Army Electronic Product Support (AEPS)
Security Policy

Army Materiel Command

Executive Agent—Web Logistics Initiatives

September 25, 2000

Version 4.0

Changes from version 1.0 to 2.0:

Add: . 1.3 s-dd.
2.5. Requesting Addition of Information (Pages/Links) to the AEPS System
4.3.c.
4.3.d.
4.3.e.

Change from version 2.0 To 3.0

Change: Para. 1.4. Responsibility – Change Project Manager (PM) to Executive Agent (EA).

Change: Para 4.3.d. Passwords will contain at least one lower-case character and two numbers.

Change Para.: 4.3.a. Changes process of acquiring authorization from supervisor's faxing form to AEPS office to supervisor's approval through email. Add: "After the information has been submitted by the user, the program will kick off an email message to the supervisor/COR/COTR for validation of the user information, approve or disapprove, and forward the form electronically to the designated AEPS ISSO for final approval."

Change from version 3.0 to 4.0

Added paragraph 4.4 on PKI.

Changed/updated reference on PKI policy: Changed to Assistant Secretary of Defense, Memorandum, 12 August 2000, subject: Department of Defense (DoD) Public Key Infrastructure (PKI).

Changed paragraph 2.5.e. to include "and javascript will be kept to a minimum".

Added to 1.3 Applicable Policies, Guidance and Regulations: DoD Manual DoD 8510.1-M, 31 Jul 00 1/4/01

Deleted Para. 2.5 Requesting Addition of Information 1/10/01
Added to Para. 2.5.a. "or PKI Certificate"
Deleted from Para 4.3.d. Passwords will contain at least one lower case character.

ARMY ELECTRONIC PRODUCT SUPPORT (AEPS) SECURITY POLICY

TABLE OF CONTENTS

Page

1. OVERVIEW.

1.1. Purpose. The U.S. Army Materiel Command (AMC) AEPS web site provides users with wholesale level logistics information as well as interactive capabilities. The purpose of the AEPS security policy is to protect the system's integrity from alteration, tampering, theft, inaccuracy, destruction, inability to process data, and intrusion by unauthorized users. This policy shall be made available to all AEPS Integrated Process Team (IPT) members and AEPS users.

1.2. Scope. This policy applies to:

a. All DoD military, civilian and contractor personnel who access the AEPS site.

b. All AEPS IPT web administrators.

c. All AEPS hardware and software located at the Rock Island, Illinois site, and the AEPS equipment fielded to other AMC installations.

d. Data derived from various applications residing on the AEPS system.

1.3. Applicable Policies, Guidance and Regulations.

a. Department of Defense (DoD) 5200.28, Security Requirements for Automated Information Systems, 21 March 1988.
b. DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria (TCSEC), December 1985.
c. DoD 5200.1-R, Information Security Program Regulation, August 1982.
d. DoD 5500-7-R, Joint Ethics Regulation (JER) with change 2, 30 August 1993.
e. National Computer Security Center (NCSC)-Technical Guide (TG)-005, Version-1, Trusted Network Interpretation, 31 July 1987.
f. Army Regulation (AR) 380-5, Department of the Army (DA) Information Security Program, 25 February 1988.
g. AR 380-19, Information Systems Security (ISS), 27 February 1998.
h. AR 380-53, Communications Security (COMSEC) Monitoring, 15 November 1984.
i. ASR 25-4, Control and Protection of Commercial Software, 15 May 1991.
j. DA SAIS-C4C Message, DTG 231030Z OCT 96, Computer/Network Security For System Administrators.
k. DA DAMO-ODI Message, DTG 32015Z SEP 96, Activation of the Army Computer Emergency Response Team (ACERT)/Coordination Center (CC).
l. DA, Director of Information Systems for Command, Control, Communications, and Computers (DISC4) Message, DTG 051550Z APRIL 96, C2 Protect Common Tools.
m. DAMI-CHS Memorandum, Certification of Telecommunications Security Monitoring Notification Procedures, 30 April 1997.
n. National Security Agency Report #C44-022-97, Securing Your Webserver, 20 June 1997.
o. AMC Information Systems Architecture, May 1998
p. Deputy Secretary of Defense memorandum, Information Vulnerability and the World Wide Web, 24 September 1998.
q. Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Web Site Administration Policies & Procedures, 25 November 1998.
r. AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA), 15 January 1993.

s. FIPS PUB 87 – Federal Information Processing Standards Publication Guidelines for ADP Contingency Planning, 27 March 1981.
t. Security Policy for USAISEC Network, April 1998.
u. SANS Institute, Intrusion Detection version 1.2.2 980905, November, 1998.
v. SANS Institute Computer Security Incident Handling, version 1.5, May 1998.
w. DoD 5200.40-M (Draft) Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document, December 20, 1998.
x. DoD Web Site Administration Policies & Procedures, November 25, 1998.
y. Netscape Communications Corporation, Single Sign-on Deployment Guide (Security), 1997.
z. DoD Public Key Infrastructure Roadmap for Department of Defense (DoD), version 2.0, Revision C, May 11, 1999.
aa. DoD Public Key Infrastructure Local Registration Authority Standard Operating Procedures Version 1.0, September 1998.
bb. Assistant Secretary of Defense Memorandum, subject: Department of Defense (DoD) Public Key Infrastructure (PKI), 12 August 2000.
cc. DoD X.509 Certificate Policy.
dd. TACOM Policy 3-96, TACOM World Wide Web Page Policy, 30 August 1996.
ee. DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

1.4. Responsibility.

a. The AEPS Executive Agent (EA) is responsible for ensuring that the AEPS system has adequate information system security, and that this policy is observed. The AEPS EA will designate the AEPS Information Systems Security Officer (ISSO).

b. The AEPS Information Systems Security Officer (ISSO) will provide coordination for security and configuration management with the Installation ISSMs and the AEPS IPT system Administrators at each AEPS site. The AEPS ISSO is responsible for configuration management of the AEPS primary domain server.

c. AEPS IPT System Administrators are responsible for ensuring that the AEPS MSC servers are maintained to the latest configuration, including all necessary security patches.

d. All authorized AEPS users are responsible for protection of AEPS information systems equipment and data regardless of the security mechanisms that are in place.

e. All users have the responsibility to report to the AEPS ISSO any actions that conflict with this policy.

2. AEPS USER ROLES AND RESPONSIBILITIES

2.1. Who is an Authorized AEPS User? Authorized users will be granted AEPS website access for a finite period of time (determined by the AEPS ISSO). Permissions are based on the least privilege principle, and need-to-know to perform official duties using the AEPS system. The following categories of personnel may be authorized access to AEPS:

a. Active duty U.S. military personnel, U.S. Reserves personnel, and National Guard personnel.

b. Department of the Army civilian personnel

c. Contractor personnel under active contract delivery orders for AMC MSCs/activities. The AEPS System Administrator or ISSO will verify contractor information with the Contracting Officer Representative (COR).

d. Other Federal department/agency civilian personnel authorized by the requesters supervisor, the AEPS PM, and verified by the AEPS ISSO.

e. Other personnel as authorized by the requestors supervisor, the AEPS EA, and verified by the AEPS ISSO.

2.2. Acceptable Use of the AEPS System.

Authorized users may:

a. Perform queries to AEPS systems.

b. Use, print, or download information obtained through AEPS in the conduct of official business.

c. Submit official documentation, such as requisitions, Supply Discrepancy Reports, Quality Deficiency Reports, etc., via AEPS.

2.3. Unacceptable Use of the AEPS System. It is unacceptable for any user to:

a. Provide false or inaccurate information when registering for an AEPS user ID and password.

b. Access accounts or resources not required in the performance of your duty nor specifically granted to you by the AEPS ISSO or AEPS System Administrator.

c. Share user IDs/passwords with other persons.

d. Attempt to “crack” passwords to gain access to the AEPS system, or to restricted AEPS data for which you have no need-to-know.

e. Send harassing or other inappropriate or unofficial e-mail using the AEPS resources.

2.4. Restricted Use of the AEPS System.

a. A valid user ID and password or PKI Certificate are required to enter the AEPS website. The identity of each authorized user will be positively established before granting access.

b. Valid users may access only data for which they have the “need-to-know” to perform their assigned duties.

c. There will be no “guest” accounts established in AEPS.

3. ACCESS RESPONSIBILITIES

3.1. Authorization to Grant and Terminate Access to the AEPS System. The AEPS ISSOs are authorized to grant and terminate access. This includes the right to disable accounts not used for 90 days. The System Administrator or ISSO will attempt to notify

users via email prior to disabling their account. The AEPS ISSO may disable accounts for misuse.

3.2. Access Control. The AEPS System Administrator will control access to the AEPS Primary Domain Server.

4. USER RIGHTS AND RESPONSIBILITIES.

4.1. General.

a. AEPS users may access data for which they have the "need-to-know " to perform their assigned duties.

b. Authorized AEPS users may access the AEPS site 24 hours a day, seven days a week.

c. AEPS users are responsible for downloading necessary browser software and tools required. This also applies to browser-side security patches.

d. AEPS users are responsible for protecting their passwords as For Official Use Only (FOUO).

e. AEPS users will access only resources as authorized.

f. AEPS users are responsible for understanding and following the AEPS security policy.

g. AEPS users are responsible for notifying the AEPS ISSO or System Administrator when a potential security violation, vulnerability, suspicious activity or system failure occurs.

h. AEPS users must update their information when there is a significant change in status, such as employment status, new duty location, or name change. Information can be updated through the AEPS system while on-line or users can contact the AEPS ISSO to have their information updated.

i. AEPS users are responsible for safeguarding any and all information downloaded from AEPS, regardless of media type.

4.2. User Actions Considered Abuse of the AEPS System. The following actions are considered AEPS policy violations:

a. Illegal or unauthorized entry, viewing, modification, destruction, manipulation or causing denial of access to information residing on the AEPS system.

b. Removal (or use) of hardware, software or media from any AEPS server site without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

4.3 Passwords.

a. Individuals requiring access to information that requires user identification and passwords will submit their request electronically through the AEPS web site. This request will then be forwarded to the supervisor for verification of user information.

The supervisor/COR/COTR will verify and/or correct user information, approve or disapprove, and forward the form electronically to the designated AEPS ISSO for final approval.

b. Passwords should not be a word or phrase that would be obvious to a hacker. Passwords that are the same as the user ID or a variant thereof, or the actual word "password" are not to be used. Examples of invalid passwords include words found in the dictionary, names, places, and commonly used acronyms.

c. Passwords must be a minimum of 8 and no more than 14 characters in length.

d. Passwords will contain at least two numbers.

e. Passwords will expire every six months (for contractors, expiration occurs at the end of the contract period or every six months, whichever comes first).

f. If an employee leaves an organization, he/she must notify the AEPS office through his/her supervisor.

g. Name changes or other user data will be updated using the AEPS web site.

h. Passwords will not be shared.

i. Passwords should not be written down in any way that would allow discovery and compromise of the AEPS system or data therein.

j. Passwords will be inhibited from unauthorized observation on terminals and video displays.

k. Users will be limited to three logon attempts. The user must contact the AEPS System Administrator to have access enabled.

4.4. Army Public Key Infrastructure (PKI) Implementation into AEPS

The AEPS web administrators have currently PKI-enabled the AEPS web site, using a 128-bit Secure Sockets Layer (SSL), for use with both DoD PKI certificates. Until full client authentication implementation is completed in October of 2002, the AEPS server will be configured to accept both Userids/passwords and a DoD PKI certificate.

4.5. Backups. The System Administrator is responsible for backing up the AEPS primary domain server daily. ARCserve software is used to perform back ups to include the back up of the Oracle data bases.

4.6. Virus Software. The AEPS System Administrator and the IPT System Administrators will ensure that the latest DoD approved anti-virus software is installed on the AEPS primary domain server and the AEPS MSC servers. AEPS users are responsible for notifying the AEPS System Administrator of any viruses contracted from the AEPS web site.

5. SYSTEM ADMINISTRATOR RIGHTS AND RESPONSIBILITIES

5.1. Administrator Rights and Responsibilities of User Files. The AEPS System Administrator will access log files for security monitoring, troubleshooting and maintenance purposes in accordance with AR 380-19, Information Systems Security, 28 February 1998.

The System Administrator will maintain confidentiality of user files and server traffic analysis.

5.2. Handling of Information. The AEPS site may store, process and transmit sensitive but unclassified (SBU) and unrestricted (publicly accessible) data.

6. SECURITY POLICY VIOLATIONS. Authorized AEPS users are subject to disciplinary action if they knowingly and willfully violate any provision of the AEPS Security Policy and its references. Unauthorized users who violate this policy are subject to conditions and punishment as provided by the *Computer Fraud and Abuse Act*, *18 U.S. Code 1030, 1984*, or the appropriate public law.

7. INCIDENT HANDLING.

7.1. Monitoring Notice. To enter the AEPS web site, the user must accept the following notice:

This is a Department of Defense computer system. This system, including all related equipment, networks, and network devices are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. It is a violation of United States Code, Title 18, to access and use U.S. Government computer resources without specific authorization. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

7.2. Incident Handling Responsibility. Any security incidents will be investigated to determine their cause and the cost effective actions required to prevent reoccurrence. Suspected or actual incidents will be reported to the AEPS ISSO, who will notify the Information Systems Security Manager (ISSM). Concurrently, the ISSO and ISSM will notify the Army Computer Response Team/Coordination Center (ACERT) and request immediate technical assistance.

7.3 Incident Notification. The AEPS ISSO will report any security violations to the Land Information Warfare Activity's (LIWA) Army Computer Emergency Response Team (ACERT).

8. PUBLICIZING THE POLICY.

8.1. Publicizing New Policy. This policy will be placed on the AEPS site for all users to review. AEPS users are encouraged to submit comments to the AEPS ISSO.

8.2. Policy Changes. AEPS users will be notified when this policy has changed. A special notice will be made available on the main menu of the AEPS site with a link to the changed policy.

ACRONYMN LIST

ACERT – Army Computer Response Team/Coordinator Center

AEPS – Army Electronic Product Support

AMC – Army Materiel Command

AR – Army Regulation

COR – Contracting Officer Representative

COTR – Contracting Officer's Technical Representative

DOD – Department of Defense

FOUO – For Official Use Only

IPT – Integrated Process Team

ISSO – Information System Security Officer

ISSM – Integrated Sustainment Management

LIWA – Land Information Warfare Activity

MSC – Major Subordinate Command

OPSEC – Operation Security

PM – Project Manger

POC – Point of Contact

PAO – Public Affairs Office

SBU – Sensitive But Unclassified