

Social Security Numbers, dates of birth, grades, non-public personal financial information, protected health information, and other similar types of sensitive information are to be protected at all times from unauthorized disclosure and/or use, consistent with applicable University policies and/or applicable Federal laws, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Financial Services Modernization Act (also known as Gramm-Leach-Bliley), the CAN-SPAM Act of 2003, and Massachusetts Data Security Regulation MA201 CMR17.00. 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.

Compliance with Copyright Law and Software Licensing Agreements:

All members of the community are required to comply with copyright law and software licensing agreements. In addition, all software installed on university-owned devices shall be the product of legal copies, and shall be properly licensed at all times. University resources shall not be used to offer, exchange or store copyrighted materials nor the indexes pointing to such materials, unless the use is in compliance with copyright law or other applicable regulation. All use of file-sharing technologies shall be in strict compliance with university policy and copyright law.

Responsibilities under Regulation:

Our responsibilities under regulation includes, among other reasonable steps, that we refrain from displaying or listing sensitive information in public venues such as hallway bulletin boards, office doors, globally shared computer files, and publicly-accessible web sites, that we observe privacy practices, and that we use appropriate safeguards to protect sensitive information and information-bearing devices from unauthorized access, alteration, theft or loss. These responsibilities include taking appropriate steps to ensure confidential/sensitive paperwork is properly discarded, that mobile devices are appropriately protected from loss or theft, and that computer disk drives and information storage devices are properly processed to remove sensitive information prior to reallocation or disposal.

Consequences Arising from Unauthorized Disclosure or Loss of Sensitive Information:

The potential consequences of unauthorized disclosure or loss of sensitive information may include for the individual, loss of privacy, identity theft, financial loss, erosion of customer confidence, and for the University, damage to reputation, civil penalties, and regulatory sanction. By recognizing the value in protecting sensitive information, the university is better positioned to avoid these consequences, maintain customer trust, and enjoy a reputation more demonstrative of the university commitment to excellence and distinction, and other goals to which it aspires.

Requirement to Read and Comply with the Appropriate Use Policy (AUP):

The Appropriate Use Policy describes policies for use of all computers, networks and telecommunications facilities at the university. All members of the university community are required to read and comply with the AUP, which can be read at northeastern.edu/aup. Use of university computer/telecommunication networks and/or computers, implies agreement with the terms of the Appropriate Use Policy.

Shared Responsibility

Security is a shared responsibility. Do your part to help promote a safer and more secure computing environment by observing and supporting secure practices in your academic or business unit. If assistance is required, please contact itsecurity@neu.edu

Thank you for your time and attention.

Warmly,

Mark T. Nardone, MIS, CISSP, CIPM
Director of Information Security