I. PURPOSE:
The purpose of this policy is to define guidelines for use of Firewalls and required protections for equipment that connect to external sources such as the Internet.

II. POLICY:
The computing assets of the Affiliated Covered Entity (ACE) will be protected from external Threats through implementation of layers of Firewall technology, as are reasonable and appropriate, to adequately protect the 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. Electronic communications with Business Associates, that include exchanges of Electronic Protected Health Information, must be managed via interaction with ACE devices maintained in a Demilitarized Zone Networks (DMZ) portion of the network.
4. Any devices set up in the DMZ must meet standards published by the ACE Network and Security groups. These standards include required equipment characteristics, standard software features, Audit trail maintenance, domain name server records, Technical Safeguards, and controlled Access to the devices.
5. This policy will apply only to those networks designated as DMZ networks by the VCU or VCUHS network management component organizations.

B. Responsibilities:
1. Resource Owners responsible for systems and communications involving interaction with external vendors must coordinate with the responsible ACE Network group on the set-up or modification of the DMZ devices.
2. Resource Owners, in collaboration with the Purchasing Department, are to assure that appropriate Business Associate Agreements are signed, defining the responsibilities for Security of shared information.
3. The appropriate ACE Network group is responsible for setting standards for device set-up and usage within the DMZ area.
4. The ACE Security Official is responsible for approval of any exceptions to the standard.

V. RESOURCES:
A. Compliance Office
B. ACE Security Official (804) 828-1990
C. Purchasing Department —
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.