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 2011 Information Security Tips:**

**Springing Forward**
Remember that at 2am on Sunday March 13th 2011, US Daylight savings time begins and we move forward one hour from standard time. It is always good practice to check computers, smartphones and timekeeping devices of all descriptions to ensure they display the correct time. Why is time so important? Certain web-based experiences and software applications will not operate if the time on your computer is incorrect.

**Complicated is Better**
This upcoming year will see new standards of password complexity for Northeastern University systems. Protect your myNEU account by creating not only a hard to guess password, but also a hard to guess password reset challenge answer. Use a combination of letters and numbers, as well as a length of 8 or more characters. An easily guessed or weak password and reset challenge answer exposes your myNEU account to “guessers” who can send email in your name, make transactions in your name, and steal your personal information and/or identity. Change your myNEU password and password reset challenge answer today, and on a regular basis going forward.

**Paging Mr Smith**
One of the great features of Microsoft Exchange is the Outlook Directory which will quickly search for the email address of a recipient as you type their name. However you should ensure that the name that is selected is the correct person you are looking for, as often when there are users with similar or identical names they can easily be confused. This is especially important when you are sending email of a sensitive or private nature. Always take a moment to verify your email is addressed properly; if you hover the mouse cursor on an addressee’s name, Outlook will give you a pop-up box where you can see the user’s job title and department.

**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 comment to excellence and distinction, and other goals to which the University 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 [www.infoservices.neu.edu](http://www.infoservices.neu.edu). 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](mailto:itsecurity@neu.edu)

Thank you for your time and attention.

Warmly,

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