ANNUAL POLICY NOTIFICATION MEMORANDUM

TO: All University of New Mexico Faculty, Staff and Students
FROM: UNM IT, UNM Main Campus Compliance Office and HSC Institutional Compliance Office
SUBJECT: Protecting Yourself from Phishing and Determining Acceptable Computer Use

DATE: May 20, 2020

The University of New Mexico (UNM) email system receives millions of messages each day, but many never reach inboxes. Information Security screening systems flag them as “spam or scams” and the messages are discarded prior to negatively affecting our email messaging systems. However, on occasion some deceptive and dangerous emails slip through. That's why it is essential for all staff to recognize email phishing scams and take proactive steps to protect yourself and UNM.

- Delete requests for sensitive information.
- Never click on suspicious links. Hover over links to where the addresses is linked to.
- Check to see if suspicious messages have been reported at phishbowl.unm.edu
- Report suspicious emails and websites to security@unm.edu
- Enable Two-Step Login when possible
- Know the signs of phishing. If an email seems like phishing, it probably is. Trust your instincts!

For 2020, UNM is adding mandatory information security and data privacy training for all employee learning plans. This training will demonstrate safe data practices and will also assist employees in better identifying phishing and other attacks that can lead to **potential** information security incidents and data breaches.
This memorandum serves the purpose of reminding everyone about UNM policies regarding acceptable computer use.

UNM Policies and Tools Related to Acceptable Computer Use:

UAP 2500 – Acceptable Computer Use https://policy.unm.edu/university-policies/2000/2500.html

UAP 2520 – Computer Security Controls and Access to Sensitive and Protected Information https://policy.unm.edu/university-policies/2000/2520.html

UAP 2550 –Information Security - https://policy.unm.edu/university-policies/2000/2550.html

UNM Health Sciences Center and Health System IT Policies and Standards - https://hsc.unm.edu/about/cio/user-support/it-policies-and-standards.html

Administrative Policies and Procedures Manual - Policy 2500: Acceptable Computer Use

UNM encourages, supports, and protects freedom of expression as well as an open environment to pursue scholarly inquiry and to share information. Access to information technology (IT), in general, and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. The computing and network resources, services, and facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, there is a possibility of misuse. In an attempt to prevent or mitigate such misuse, UAP 2500 outlines proper and improper behaviors, defines misuse and incidental use, explains rights and responsibilities, and briefly reviews the repercussions of violating these codes of conduct.

UNM provides computing services to University faculty, staff, students, retirees, and specified outside clients of the University and periodically to visitors and guests. These services are intended primarily for furthering the education, research, and public service mission of the University and may not be used for commercial purposes or profit-making. This policy is applicable to all individuals using University-owned or -controlled computer equipment, communications equipment, data network (wired and wireless), storage devices, and computer-related facilities, whether such persons are students, staff, faculty, or third-party users of University computing resources and services. All University policies including, but not limited to, intellectual property protection, privacy, misuse of University equipment, sexual harassment, hostile work environment, data security, and confidentiality shall apply to the use of computing services.

Individual departments within the University may define “conditions of use” for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions.

To review the complete policy, please see: https://policy.unm.edu/university-policies/2000/2500.html

Administrative Policies and Procedures Manual - Policy 2520: Computer Security Controls and Access to Sensitive and Protected Information

UNM provides computing services to the University community in accordance with UAP 2500, which applies to all users of University computing systems. This policy describes additional requirements and responsibilities applicable to faculty, staff, students, vendors and volunteers who are in IT-related positions or are in positions that have access to sensitive and protected information.

Due to the differing regulatory constraints imposed upon the UNM Health Sciences Center (HSC) and UNM Health System relative to privacy and security of health information both in the clinical and research areas, the UNM HSC and UNM Health System are excluded from application of this Policy and shall be covered by as restrictive or more restrictive IT: Administrative Policies adopted by the UNM HSC and UNM Health System; provided that the provisions of Section 4. herein relating to remote access to the Enterprise Resource Planning (ERP) suite of tools shall apply to the UNM

HSC and UNM Health System and HSC IT will promptly report any security violations to the University IT Security Office at security@unm.edu.
To review the complete policy, please see: https://policy.unm.edu/university-policies/2000/2520.html

Administrative Policies and Procedures Manual - Policy 2550: Information Security
UNM is committed to protecting and safeguarding all data and information that it creates, collects, generates, stores, and/or shares during the generation and transmission of knowledge as well as during the general operation and administration of the University. The University is also committed to complying with all federal and state laws pertaining to securing this data and information and preventing its disclosure to unauthorized individuals. These laws include, but are not limited to, 32 CFR Part 2002, also known as the Controlled Unclassified Information (CUI) implementing directive, and the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA). In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law and promulgated the GLBA Safeguards Rule, 16 CFR Part 314, which requires higher education institutions to have an information security program to protect the confidentiality and integrity of personal information. This policy describes the basic components of the UNM Information Security Program which applies to employees (student, staff, and faculty), contractors, vendors, volunteers, and all other individuals who work with UNM data and information. In accordance with New Mexico law, some employee information is considered public information; however, such information must still be protected from inadvertent destruction or unauthorized changes. Refer to UAP 3710 ("Personal Information Disclosure Policy") for additional information.
To review the complete policy, please see: https://policy.unm.edu/university-policies/2000/2550.html

UNM Health Sciences Center and Health System IT Policies and Standards
The different HSC and Health System IT Policies and Standards can be found at: https://hsc.unm.edu/about/cio/user-support/it-policies-and-standards.html