MANAGEMENT DIRECTIVE

535.9
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

Physical and Information Security Awareness Training

By Direction Of:

Kristen Miller, Acting Secretary of Administration

Date:

October 3, 2006

This directive states the policy and procedure agencies must follow to allow all employees and contractors to receive information security awareness training at least once a year.

1. PURPOSE. This management directive establishes the requirement for security awareness training for all Commonwealth of Pennsylvania (CoPA) employees and contractors that access CoPA computer networks. Security awareness training will assure that all Users are familiar with information technology security best practices, policies, procedures and standards as well as the importance of protecting confidential and sensitive information. Security awareness training is also a requirement of state and federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

2. SCOPE. This directive applies to all Users in departments, boards and councils (agencies) under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow the policy and procedures stated in this directive.

3. DEFINITIONS.

a. Anti-Virus Software - A program that searches a hard disk for viruses and removes any that are found. Most anti-virus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.

b. Firewall - A system designed to prevent unauthorized access to or from a private network. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

c. Intrusion Detection System (IDS) - Inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

d. Security Awareness Training – The learning of potential security threats and the safeguards required to handle those threats for the purpose of protecting valuable Commonwealth resources and information.

4. BACKGROUND. A layered defense is one of the key basic principles of security. A layered defense implements different security solutions at different points within the enterprise to achieve an overall blanket of security. The more lines of defense an organization has the less likely there will be a successful security breech. Security layers increase the likelihood an attack will be detected, forcing the attacker to give up and move to another target. Physical security layers include police and fire protection, anti-intrusion mechanisms such as doors, locks, closed-circuit monitors and access cards. Technical security layers include firewalls, network intrusion detection system, and anti-virus software. Administrative security layers include security policies, procedures, and security awareness training. Educating an organization's employees has proven to be the most cost-effective countermeasure against security violations. Employees that are aware of potential security threats can prevent or minimize the detrimental effects of those threats.

5. POLICY.

a. All Users are required to complete security awareness training once every 12 months. All new Users will receive mandatory security awareness training as part of new employee orientation.

b. Managers will assure that Users under their supervision are aware of and complete the security awareness program. Training Coordinators will work with agency managers to assure all their Users have completed security awareness training on a yearly basis.

c. The agency security officers in conjunction with agency training officers shall be responsible for maintaining and reviewing security awareness reports and reporting compliance to the Office of Administration. Enterprise learning management tools will be used to provide reports of agency and employee compliance.

d. If the provisions of a collective bargaining agreement, memorandum of understanding, or arbitration award are inconsistent with any of the policies or procedures of this directive, those provisions shall take precedence insofar as they apply to the Users encompassed by the agreement, memorandum, or award.

6. RESPONSIBILITIES.

a. Office of Administration Responsibilities:

(1) The Office of Administration will be responsible for developing the security awareness content and distributing that content in any form (i.e. computer-based training, classroom, video etc.) necessary to reach all CoPA Users.

(2) Assure that all agency training is delivered in a non-discriminatory manner consistent with Commonwealth equal opportunity policy and the Americans with Disabilities act.

b. Agency Responsibilities:

(1) Assure that all Users receive yearly security awareness training.

(2) Report training compliance to the Office of Administration on a yearly basis.

7. DISCIPLINE. Users who fail to complete the security awareness training may be subject to disciplinary action.

8. QUESTIONS. Questions pertaining to this policy should be directed to the Bureau of Enterprise Architecture via ra-oaitb@state.pa.us.