

Information Management

Procedures for Safeguarding Material on Portable Computers

By Order of the Adjutant General:

JONATHAN P. Small
Brigadier General, KSARNG
Commander, KSARNG

Official:



ERIC C. PECK
COL, GS, KSARNG
Chief of Staff

History. This issue publishes an initial issue of this publication.

Summary. This publication establishes Policy of The Adjutant General pertaining to the protection of data on portable notebooks, tablet-PCs, and similar systems, referred to as mobile computing devices (MCD).

Applicability. This regulation applies to the office, as a State agency and a military headquarters (Hqs),. Joint Forces HQ

Supplementation. This regulation may be supplemented. Supplement must be coordinated with the Deputy Chief of Staff for Information Management (DCSIM).

Exceptions and waivers. Exceptions and waivers to this SOP must be in writing for each system covered. Items covered in Regulations and higher cannot be waived.

Suggested Improvements. The proponent of this regulation is the DCSIM. Users are invited to send comments and suggested improvements directly to DCSIM KSARNG, 2800 SW Topeka Blvd, Topeka, Kansas 66611-1287.

Distribution. A

Chapter 1 - Introduction

Overview 1-1, *Page 3*
References 1-2, *Page 3*
Descriptions 1-3, *Page 3*
Administrative requirements 1-4, *Page 3*
Products 1-5, *Page 4*

Chapter 2 – Basic Physical Security Requirements.

Securing MCDs 2-1, *Page 4*
Traveling 2-2, *Page 5*

Chapter 3 – Operating Systems

Authorized Operating Systems 3-1, *Page 5*
Ports and Services 3-2, *Page 6*
Account Management 3-3, *Page 6*
Administrative 3-4, *Page 6*

Chapter 4 – Installing Information Assurance (IA) products

Auditing 4-1, *Page 7*

Antivirus 4-2, *Page 7*
Encryption 4-3, *Page 7*
VPN 4-4, *Page 7*
Firewalls 4-5, *Page 7*

Chapter 5 – Protect the Information

Encryption (Data at Rest) 5-1, *Page 7*
Backups 5-2, *Page 8*
Privacy Screens 5-3, *Page 8*

Chapter 6 – Returning from Travel

Compliance Checks 6-1, *Page 8*
Updates 6-2, *Page 8*

Procedures for returning a “Lost” MCD

Connection 7-1, *Page 8*
Forensics 7-2, *Page 8*

Chapter 1 Introduction

1-1 Overview

- a. Laptops, portable notebooks, tablet-PCs, and similar systems, referred to as mobile computing devices (MCD), pose unique security challenges. Users of these information systems (IS) are tasked with the physical security of these mobile devices while administrators must protect the IS from compromise when used as a standalone system or when remotely connected.
- b. These systems shall be configured to provide host-based security as the primary defensive measure. Combined with the capability to connect securely from trusted or untrusted sources, the IS must protect the networks during remote user access and permit adequate configuration and security management balanced with user functionality. Technology exists to provide host-based IS protections coupled with the capability to remotely access Army internal resources through protected and securable connectivity.
- c. This Policy does not apply to two-way electronic data-retrieval devices such as BlackBerry®, two-way text messaging devices, pagers, cell-phones, and similar technologies. This SOP establishes the minimum requirements for non-compliant MCDs and shall not be used as justification to circumvent stronger protection mechanisms and products as authorized by the Designated Approval Authority (DAA). The DAA for Kansas National Guard systems connecting to an army network is the J6. All systems and subsystems connecting to the Army network, must have DAA approval.
This policy will be incorporated into the KS-SOP 25-2 when revised.

1-2. References

- a. DA 06-EC-O-0007, "Road Warrior" Laptop Security
- b. AR 25-1, Information Management
- c. AR 25-2, Information Assurance
- d. AR 380-53, Information Systems Security Monitoring.
- e. Army Information Assurance (IA) Best Business Practice (BBP), Wireless Security Standards
- f. Department Of Defense Directive (DoDD) 8100.2, Use of Commercial Wireless
- g. Devices, Services and Technologies in the Department of Defense (DoD Global Information Grid (GIG))
- h. Defense Information Systems Agency (DISA) Secure Remote Computing STIG, Ver 1, Rel 1
- i. DISA Wireless STIG, Ver 3, Rel 1
- j. Laptop Security Guidelines: <http://labmice.techtarget.com/articles/laptopsecurity.com.htm>

1-3. Descriptions

- a. Description of Former State: AR 25-2 outlines general requirements.
- b. Description of Changes Instituted: This establishes laptop security procedures.
- c. Description of End State: The following end-state standards can be effectively achieved:
 - (1) Standardized procedures and guidance for securing laptop IS.
 - (2) Conduct of multi-level awareness training will focus on management, user, and technical personnel.
 - (3) Use of technical solutions from approved vendor sources will standardize support, installation, and transportability requirements throughout the Army. These solutions can be hardware or software derived.
 - (4) Use procedural security for the return of ISs when an IS goes outside of the supporting infrastructure and connects to any external or untrusted wired or wireless network.
- d. Description of Required Resources: Authorized tools are obtained from the identified sources and installed IAW DAA approved Certification and Accreditation procedures.
- e. Description of Derived Benefits Resulting from Implementation: Uniform application of baseline laptop security requirements across the Army enterprise. Additionally, this will provide a reduction in the threats associated with connecting to "untrusted" wired and wireless networks, rapid deployment, cost effective security, and workforce mobility.

1-4. Administrative Requirements:

- a. This Policy addresses fundamental requirements for laptop usage. Security of the device is absolutely required and remote connectivity is absolutely protected.
- b. All firewalls used in a host-based security solution shall protect the laptop during the boot processes. Ideally the firewall should be certified to meet National Information Assurance Partnership (NIAP) certification to

Evaluation Assurance Level (EAL) 4 as a minimum. However, Designated Approval Authority (DAA) and System Administrators (SAs) shall evaluate the existing DoD AV contracts that provide a free firewall capability as part of the host-based security product and IS configuration in lieu of no firewall or the use of an unfunded or uncertified product. Products not certified will be replaced with approved products or the vendor must provide documented proof in meeting this certification requirement within 12 months of this BBP.

c. Users are the weakest link in MCD physical security. The laptop contains critical operational, security, or sensitive information that's a valuable foreign-intelligence resource. Users must be given the tools and training to support mobile IS security initiatives, and subsequently held accountable for such security.

d. Proper security and configuration of the laptop will prevent or hinder exploitation of the systems through physical theft, malicious logic, viruses, trojans, unauthorized access, remote viewing, replay attacks, or intruder activities. Implementation of host-based security mechanisms will secure the remote access into the trusted network and prevent unauthorized accesses, while allowing trusted access to authorized individuals.

e. The DAA, appointed in accordance with (IAW) AR 25-2, is responsible for the security configuration of MCDs and ensuring that all users adhere to the requirements outlined in AR 25-2 and this BBP. DAAs shall include MCDs as part of the risk to the existing network certification and accreditation. For brevity in this document, the term DAA/SA is used as the primary individual responsible for the security or the configuration of the MCD, however any person in the IA professional structure is included IAW local command structure or as delegated by policy.

f. Currently fielded MCD technologies that are not in compliance with this SOP must have the IASO Plan of Action and Milestones (POA&M) migration plan developed for critical requirements within six months of the effective date of this BBP to ensure the systems meet the requirements. For non-compliant procedures and devices by the IASO, the DAA is responsible for approving and maintaining these migration plans as part of their acceptable level of risk determination. Any device or procedure not in compliance and currently connecting to an Army network that is processing sensitive information should be immediately disconnected until approved.

g. Respective Directorate of Information Management (DOIM) offices shall identify and monitor all devices and local procedures. They shall have the ability to run asset management tools and perform assessment scans to locate authorized and non-compliant systems.

h. Related BBPs: (<https://informationassurance.us.army.mil/bbp/>)

- (1) 04-EC-M-0003 Wireless Security Standards
- (2) 04-EC-O-0004 Network Assessment Scanning
- (3) 04-IA-O-0001 Army Password Standards
- (4) 05-EC-M-0005 Deployment Planning for Information Systems

1-5 Products

a. The Office of IA and Compliance (**OIA&C**), NETCOM) has identified IA tools and products that enable MCDs to meet the requirements of this SOP via the Army Information Assurance Approved Products List (AIAAPL). IAM Check this list often as changes will occur frequently. AIAAPL: https://informationassurance.us.army.mil/ia_tools/IAPProducts.xls

b. The products identified below are not IA tools as they are representative of tracking and reporting technologies or capabilities. Local acquisition and use requires approval to operate and must be included in Army Certification and Accreditation standards with DAA approval. This listing is neither all-inclusive nor indicative of approved products, but indicates the type of technology available.

- (1) Asset Tracking: http://www.secure-it.com/products/stop/stop_asset.htm
- (2) CompuTrace, <http://www.computrace.com/public/main/default.asp>
- (3) StealthSignal, <http://www.stealthsignal.com>
- (4) ZTrace, <http://www.ztrace.com/>

Chapter 2 - Basic Physical Security Requirements

2-1 Securing MCDs

a. DAAs/SAs should provide users with a cable lock or alarm for traveling. Modern laptops are equipped with a Universal Security Slot (USS) that allows them to be secured via a cable lock or laptop alarm. While this may not stop determined thieves with bolt cutters, it does deter opportunistic thieves. Tubular locks are preferred over the common tumbler lock designs. Tether the MCD to permanent objects while traveling. Users should consider other alarms or devices such as motion detectors or hard drive locks for increased security. Users

Will request these items through their IA channels for a lock.

b. Users shall remove and secure removable PCMCIA cards and peripheral devices. When not in use, these items shall be kept in the MCD carrier. Eject these cards from the laptop and secure them separately. Peripheral devices may introduce additional access capabilities from insider threat personnel depending on your environment.

DAAs/SAs shall ensure that the IS information is properly annotated in property book accounts and hand receipts IAW local policies. Users shall maintain laptop serial and model identification numbers, system and domain names, and emergency POC contact information at the home office while traveling.

c. DAAs/SAs shall enable two-factor authentication through the use of CAC authenticated access. Use other biometric access systems when the MCD cannot support CAC technologies and the security of the information is paramount. Embedded CAC readers and authentication software greatly increases laptop security and user functionality. Users are responsible for ensuring their CAC credentials are valid for the length of time the MCD is disconnected or while traveling.

d. DAAs/SAs shall asset tag or engrave the MCD. There are also a number of tamper-resistant, commercially registered, asset-tagging capabilities that could help civil authorities return any recovered MCD. External markings of a registered MCD may deter opportunistic thieves and prevent its resale locally or over the Internet. Permanently marking (or engraving) an accessible, yet internal area of the IMCD with the name, address, and phone number of the security or property book POC increases the chances of having the laptop returned while maintaining OPSEC. Commanders, DAAs, and SAs must balance the external marking of laptops with security and OPSEC concerns, especially for those users traveling to remote or sensitive areas. User shall include a business card or similar identifier affixed to the laptop or in the carrying bag in all cases.

2-2 Traveling

a. Users shall secure the laptop at all times when not in use and in their possession.

b. Users should use non-descript carrying cases. Do not publicly display a laptop case highlighting the manufacturer, organization, military affiliation, or company's logo on the side. Consider using a form fitting padded sleeve for your laptop and carrying it in a backpack, courier bag, briefcase, or other common carrying case. If you are traveling in airports and train stations, secure or lock the zippers of your case so no one can simply reach into the bag and remove the laptop.

c. Users must remain vigilant during air or rail travel. There are a number of sophisticated professional crime rings targeting laptop carrying travelers. Be vigilant in any circumstance where there is a sudden diversion involving you or another person in your vicinity, especially during security checkpoints. Keep the laptop in sight at all times, especially through security checkpoints as the MCD will normally precede you through security scanners. If possible send the MCD through the security checkpoint when the exit is free of previous travelers. Laptops shall never be placed in checked or unattended baggage.

d. Car rental and travel. Always rent a car with a locking trunk and never leave your laptop in a vehicle where it can be seen. Use the cable lock to secure it to permanent vehicle mount. If possible, choose rental cars with an alarm system and no external rental identification stickers. Keep in mind that the extreme temperature ranges inside an unattended vehicle could easily destroy the MCD.

e. During hotel stays, users shall anchor the MCD to a fixed object.

f. Users shall never leave the MCD unattended in public, meetings, conventions, or conferences. Laptop thieves, intelligence agents, and corporate espionage personnel target business meetings as they know that the attendees represent government interests. Most conventions only check ID's and registration on the first day. Thieves, staff, employees, and other visitors often walk in and out of conference rooms without being challenged or even noticed in the days following the initial registration.

g. Users shall immediately report the loss of the MCD during travel to their SA, IAM and/or IASO, who in turn will report this information to their Commander, intelligence, and law enforcement representatives immediately. Since network administrative and user accounts could be cached on the MCD, the SA shall change all potentially compromised network administrative and user authenticators and configure IA devices to monitor and capture remote-access attempts to access the network.

Chapter 3 - Operating Systems

3-1 Authorized Operating Systems

DAAs/SAs shall install a secure operating system and lock it down. Only use Windows XP SP2 or Windows 2000 SP4, and DOD antivirus products. The current recommended Army baseline is a Windows XP

Professional IS. ISs running Windows 95/98/Me/NT are prohibited. The helpdesk will build the OS to Army Gold Master Standards, perform a vulnerability assessment, and eliminate or mitigate all identified vulnerabilities IAW the developed Plan of Action and Milestones (**POA&M**). Other OSs may be authorized based upon local DAA requirements, guidance, and supportability with STIG compliance.

3-2 Ports and Services

- a. DAAs/SAs shall configure MCDs to disable all unnecessary ports, protocols or services. The use of emerging protective technologies to secure the OS is recommended when they are automatically enabled at boot or immediately before the OS enables connection states. These technologies offer real-time, non-policy or non-signature based capability that can provide comprehensive OS protection, while still providing capabilities for configuration management.
- b. DAAs/SAs shall disable other-drive boot capabilities. Disabling the secondary boot drive sequences hinders the ability to access the system from another drive, such as with another operating system or boot disk. Combined with the bios password, administrators can still access the system in the event of failure.
- c. DAAs/SAs shall disable the Infrared Port and all unnecessary external media ports. Infrared ports are normally not used in enterprise environments and data can be retrieved via the infrared port if used. Disable the IR port via the BIOS and cover it with a small piece of black electrical tape, on the inside of the laptop if possible, to prevent accidental or intentional removal by the user.

3-3 Account Management

- a. DAAs/SAs shall disable the guest account and double check to make sure the account is disabled. For additional security assign a complex password to the account and restrict its logon.
- b. DAAs/SAs shall rename the administrator account. Renaming the Administrator account prevents simple automated exploitation and increases the level of effort required to manually exploit the IS using default permissions. Remember that intruders will try to compromise any local account they find and then try other accounts as they go on to improve their access. When you rename the account, do not use the word 'Admin' or any other easily guessed word in its name.
- c. DAAs/SAs shall create a dummy administrator account. Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +15 character complex password.
- d. DAAs/SAs shall prevent the last logged-in user name from being displayed in the login dialog box. This can be disabled using the security templates provided on the installation CD, or via Group Policy snap in. For more information, see Microsoft KB Article Q310125.
- e. DAAs/SAs shall disable the LanMan/NTLM protocols. All password security measures are subverted if these protocols are enabled on the IS. These protocols are not required for Win 2K or Win XP Professional networks.
- f. DAAs/SAs shall replace the "Everyone" Group with "Authenticated Users" on file shares if used. "Everyone" in the context of Windows XP security, means anyone who gains access to the network can access the data. Never assign the "Everyone" Group accesses to a file share, use "Authenticated Users" instead.

3-4 Administrative

- a. DAAs/SAs shall provide a Statement of Compliance (SoC) to the user. The SoC shall include identifying the IS by make, model and serial number, or other property code, that identifies the over-arching Authority To Operate (ATO) under which the device is approved to operate on the Army Infrastructure and the STIG and IAVM compliance status of the device. The DAA/SA should include a Letter of Accreditation (LOA) from the DAA on the IS so that the appropriate information can be presented to any visited "Trusted" Army or sister service network.
- b. DAAs/SAs shall ensure that ISs will allow only one active connected interface at a time, i.e. if WiFi access is enabled then other wireless, wired, and modem access methods shall be disabled. This ensures that devices cannot be accidentally or intentionally used as bridging or routing devices (backdoors) between two or more networks. This can be accomplished through boot-up scripts or location aware tools/applications that push policy rules to ISs based on location and current access method.
- c. Users shall never download and install third-party software and applications or enable unauthorized protocols or services.
- d. DAAs/SAs shall consider granting users elevated privileges when the threats to unpatched systems are greater than the risks posed by granting the user elevated privileges. This elevation will only be during the

period travel. If OS updates are absolutely required while on travel and the user has elevated privileges and permissions to install system updates, then the user shall update the system from pre-approved DoD, Sister Services, or Army patch server sites only.

Chapter 4 - Install authorized IA products:

4-1 Auditing

DAAs/SAs shall enable auditing. Enable all auditing available on the MCD necessary to support the network environment. DAAs/SAs will restrict permissions to the files and services to prevent any user intervention. When possible, automatically download these audit logs when the system is reconnected to the network to review the audit logs for indications of suspicious traffic or events.

4-2 Antivirus/Patch Management

a. DAAs/SAs shall install an Antivirus (AV) product. Use of AV technologies and products are mandatory and anti-virus real time protection shall be enabled by default. Laptop systems incapable of implementing DoD approved AV products are prohibited from use.

b. DAAs/SAs shall use client management/patch management software. Updating the MCD while traveling is usually not achievable due to network configurations. Procedures and policy must quarantine the reconnecting laptop, then scan the system for compliance. The system will be updated and rescanned before or when operationally reconnected to the network.

4-3 Encryption

DAAs/SAs shall enable encrypted protections on connections from untrusted to trusted network connections. Modem connectivity is no longer adequate to meet the traveling users' needs to accomplish many daily tasks. Implementing a low level encryption of the laptop is necessary due to the complex threats and inherent vulnerabilities within the operating system environments while connecting through untrusted networks.

4-4 VPN

DAAs/SAs shall install and use Virtual Private Network (VPN) technologies if backbone access to the KSNG installation LAN is required. To protect the installation network when backbone access is not required, application layer "thin client" solutions or other approved application layer SSL solutions for example Outlook Web Access (OWA) or Citrix are preferred. For VPN connectivity, DAAs/SAs shall ensure split tunneling is disabled for all internet access while on travel when backbone access to the home Army network resources (i.e. mapped drives, mail server) is required. Data access using application layer security through "thin client" (i.e. CITRIX) or Secure Sockets Layer (SSL) access to email (i.e. Outlook Web Access, or OWA) is encouraged if VPN access to the KSNG backbone is not an absolute requirement.

4-5 Firewalls

a. DAAs/SAs shall install a host-based firewall. Protect the laptop by installing a firewall to deter intruders or malicious logic from entering the system via the untrusted connection, then subsequently introduced into the KSNG network when the systems is returned to the local network. The firewall should be capable of isolating the laptop during boot processes. The use of free, foreign owned, or trial-use host-based (resides on the system itself) firewalls on government systems shall be prohibited, as much of the desired functionality and granularity required to adequately protect the IS or manage the firewall is nonexistent. Free or limited-use licenses installed on government systems violate the end license agreements of the firewall vendor. Host-based protective software shall not be capable of user disablement. The firewall should be capable of implementing application level controls and shall be centrally manageable.

b. DAAs/SAs shall install all emerging DoD provided solutions when appropriate to that IS. Use host-based adware/spyware/malware prevention and the emerging host-based security system (HBSS) solution when made available. Update the web-browsers to include the capability of blocking unwanted pop-ups or adware as part of the default configuration of the laptop.

Chapter 5 - Protect the Information:

5-1 Encryption

DAAs/SAs shall ensure that approved encryption is used for protecting data-at-rest on all mobile ISs. This

can be accomplished by using “whole disk” encryption tools or “file system” encryption tools for sensitive or unclassified information as available on the AIAAPL. Additional encryption security requirements may be required depending on the sensitivity or classification of the data. All ISs processing Army information in a mobile computing environment shall provide a capability to protect data at rest and in transit. Both Windows 2000 and XP Pro ship with Encrypting File System (EFS), an encryption system that adds an extra layer of security for drives, folders, or files. This will help deter an attackers’ ability to access files such as physically mounting the hard drive on another PC and taking ownership. If EFS is used, be sure to enable encryption on Folders, not just files as all files that are placed in that folder will then be encrypted.

Note: There are significant issues associated with the implementation of EFS and the creation and maintenance of EFS certificates that the DAA and the data-owner must consider before implementing this solution.

5-2 Backups

Users shall conduct backups of the data on the IS periodically and before the user departs. It is harder to recreate the information than it is to acquire another laptop. As users, always backup and synchronize the information before you travel. Capabilities and applications exist that can image and store a laptop image and configuration over network resources, and should be part of the DAAs/SAs enterprise management structure. The time spent to perform image backups is considerable less than recreating these environments. SA/NAs should perform and store an image of the system configuration before every user departure. It is easier to restore an image of the OS when the laptop contains proprietary, specialized, or restricted distribution applications or configurations. Users must implement and practice an alternate data security and recovery plan during travel as traveling places all of your data at risk.

5-3 Privacy Screens

Users shall use privacy screens in public facilities or during travel. There are privacy screens and privacy filters designed for laptops. Excellent for open, high-traffic environments where on-screen data needs to be unreadable, products such as 3M's® Blackout Privacy Technology makes on-screen data visible only to persons directly in front of the monitor without distortion. Any similar vendor capability is acceptable. Users need to request privacy screens and filters through their IA channels.

Chapter 6 - Returning From Travel:

6-1 Compliance checks

- a. DAAs/SAs shall check any IS that has been on travel or was connected to an external or untrusted network for compliancy and contamination.
- b. Automated quarantining and scanning of the re-connected system is preferred over manual assessment methods. As such, the following shall be checked as a minimum:
 - (1) Using a Vulnerability Assessment Scanner or configuration management application (i.e. Citadel Hercules), all reconnected IS shall be checked for vulnerability compliance.
 - (2) Scan for spyware using Army approved tools.
 - (3) Compare the assessment to pre-deployed baselines or original security baseline configuration to determine if the IS or the registry has been altered. Any registry changes shall be identified and verified as authorized.

6-2 Updates

- a. Update the anti-virus definition file and perform a full system scan.
- b. Keep IS scan results for verification that the IS was clean if a discrepancy ever occurs.

Chapter 7 - Procedures for a returned “lost” MCD:

7-1 Connection

DAAs/SAs shall treat all returned “lost” MCD, regardless of the length of time, as compromised and the state of the IS shall never be trusted. **Never connect a returned “lost” system to any operational LAN environment.**

7-2 Forensics

a. Once a "lost" MCD has been returned, Commanders and DAA shall notify the NGB Law Enforcement (LE) Computer Crimes Investigative Unit (CCIU) and Counterintelligence (CI) representatives available through their supporting Regional Computer Emergency Response Team (RCERT) of such recovery.

b. The DAA/SA will provide all associated information available relating to the loss, such as time and date of the loss, returning organization, method of recovery, location of recovery, data type and sensitivity, content, and any other related information to determine if there is any LE/CI interest in the MCD.

c. The DAA/SA will secure the MCD and take no actions to recovery any information until the LE/CI agents provide their response. If both LE/CI agents release the system, the DAA/SA shall consider the types and methods of transferring any remaining information and the risks associated with such activity. Preference is to not allow such activity when possible.

d. A bit by bit image will be taken of the storage media and kept for future use.

e. If data is to be moved, the SA shall update all existing IA product definitions such as antivirus, spyware, and other locally approved malware identification applications on the system and run in-depth scanning.

f. Transfer only user identified irreplaceable or critical information to an external media, preferably to write-once optical media. Under no circumstances shall executable code be copied from the compromised IS.

g. Remove and store the original hard drive, and all related actions and data, for future forensic or investigative requirements for a period of at least 1 year. Replace and rebuild a new drive for the returned system.