Information Access Management Policy
April, 2026

APPLICABILITY:
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), including applicable amendments and requirements established under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

POLICY STATEMENT:
FAU restricts access to protected health information (PHI) and electronic protected health information (e-PHI) to the minimum necessary and requires workforce members to take reasonable measures to safeguard such information from unauthorized access or disclosure. Access to e-PHI is authorized, maintained, and modified as an administrative safeguard based on the minimum amount of e-PHI necessary for individual members of the workforce to perform their jobs effectively.

REASON FOR THE POLICY:
To ensure that FAU gives workforce members access to e-PHI on a need-to-know basis and only to the extent necessary to perform their job functions. To establish a process to grant, restrict, and terminate access to e-PHI based on the members' change in status with FAU.

RELATED INFORMATION SECURITY POLICIES:
The policies, standards, and procedures documented herein are implemented in reference to FAU's Information Security Policies listed below. In the event of any discrepancy between this document and the referenced FAU Information Security Policies, the more restrictive requirement shall apply and must be observed.

IS-POL-1: Protecting Electronic University Data
IS-POL-3: Virtual Private Network (VPN) and Remote Access Policy
IS-POL-5: Mobile Device Management
IS-POL-8: Change Management and Approval

PROCEDURES:

User Access to Computer Resources

1. Accounts and Passwords - The Office of Information Technology (OIT) will assign each new workforce member with a unique, individual user identification and initial password. Workforce members are required to immediately change their initial system to access password upon first use. Thereafter, workforce members should change their passwords at least once every ninety (90) days unless other compensating password protections are in place, such as multi-factor authentication. Where feasible, OIT will implement reminders or other mechanisms to support compliance with password change requirements.

2. System Permissions - Standard user permissions will be assigned to all authorized users and will limit the ability to install software or modify secured system configuration settings. Administrator-level permissions are restricted to OIT staff or designated departmental IT personnel. Installation of software applications, software patches, or plugins will be managed exclusively by OIT or designated departmental IT staff. Any request to grant administrator privileges to faculty or staff must be supported by a valid business justification and approved by the Information Security Officer or the director of the responsible departmental IT group.

3. Workstation Security - FAU workforce members should position computer screens to minimize visibility by unauthorized third parties or implement the use of approved screen protectors. Workforce members are required to log off their computers or lock their screens whenever they are not actively using their workstation, including during absences such as lunch or breaks. Where possible, the Office of Information Technology (OIT) or responsible departmental IT staff will configure systems to automatically log off users or lock screens after a defined period of inactivity to reduce the risk of unauthorized access.

4. Standard Access - All FAU workforce members, staff, students, researchers, personnel, and any other individuals authorized to access FAU computing resources, application systems, or the FAU network will be granted standard access by default. Individual user credentials and access to information systems may not be shared, copied, or distributed to others for any purpose.

5. Remote Access - VPN and other remote access to systems will be based on the established Office of Information Technology (“OIT”) approval processes and managed by OIT. Any change in the user status related to access rights will be

managed by the OIT workflow process. Devices used for remote access must conform to the security and privacy requirements in this policy document and Information Security policies.

6. Access Reports - OIT or departmental IT staff will review user access reports on a periodic basis on systems which store (or can access) e-PHI, PHI, or other confidential information to determine if the appropriate need-to-know standards have been applied and if policies and procedures are adhered to. Annual reviews will be conducted on network information resources to verify access rights.

7. Need to Know Checklist - All FAU workforce members and anyone else accessing FAU's networks must complete an OIT checklist to determine required access to systems. OIT will work with administrative staff during the onboarding process to determine the level of access based on necessity.

8. Portable Media Access - Any user who accesses e-PHI, PHI or other confidential information is prohibited from using unencrypted portable media devices, such as USB or CD/DVD to store, process, or transfer such information.

Changing System Access

1. OIT or responsible departmental IT staff are responsible for granting, changing, and removing system access. After access privileges have been authorized, a user account is established that enables a workplace member to access e-PHI and FAU's information systems as appropriate to his or her job function.

2. OIT and responsible departmental IT staff will maintain documentation of all user accounts and authorized access privileges.

3. Access privileges will be modified or revoked whenever a workforce member's job function or access needs to change. Modifications to user accounts are made with appropriate authorization from the affected workforce member's department in conjunction with the Office of Information Technology. Such modifications include disabling the terminated workforce member from accessing e-mail and software accounts and changing any passwords to common systems to which the terminated workforce member may have had access.

4. Each department shall ensure that reviews of access rights and user accounts for its assigned workforce members are conducted no less than quarterly to ensure continued appropriateness of accounts and levels of access. Any discrepancies identified during these reviews shall be reported to the Office of Information Technology or the responsible departmental IT staff.