



DEPARTMENT OF THE ARMY  
UNITED STATES ARMY JAPAN AND I CORPS (FORWARD)  
UNIT 45005  
APO AREA PACIFIC 96343-5005

REPLY TO  
ATTENTION OF

APAJ-IM

8 February 2016

COMMAND POLICY MEMORANDUM 16-02

FOR SEE DISTRIBUTION

SUBJECT: Cyber Security Policy

1. References:

a. Army Regulation (AR) 25-2, Information Assurance, RAR 23 March 2009.

b. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

2. Purpose: To set the standard for prevention of and proper resolution of all cyber-related incidents.

3. Applicability: This policy applies at all times and in all locations to all Soldiers, Civilian Employees, Contractors, and Local National Employees who access unclassified and classified networks through any Army portals in Japan.

4. Cyber security is critically important to the Army's ability to complete its missions. Army information constitutes an asset vital to the effective performance of our national security roles. While all communication systems are vulnerable to some degree, the ready availability of low-cost IT, freely distributed attack tools, increased system connectivity and asset distribution, and attack-standoff capabilities make computer network attacks (CNAs) an attractive option to our adversaries. Information Assurance capabilities and actions protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense (CND). Management of Army information is imperative so that its confidentiality, integrity, availability, and non-repudiation can be ensured, and that users of that data can be properly identified and authenticated.

5. Civilian and military personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policies and procedures.

APAJ-IM  
SUBJECT: Cyber Security Policy

a. Sanctions for Civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral admonition or written reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to Information Systems (IS) or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; involuntary reduction in grade or pay, and/or dismissal from employment. Sanctions for Civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may be awarded only by Civilian managers or military officials who have authority to impose the specific sanction(s) proposed.

b. Sanctions for military personnel may include, but are not limited to, some of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to IS or networks and classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by service directives and any administrative measures or non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ).

c. Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations and must maintain employee discipline. The contracting officer, or designee, is the liaison with the defense contractor for directing or controlling contractor performance.

d. Local National Employees are subject to loss or suspension of access to IS or networks, and referral to the Contracting Officer's Representative (COR) for discipline under the terms of the negotiated labor contracts and agreements. Intentional violations will be referred to the Government of Japan for consideration of prosecution under appropriate Japanese laws.

6. Point of Contact for this action is the Director, Network Enterprise Center, Japan: 78th Signal Battalion Commander at 262-3100.



JAMES F. PASQUARETTE  
MG USA  
Commanding

DISTRIBUTION:

A  
B

*Team, Cyber Security is  
critically important to the success  
of US Army Japan*