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.

**Fall 2012 Information Security Tips:**

**Falling Back**
Remember that Daylight Savings Time ends this weekend at 2am November 4th. Remember to set your clocks back 1 hour as we return to Standard 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.

**Don’t Take the Bait**
Once again a major source of problems are what are termed as “Phishing” emails. These usually take the guise of an ‘official looking’ communication requesting your account name and password to avoid the cancellation of your neu.edu account. These social engineering methods play on your trust and attempt to circumvent your judgment by using familiar information and subtle threats. Many victims relate a “feeling that something wasn’t right”, but respond despite their better judgment. If you receive any such email it is often best to delete it immediately, or contact the NU helpdesk at x4357 or help@neu.edu if you have any doubts.

**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 the relevant password immediately. Each of us is held responsible for all activity conducted under our user ID and password.

**Mailing John Smith**
The University Community is growing and as often happens with large populations you may find there is more than one person with the same or similar names. Take extra care when you are sending emails of a sensitive nature or that contain protected FERPA information. Microsoft Outlook will auto-fill a recipient’s name as you type it into the address bar, but you need to make sure that it is the correct person. If Outlook does not auto-fill, use the Check Names button for possible matches, and then simply hover your cursor over the person’s name to see their job title and department. It is your obligation to ensure that emails are properly addressed; failure to do so can lead to potential wrongful disclosures of information and be harmful to the University’s reputation.

**Helping You SecureNU**
Information Security launched its web resource [www.northeastern.edu/securenu](http://www.northeastern.edu/securenu) earlier this year. We also keep the Northeastern Community updated on events and information through Twitter @SecureNU. Visit the webpage or follow our Twitter-feed for breaking news and tips on keep you and the University secure.

**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

Thank you for your time and attention.

Warmly,

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