I. PURPOSE

This standard reflects East Carolina University’s commitment to provide regular training and awareness to its workforce members about creating, changing, and safeguarding passwords.

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. STANDARD

ECU must train Health Care Component workforce members on appropriately creating, changing, and safeguarding passwords.

IV. APPLICABILITY

This standard 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 safeguards must be implemented to satisfy the requirements of this standard:

1. ECU must train workforce members on following procedures for creating, changing and safeguarding passwords.

2. Training and awareness must cover the following topics at minimum:
   - ECU’s Minimum Passphrase (password) requirements
   - Good password practices
   - Ensuring that ECU Health Care Component workforce members understand that all activities involving their user identification and password will be attributed to them

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.