I. **PURPOSE:**
To establish technical mechanisms and Security Measures designed to guard against any Unauthorized Access to Electronic Protected Health Information being transmitted over electronic communications networks.

II. **POLICY:**
The Affiliated Covered Entity (ACE) shall implement reasonable and appropriate Technical Safeguards to detect and avoid the incidence of Unauthorized Access attacks on the component organizations of the ACE computing infrastructure connected with the storage or Transmission of Electronic Protected Health Information.

III. **DEFINITIONS:** See document “SECURITY POLICY GLOSSARY FOR DEFINITIONS OF SPECIAL TERMS (ACE-0999).”

IV. **PROCEDURES:**
A. **Standards:**
1. The policies and procedures of the ACE relating to Information Security apply to all component organizations of the ACE and all members of the Workforce.
2. All computing resources shall be assigned a Resource Owner who is responsible for the Integrity, Confidentiality, and Security of the resource.
3. When Electronic Protected Health Information is transmitted beyond the boundaries of the VCUHS and VCUSecureNet Firewalls, the information must be encrypted. The VCUHS and VCUSecureNet networks are peers and allow unencrypted access between them.
4. Whenever passwords are included in messages they must be encrypted.
5. Certain protocols and services will not normally be allowed on the networks and servers within the Firewalls. The following technical protocols are NOT allowed to be active on the production servers or network:
   a) Internet Protocol (IP) directed broadcasts.
   b) Oncoming packets to any network router equipment sources with invalid addresses.
   c) Transmission Control protocol small services.
   d) User datagram protocol small services.
   e) All forms of source routing.
6. Configuration of local user accounts within the properties of the transmission security mechanisms will be prohibited.
7. An “enable password” capability within the configurable properties of the Transmission Security Mechanisms will be maintained in a secure Encrypted format. The Transmission Security equipment configurable mechanisms to “enable password”, will be set to the current authorized Transmission Security equipment password as established by the authorized technical support components of the ACE component organizations.
8. Provide assurance that all Transmission Security Mechanism equipment is included in the ACE’s information system inventory control process and that designated individuals appointed to ensure these devices are accounted for are aware of their duties and responsibilities to inventory Transmission Security Mechanisms.
9. Initiate a standardized security warning signage message, in hardcopy and electronic format, that is directly affixed to the equipment frame, case or operators panel; and is caused to be displayed on the user access terminal upon initiation of internal operating software boot that is, or is similar in content to: "Unauthorized Access to this Network Device is Strictly Prohibited. You must have authorization by the VCU or VCU Health Systems Wide Area Network management organization(s) to access, remove, or electronically configure this device. All maintenance or replacement activities involving this device are monitored. Unauthorized attempts to access, disable, remove, or in any way tamper with this device is cause for disciplinary action and may be reported to law enforcement."

B. Responsibilities:
1. Resource Owners, including specifically the owners of the networks and common aspects of the computing infrastructure, are to implement the following safeguards to the extent reasonable and appropriate:
   a) Technical protocols that involve Security Mechanisms designed to detect and deter any Unauthorized Access to Electronic Protected Health Information.
   b) Technical protocols to protect the Confidentiality, Integrity, and Availability of Electronic Protected Health Information while being transmitted over electronic communications networks. These mechanisms may include the use of gatekeeper functions designed to deny Access to Electronic Protected Health Information to all except authorized users; and the application of Security Mechanisms, designed to detect malicious code. These mechanisms further serve to secure the Integrity of the information via internal controls, which monitor activity and analyze stored information, in an attempt to detect the presence of unwanted intrusion.
   c) Technical protocols to provide safeguards to ensure that Electronic Protected Health Information is not modified without detection, until disposed of properly.
   d) Technical protocols to provide Security Mechanisms that Encrypt Electronic Protected Health Information, whenever deemed appropriate.
   e) Technical protocols and Security Mechanisms designed to reasonably and appropriately scan the network, to identify hosts that are potentially connected to the ACE electronic network, as well as the network services operating on those hosts (such as file transfer protocol).
   f) Technical protocols and Security Mechanisms to reasonably and appropriately conduct Vulnerability scanning (both network- and host-based) to validate that operating systems and major applications are current with regard to Security patches.
   g) Technical protocols, Security Mechanisms, and automated tools to reasonably and appropriately identify problems and suspicious activity.
   h) Technical protocols and Security Mechanisms to reasonably and appropriately check file Integrity, allowing for the identification of changes to vital files, particularly unauthorized changes.
   i) Technical protocols and Security Mechanisms to reasonably and appropriately defend against trespass where malicious code is introduced by means of an electronic network.
   j) Technical protocols and Security Mechanisms to reasonably and appropriately detect intrusion over the distributed electronic network, identify the intruders, and eject the intruders from the network prior to any harm or data compromise.
   k) Technical protocols and Security Mechanisms that reasonably and appropriately defend against Threats to the electronic network and exploit Vulnerabilities within the network defenses.
1) Technical protocols and Security Mechanisms to conduct periodic network penetration testing.
m) Technical protocols and Security Mechanisms that reasonably and appropriately secure wireless networks to prevent insertion attacks, interception of information, or cause a denial of service.

2. The Information Security Contacts within each of the component organizations of the ACE shall assist Resource Owners with the selection of tools and processes to support the above objectives and will assist with the use of the tools and the review of the results.

3. The Information Security Contacts, in collaboration with the Resource Owners and the designated ACE Security Official, shall develop a schedule of Audits of the Security of the networks and resources of the ACE. These Audit steps will supplement the steps being taken by the Resource Owners as noted above and will include such activities as Vulnerability scanning.

V. RESOURCES:
A. Compliance Office
B. ACE Security Official (804) 828-1990
C. Information Security Contacts

VI. REFERENCES:
A. HIPAA: 45 C.F.R. §164.312 (e) (1).
B. VCU Health Systems — Glossary of HIPAA Terms
C. VCU Health Systems Compliance Manual
D. Implementation Directive – Policy ACE-0002

APPROVED:

Signature on File

Dr. Sheldon M. Retchin, M.D., M.S.P.H.