I. PURPOSE

This policy reflects East Carolina University’s commitment to provide regular security awareness and training to its workforce members.

II. AUTHORIZATION AND ENFORCEMENT

Health Care component management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the ECU IT Security Officer, ECU HIPAA Security Officer, and ECU HIPAA Privacy Officer.

III. POLICY

ECU must develop, implement, and regularly review a formal, documented program for providing appropriate security training and awareness to its workforce members. All Health Care Components’ workforce members must be provided with sufficient training and supporting reference materials to enable them to appropriately protect EPHI on ECU information systems.

All new ECU Health Care Components’ workforce members must receive appropriate security training before being provided with access or accounts on ECU information systems. Existing workforce members must receive security training updates at a minimum of once a year.
Business associates must be made regularly aware of ECU security policies, standards, and procedures. Third party persons who access ECU healthcare computing systems or EPHI must be made aware of ECU security policies, standards, and procedures.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this policy:

1. As defined in ECU’s Security Reminders Standard, ECU must provide regular security information and awareness to its workforce members.

2. As defined in ECU’s Protection from Malicious Software Standard, ECU must regularly train its workforce members about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data.

3. As defined in ECU’s Log-in Monitoring Standard, ECU must regularly train its workforce members about its process for monitoring log-in attempts and reporting discrepancies.

4. As defined in ECU’s Password Management Standard, ECU must regularly train its workforce members about its process for creating, changing and safeguarding passwords.

VI. COORDINATING INSTRUCTIONS

1. All section policies, standards and procedures will be reviewed annually. Every section policy, standard and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention.