Workstation and Network Appropriate Use Policy
July 19, 2016

SCOPE

This policy applies to Florida Atlantic University's Covered Components and those working on behalf of the Covered Components (collectively "FAU") for purposes of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

POLICY

FAU shall have a policy governing the appropriate use of workstations and FAU networks.

REASON FOR POLICY

To establish information technology safeguards that will protect FAU's network, hardware, software and data which are issued and/or managed by the University. These safeguards are intended to reduce the risk of threats to FAU information technology resources, protect confidential and otherwise sensitive information, and augment the Acceptable Use of Technology Resources policy.

DEFINITIONS

Refer to Glossary and Terms.

PROCEDURE

1. **Internet and E-mail Use:** Access to the Internet and an FAU email account is provided to workforce members to perform their job duties. Internet and e-mails are to be used for business purposes with incidental personal use.

2. **Passwords:** Each user of FAU's network is assigned a unique, personal access account and identification number to access the network. Users will also be assigned an initial password to access the network. Users must change the initial passwords provided to them if they were automatically generated. Users must enroll in the University's two-factor authentication program.

   To ensure compliance with this provision, the Office of Information Technology ("OIT") will establish reminders and automatic password expiration if passwords are not regularly changed. Users are responsible for all activity occurring under their user identification. As such, users should not share, and are prohibited from sharing, their login ids or passwords with any third party.

To ensure the security of passwords, OIT will set password parameters that require passwords to be a combination of letters, numbers and special characters. Users should not write down passwords or store them in their offices. Local password managers may be used if the particular product is approved by the University Information Security Officer.

3. Workstation Protection

- Desktop Lockout

    - Users should ensure that all devices used to access FAU systems have a feature that is enabled at all times to ensure an automatic lockout and timeout after no greater than 10 minutes of inactivity for devices not generally accessible to the public and 5 minutes for devices that are generally accessible or viewable by the public.

    - Users must lock their computers during temporary absences.

    - At the end of each workday or for long periods of absence, users should log off of their computers.

- Users are not permitted to download or install software on their computers without approval and assistance from OIT or the responsible IT group which also ensures that FAU has the appropriate licenses to install or use such software. Users should only request to download or install software necessary for their job functions.

4. Asset Management

- All databases, spreadsheets, documents, information, and images created, stored, transmitted, or maintained on FAU servers, in workstation applications or stored on FAU servers, local hard disks, or equipment ("Institutional Data") are the exclusive property of FAU.

- All computer equipment issued or used by the Covered Components constitute FAU property regardless of funding source. Users are required to contact OIT or responsible IT group before relocating any equipment.

5. Network Management, Files, and Data

- FAU uses system administrators to administer its networks. System administrators have the same responsibilities as other system users to maintain the integrity of FAU's confidential information and network systems. All files accessed, viewed, transmitted, maintained, or stored by systems administrators are private and should at all times be treated as such. System administrators and all users should access no more data than necessary to complete their job functions.

- Each workforce member must recognize the importance of Institutional Data and take any and all actions necessary to maintain the confidential status of such Institutional Data. If a workforce member becomes aware of any instance in which Institutional Data is at risk of unauthorized disclosure, dissemination, destruction, or other unauthorized use, he or she should immediately report such instance to the Chief Information Officer.

- Any unauthorized personal wireless access points, Wi-Fi enabled hotspots, and wireless printers in buildings with FAU provided wireless networking will be disabled and the owner of the device or hotspot will be required to conform to University policy. Any use of such device or hotspot to circumvent or threaten the integrity of the University Wi-Fi or the University network will not be permitted.

  Such devices cause radio frequency interference with the university wireless network. This interference degrades the effectiveness of the FAU Wi-Fi, which in turn has a negative impact on Wi-Fi service in the surrounding areas. In order to maintain the highest level of wireless service, particularly in academic buildings where class delivery depends on the optimal operation of the FAU wireless network, all rogue wireless devices shall be disabled.

6. Hardware and Software

- **Software:** Computer software is protected by copyright and is not to be copied or replicated without permission of OIT or the responsible IT group. Workforce members and OIT or the responsible IT group are responsible for ensuring that FAU has obtained any necessary software licenses. Users may only use software in accordance with the terms of the applicable software license.

- **Software Catalogue:** OIT maintains a comprehensive software and licensing catalogue of OIT-approved applications for all FAU system users. FAU has agreements with various vendors to provide discounted licenses for FAU-owned computers. OIT or the responsible IT group will manage the distribution, installation, and implementation of software products across all FAU computing resources.

- All requests for currently unapproved software must be submitted to OIT or the responsible IT group for approval. In general, shareware and demo software are not to be utilized on systems housing PHI unless as part of an approved software evaluation process. Personally owned devices or personally-maintained software may not be used to access PHI without the written approval of the University Information Security Officer.

- **Hardware Configuration:** FAU does not permit workforce members and other users to modify their FAU workstations or the software installed on them, except as provided below. Workstations may only be used for the purpose of performing work duties and incidental personal use which does not require installation of new software or modification of the system. If your position requires special configurations or special software, contact OIT or the responsible IT group to coordinate such installation or configuration of the items you need to perform your job duties. Despite the foregoing, workforce members/users may

change their desktop background screen and personal desktop and application settings that do not interfere with the shared operation in the network environment.

7. Personal Use

- FAU equipment and resources may only be used for FAU-related business purposes and incidental personal use which does not require installation of new software or modification of the system.

- The use of instant messaging services presents a security risk to FAU's systems. Users may not access or use instant messaging services on FAU issued equipment, or personal equipment used to create, store, maintain, or transmit FAU Institutional Data, unless the messenger system has been approved by the workforce member's supervisor and approved and installed by OIT or the responsible IT group.

- Internet browsing should be limited to FAU-related business purposes. FAU has the right to monitor the use of its networks and systems, including, without limitation, the information contained on FAU-issued equipment and personal equipment that may be used to maintain, transmit, store, or create Institutional Data, or web browsing histories and information. **Workforce members and other FAU network and systems users do not have a right or expectation of privacy when using any FAU issued equipment or system, or personal equipment that contains Institutional Data.** FAU routinely monitors the use of its systems and has the right to restrict use, block inappropriate websites, and take any other action necessary to protect the integrity of its Institutional Data and systems.

8. Security

- **Standard Anti-Virus/Malware Software:** All FAU computing resources are required to use the anti-virus and anti-malware solutions implemented by OIT or the responsible IT group.

- **Hacking and Viruses:** Users should immediately notify OIT and the responsible IT group if applicable as soon as he or she becomes aware of an event that the workforce member knows or suspects has or will compromise a network account, workstation, or other FAU equipment, network, or system.

- **Unauthorized Access:** Users are only authorized to access systems or network resources to the extent necessary to perform their job functions or other purpose. All other access is unauthorized. Attempting to access systems or network resources for which the workforce member is not authorized is a security violation for which appropriate disciplinary action will be taken as further set forth in University Policy 12.2 Acceptable Use of Technology Resources Policy.

- **Physical Security:** Workforce members should lock all file cabinets and office doors when they are not in their offices.

9. Encryption and Backup

Full Device Encryption: All FAU-issued mobile devices, desktops and laptops (regardless of Operating System or Platform), and USB drives (or devices used to access FAU networks or systems regardless of whether or not they are issued by FAU) that store, collect, or process PHI data must be fully encrypted using OIT-approved encryption methods and software. Full disk encryption will be used where possible on all FAU devices. All data being sent must be encrypted. Software-specific file passwords (such as Microsoft Word or Adobe PDF passwords) cannot be used as a substitute for encryption or protection. Servers may be operated without full-disk encryption provided adequate measures are taken to protect the server from loss or theft only with the written approval of the University Information Security Officer.

- **Secure Encrypted Email:** All e-mails that contain e-PHI or other confidential information must be sent securely using OIT-approved, end-to-end encrypted e-mail technologies.

- **Encrypted Backup Process:** All FAU desktops and laptops are required to use the file and document backup storage solution implemented by OIT or the responsible IT group. All FAU desktops, workstations, and portable devices using the file backup solution must be fully encrypted to protect both PHI and e-PHI in motion and at rest. The files and data stored on these backup servers are restricted on a need-to-know basis.

10. Mobile Device Management

All users of FAU issued mobile and tablet devices used to access or store PHI are required to enroll in a Mobile Device Management (MDM) solution implemented or approved by OIT or the responsible IT group.

Bring Your Own Device: FAU workforce members, staff, students, and other FAU network or system users may choose to bring their own mobile or laptop device and connect to the FAU network for official business, educational, or research purposes. Personal devices may not be used to access or store PHI without the express written approval of the Chief Compliance Officer, the Chief Information Officer, and the Information Security Officer.

REFERENCE

University Policy 12.2 Acceptable Use of Technology Resources.