1. Standard Access- All FAU workforce members, staff, students, researchers, personnel, and any other persons who are given access to computing resources, applications systems and the FAU network will be granted ‘standard access.’ Individual passwords and access to these information systems may not be shared, copied or distributed with others for any purpose.

2. 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.

3. 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.

4. <u>Need to Know Checklist</u>- All FAU workforce members, students, and anyone else accessing FAU’s networks must complete an OIT checklist to determine required access to systems. OIT will work with adm

members who should not have access from obtaining access to e-PHI.

User and Administrator Permissions

1. Standard User Permissions- All FAU workforce members and system or network users will be granted standard user permissions by default to their approved computing resources. These users will be restricted from installing software or altering their secured computer configuration settings. All installations of new software applications, software patches or plugins will be managed through OIT or responsible departmental IT staff.

2. Administrator Permissions- OIT staff or responsible departmental IT staff will be the only authorized group of users with Administrator rights to any desktop or laptop. A valid business justification for granting administrator rights to any faculty or staff must be submitted to the Information Security Officer or the director of the responsible departmental IT group.