VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 27) 20 May 2024

Security Awareness Policy

VMI requires everyone who possesses a network account to participate in security awareness training within 30 calendar 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 Human Resources purposes, security awareness training is not required.

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

Users with administrative network accounts will be required to take supplemental role-based training.

Faculty and staff will also receive simulated phishing email, annually. Employees who fail the simulated phishing email exercise will be required to complete supplementary security awareness training.

Process:
The training mechanism and its contents are approved by the VMI ISO (InformationSecurity 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.

Cadets will have an administrative hold placed on their accounts at the beginning of the Fall semester. Upon completing the required training, the hold will be released.

For Employees who fail to complete the required training within the established 30-day timeframe, their network account and any administrative network account will be disabled. When a network account is disabled, services such as Post View, network drives, and Canvas learning management system are not accessible. When an administrative network account is disabled, the user will lose the ability to perform administrative functions. The account will remain in a disabled state until the user contacts the Help Desk in Nichols Engineering Building (NEB).

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

- call the NEB Help Desk in order to have the account privileges enabled until 1700 the

same day. The user will be required to provide an account ID to the Help Desk personnel.

If the user does not complete the training program by 1700 the day the account was re-enabled, their account willbe disabled again. Administrative network accounts will not be re-enabled. Upon a second instance of a disabled account, for non-administrative network accounts, the user must:

- physically report to the NEB Help Desk with valid photo identification.Upon IT Help Desk ID verification, the account privileges will be enabled until 1700 the same day.

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

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

John M. Young
Colonel, Virginia Militia
Chief of Staff

DIST: E, Cadets
OPR: IT