VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 27) 17 August 2006

Virginia Military Institute Security Awareness Policy

The Commonwealth of Virginia has developed an Information Technology Security Standard, upon which the VMI Security Awareness Policy is based. This standard is documented in Appendix 1.

VMI requires everyone who possesses a network account to participate in security awareness training within 30 days of their engagement date. After the initial training, periodic refresher training will be required on as needed basis which may be conducted two or more times annually.

Process:
The training mechanism and its contents are approved by the VMI ISSO (Information Systems Security Officer). The training URL is http:\www.vmi.edu/sa.

An email is automatically generated to each user as a notice to take or retake the training as appropriate. The first notice will normally be sent 30 days prior to the training completion deadline. A second notice will be sent 15 days prior to the training completion deadline. If the user has not completed the training within 10 days of their deadline a notice will be sent to them each day until they complete the training or the completion date has passed.

If a user fails to complete the required training by the deadline set for them, their network access will be disabled the morning of the following day-of-business. Disabling an account will not corrupt any user data and email message will continue to be received. However, the user will not be able to access any of these services. To enable a network account, the user must present him/herself, along with a photo ID, to the Help Desk. The Help Desk will reset the training completion deadline by one additional business day so that the user may complete the Security Awareness Training.

A user history file is maintained in a secure access database where reports are generated upon request of an authorized user. Authorized users include the APA auditor, the Human Resources department, and the VMI ISSO (Information Systems Security Officer). Upon separation of a VMI employee, the Human Resources department will print the employee's training history to be placed in their permanent file. At that time the employee will be purged from the security awareness history file. All other user's history will be purged when their network account is deleted.

FOR THE SUPERINTENDENT:

Walter L. Chalkley
Colonel, US Army (Retired)
Chief of Staff

DIST: B C

APPENDIX 1

COV ITRM Standard SEC2001-01.1

Section B:
Security Awareness

Security Awareness refers to those practices, technologies and /or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources. A "User" is an individual or group who has access to an information system and/or its data. (A "User" includes employees, cadets, contractors, emeritus faculty, and anyone else who has been assigned a VMI network account.)

Users within an Agency need to understand the sensitivity of the Agency's information resources and their responsibility in protecting those resources. For example, Users need to be aware of the threats and the associated impacts of a compromised password; of potential viruses transmitted over the Internet, email, and IM (Instant Messaging), sensitive data copied to laptop computers, floppy disk, CD/DVD, and USB flash memory devices; of corrupted databases; and of the accessibility of printed information generated from the system.

Although responsibility to adhere to State statutes and Agency policy and procedures is accepted by personnel upon engagement, Security Awareness programs provide a proactive mechanism to foster further comprehensive of an individual security responsibilities; to contextualize security responsibilities to specific job duties and case examples; to motivate personnel towards security-conscious behavior while performing their duties, and to reinforce the consequences of security failures on the State, the Agency, its missions, its customers, and the User.

Defining the appropriate amount, depth, and timing of Security Awareness is a risk-based decision. Best practices suggest that a Security Awareness program that utilizes a combination of periodic training sessions (introductory/refresher) and on-going security awareness promotion (marketing) are most effective. In addition, where appropriate, an Agency may decide not to grant certain access rights to personnel until the desired level of Security Awareness Training has been successfully completed. Lastly, as the business and technical environment changes, security awareness material will need to be updated accordingly.

B.1 Standards

B.1.a) Each Agency must establish and maintain information technology security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

B.1.b) A security awareness training program must:

- be approved by the Agency's Information Systems Security Officer (ISSO);
- specify timeframes for receiving training (initial, ongoing and/or refresher);
- provide both general and position appropriate security awareness content, and,
- be documented on an auditable medium

B.1.c) All new hires who use information resources or who have access to areas where information resources reside must receive formal security awareness training as designed by their Agency within 30 calendar days of their state date.

B.1.d) Receipt of Security Awareness Training must be documented in the employee's personnel file with employee's acknowledgement of receipt and understanding.

B.1.e) Security Awareness Refresher Training must be provided to personnel annually at a minimum.