VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 27) 21 October 2019

Virginia Military Institute Security Awareness Policy

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 at least once annually. Any user who is found to be associated with a compromised system may be required to complete additional refresher training. For users whose access is restricted to Post View for HR purposes, security awareness training is not required.

An account that grants a user access only to VMI Email is not considered a network account.

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

Users are notified by email that they must complete the training within a specific timeframe. 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 within the established 30-day timeframe, their network account will be disabled. When a network account is disabled, services such as Post View, network drives, or Canvas learning management system are not accessible. The account will remain in a suspended state until the user contacts the Help Desk in Nichols Engineering Building (NEB) or Barracks Help Desk.

When a user account is initially disabled, the user can:

- call the NEB or Barracks Help Desks in order to have the account privileges enabled for a 24-hour timeframe. The user will be required to provide an account ID to the Help Desk personnel.

If the user does not complete the training program in the 24-hour timeframe, their account will be disabled again. Upon a second instance of a disabled account, the user must:

- physically report to the NEB or Barracks Help Desk with a valid photo identification. Upon IT Help Desk ID verification, the training deadline will be reset for an additional 24 hours.

If a third instance of non-compliance occurs, the user must:

- physically report to the NEB or Barracks Help Desk with a valid photo identification. At this time the Help Desk personnel will enable the account and the user will be led to a computer lab where they are required to complete the training program. Upon completion, the user must physically go to the Help Desk where the program completion will be verified by support personnel.

A user history file is maintained in a secure database where reports are generated upon request of an authorized user. (Authorized users include the APA auditor, the Human Resources department, IT Support Staff, and the VMI ISO. When the user leaves VMI and their network account is deleted, the user's training history is moved to the security awareness history file.

FOR THE SUPERINTENDENT:

James P. Inman
Colonel, US Army (Ret.)
Chief of Staff

DIST: E, Cadets
OPR: IT