Compliance Component

DEFINITION

Name	Securing Personal Digital Assistants (PDAs) and Other Handheld Devices
Description	Personal Digital Assistants (PDAs) and Other Handheld Devices are devices that provide computing, information storage and retrieval capabilities. They are capable of transmitting and receiving data either remotely or when directly connected to a network or network device.
Rationale	Ensure that only authorized devices have the capability to be connected to an agency network.
Benefits	Properly securing these devices: • Protects the network from malicious activity • Prevents compromise of agency information

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Remote Access Controls
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Standard
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	• PDAs and other handhelds are remote devices and must adhere to all policies and guidelines as other remote devices. • Only agency-approved equipment may have access to the agency's network regardless of the method of access. • Users must be briefed in computer security awareness. • Users shall exercise due diligence in protecting the device and the network they access from unnecessary risks. • Information that is confidential or classified as sensitive shall be encrypted if stored on a device. • Shall conform to the same logon and aging password policies as state-owned equipment within the agency. • Desktop applications used to synchronize devices shall be password protected. • Applications that utilize confidential or sensitive information shall be

	protected using encryption and password protection utilities. • Infra Red (IR) communication ports shall be disabled during periods of inactivity. • Antivirus and personal firewall software, where applicable, shall be installed. • Any device that is lost, stolen, or no longer in the user's possession, shall immediately be reported to the appropriate agency personnel. • Where applicable, devices shall be configured to be locked or erased remotely in the event it is lost, stolen, or no longer in the user's possession. NOTE: Agencies must review the Architecture documents and identify all applicable policies for any given device before allowing connection to the agency network. (See Securing Remote Computers and Connections CC.) Given the wide variety of PDAs and other devices that fall into this category, it would be impractical to attempt to list specific security compliance details for each type of device.		
Document Source Reference #			
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Cell, ipod, mobile, phone, blackberry, palm, pilot, Bluetooth, memory stick, jump drive, zip drive, thumb drive, flash drive, mp3, Treo, USB, encryption, password, anti-virus, firewall.		
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	04/06/2006	*Date Accepted / Rejected*	4/18/06
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			