VA Ann Arbor Healthcare System

Policy Memorandum 40-26
March 31, 2005

NETWORK ACCESS CONTROL POLICY

1. PURPOSE: To establish policy and procedure for network access control to protect information that is transmitted or processed on the local area network (LAN) and information systems connected to the LAN.

2. POLICY: Network access control mechanism must be in place for network devices and information systems that connect to the network to limit access to sensitive or critical information based on business requirements and a need to know.

3. PROCEDURES:

a. Granting Network Connections. The Information Office (IO) must approve all network devices and information systems connecting to the LAN, including but not limited to personal computers, portable computers, telecommunications lines, routers, switches, hubs, and wireless networking devices.

b. Trusted Host Relationships. Unless approved by the IO in writing, host computers must not automatically login with a predefined user ID and password to connect to network resources or devices. Whenever possible, users must be prompted for user ID and password before being granted access.

c. Security Configurations. Host computers, applications, and network devices must be configured with optional network services and programs disabled when connecting to the LAN, this includes but is not limited to, web services, simple mail transfer protocol, simple network management protocol, computer browsing, and file transfer protocol. Only network services and programs necessary to conduct legitimate business needs should be enabled.

(1) Network Communications Protocol. All network devices will be configured to communicate with the Transmission Control Protocol/Internet Protocol (TCP/IP) whenever possible.

(2) Sharing Network Resources. All network resources on the network shall implement VA approved centralized access control mechanisms and servers whenever possible. Personal computers, portable computers, and similar devices that do not follow VA user or network access controls or share network resources locally must be approved in writing before being placed on the network.

d. Encrypted Message and File Protection. All sensitive information transmitted over the VA internal network, third party network, or public networks will be encrypted using VA approved applications, algorithms, and procedures.

(1) Use of Encryption. Unless approved by the IO, all unauthorized forms of data encryption for network transmissions or file protection is strictly prohibited.

(2) Trusted Networks. A network that meets information security requirements to protect sensitive information from the time it is created to the time it is disposed, is considered a trusted network and does not require encryption. It must be sufficiently demonstrated that wherever sensitive information is processed, transmitted, or stored, it is protected from unauthorized disclosure, access, modification, or destruction.

e. Network Connections with Outside Organizations. The IO must approve in writing the establishment of direct connections between VA information systems or network devices to a network or computers at external organizations through the Internet, business affiliate, or other public networks.

(1) Firewalls. All connections between the LAN and external third party networks must be controlled and restricted by a firewall and must follow OCIS firewall configuration guidelines for applications, services, and communication ports. By default all incoming communication traffic from an external third party network to the LAN must be denied or blocked.

(2) Multi-homed Network Connections. Rooms with multiple network interface jacks connecting to the LAN and third party external networks must have additional controls in place that prevent personal computers, portable computers, and other approved network devices from being switched between the LAN and the external third party network.

(3) Multi-homed Host Connections. Host information systems with network interface cards that connect to the LAN and the external third party network is strictly prohibited.

(4) Wireless Devices. Wireless networks and access points are considered an external third party network, and must implement equivalent security mechanism to a firewall to control and restrict access to the LAN.

(5) Wireless Encryption. All wireless network communication devices connected to the VA LAN will implement layer 2 wireless network security using National Institute of Standards and Technologies (NIST) Federal Information Processing Standards (FIPS) 140 certified.

f. Modems Connections. The IO must approve in writing all inbound and outbound modem connections or dial-up lines connected to the LAN. Modem numbers are for business use only, and must not be posted in public forums, web sites, or documents.

g. Network Monitoring. All network activity must be monitored and reviewed for security relevant events on a regularly scheduled interval in a timely manner; including but not limited to hubs, routers, switches, and firewalls.

4. RESPONSIBILITY:

a. Information Security Officer (ISO). Will periodically review and audit network access control and procedures to review compliance.

b. Chief Information Officer (CIO).

(1) Authorizes all network connections to the VA Ann Arbor Healthcare System and external third party networks, including network device connections.

(2) Approves and inventories all modem connections, including faxes, for all inbound and outbound lines.

(3) Creates, updates, and maintain the local area network, wireless network, firewalls, and monitors the network and connections for security related events.

(4) Ensures network resource on the network use a centralized access control policy.

(5) Will ensure network devices only network service that are need are enabled, and other optional services that may pose a security risk are disabled.

c. Service Chiefs.

(1) Will not transmit sensitive information or files over the network without the appropriate encryption.

(2) Ensure employee under their immediate supervision do not setup modems, or network connections to external third party or public networks.

(3) Ensure employees under their control will not connect personally owned computer systems to the network unless approved by the CIO.

(4) Ensure all network devices or computers under their control do not use automatically login to a network resource unless approved by the CIO.

d. Employees. Will comply with network access control policy and procedures.

5. REFERENCES:

Policy Memorandum 40-01, Information Security Policy, March 31, 2005
Office of Cyber and Information Security Policy, Directives, and Guidelines
Federal IT Security Laws and Regulations
Computer Security Act of 1987
Office of Management and Budget (OMB) Circular A-130
Federal Information Security Management Act of 2002 (FISMA)
Health Insurance Portability and Accountability Act (HIPAA)
National Institute of Standards and Technology (NIST) guidance

6. RESCISSION: None

7. EXPIRATION: April 2008

8. FOLLOW-UP RESPONSIBILITY: Information Security Officer

JAMES W. ROSEBOROUGH
Director

Distribution A