Compliance Component

DEFINITION

Name	Personal Firewalls
Description	Personal Firewalls are devices or systems that control the flow of traffic between a network (including wireless network) and a personal computing device or a small network.
Rationale	Securing personal computers at remote locations is as important as securing them at the office. People who telecommute or access agency systems remotely must protect their systems and the data. Users accessing external networks should have personal firewall protection. Other networks and Internet Service Providers (ISPs) cannot be relied upon to provide adequate firewall protection. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls.
Benefits	• Provide protection when connecting to external networks, or from internal network threats. • Can be used as an endpoint for a Virtual Private Network (VPN).

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technology Controls
List the Technology Area Name	Secure Gateways and Firewalls
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	• Personal Firewalls shall be used on all personal computing devices that can be connected to any untrusted network. • Personal Firewalls shall be able to: o Control ports and protocols that applications use, o Work with local area network (LAN), Point-to-Point Protocol Over Ethernet (PPPoE), VPN, and dial-up connections, o Specify the systems or networks with which programs can communicate (i.e., create trusted zones or networks), o Allow virus detection software to function, o Create logs and make them available to the administrator, o Alert the user of any unusual activity, o Function as a stateful packet filter, o Be disabled and enabled by an administrator, and o Cover its IP address (operate in stealth mode).

	• Personal Firewalls should be able to associate each application with the traffic it initiates. • Personal Firewalls are implemented in one of two configurations as follows: o Personal Firewall Software shall be installed on the individual system, such as the laptop, it is meant to protect. Personal firewall software is not designed to offer protection to other systems or resources o Personal Firewall Appliances shall be used to protect small networks. Appliances include: ▪ Cable Modem WAN Routing ▪ LAN Routing (dynamic routing support) ▪ Network hub ▪ Network switch ▪ Dynamic Host Configuration Protocol (DHCP) server ▪ Simple Network Management Protocol (SNMP) agent ▪ Application-proxy agents • Refer to the Firewall Rules Compliance Component for configuration guidance		
Document Source Reference #			
Standard Organization			
Name	NIST SP 800-41, Guideline for Firewalls and Firewall Policy	*Website*	www.csrc.nist.gov/publications/nistpubs
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST)	*Website*	http://csrc.nist.gov/
Contact Information			
KEYWORDS			
List all Keywords	Personal Computer, PC, VPN, telecommute, laptop, portable, firewall rules, firewall appliance, port scan, mobile user, DSL, MDT, PDA, wireless		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

CURRENT STATUS

Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*

AUDIT TRAIL

Creation Date	06/24/2004	*Date Accepted / Rejected*	06/24/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			