Dear Members of the Northeastern Community,

This is the next in our 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 2015 Information Security Tips:**

**Cyber Security Awareness Month**
The month of October has been deemed National Cyber Security Awareness Month and Northeastern is taking the opportunity to help our community become aware. It is the perfect time to educate yourself about the everyday issues of information and cyber security, which can affect you in your work and daily life. Watch for posts and tweets from the SecureNU website and the Information Security team about topics of interest. Also look for on campus events and remember that information security begins with you!

**Falling Back**
Daylight Savings Time ends at 2 a.m. on November 1, 2015. Remember to set your clocks back one 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.

**Say Hello to the Policy Oversight Committee**
*Are you wondering how the new Massachusetts sick leave law has affected University policy? Have you heard there is a new mobile device policy, but haven’t read it? Have you long thought the University should have a policy on something that you don’t think exists already, but don’t know whom to suggest this to?*

Turn to the [university policy website](#) as the exclusive authoritative source for university policies where you can find answers to questions like the ones above and many more. Following the successful conclusion of the Operations Council’s policy project to review, revise and standardize all University policies, oversight of the policy development process is now handled by the Policy Oversight Committee (POC), comprised of representatives from across campus. The POC members bring the views of their respective areas to bear in discussions of policy needs for the University.

**If it Smells Phishy, it Probably is!**
It may seem like the oldest scam in the book, but phishing is still the number one way accounts and systems get compromised. This year we have seen a large increase in the number and sophistication of phishing attempts directed specifically at Northeastern. Always listen to your inner voice of doubt when confronted with emails that attempt to alarm or elicit responses through emotion. If you receive any such email, it is often best to delete it immediately. If you are unsure whether an email is safe, or not, please contact the ITS Service Desk at 617.373.4357 (xHELP) or help@neu.edu for assistance. Also look for our Twitter thread #NEUPhishCatcher to see what our students are submitting for our Phishing Contest, and check [here](#) to see how to become a skilled PhishCatcher.

**REMEMBER: Northeastern University WILL NEVER ASK FOR YOUR PASSWORD.** Any email you receive claiming to need your login and password is fake 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.
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 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 northeastern.edu/policies. 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 OIS@neu.edu

Thank you for your time and attention.

Warmly,

Mark T. Nardone,
Chief Information Security Officer