

VIRGINIA MILITARY INSTITUTE  
Lexington, Virginia

GENERAL ORDER)  
NUMBER 50)

26 August 2013

Appropriate Use of VMI Information Systems

1. Purpose

The purpose of this policy is to establish the standards for which actions are and are not permitted on VMI information systems and the VMI network. VMI's information systems and the VMI network are designed to enhance educational and research work and to facilitate administrative processes.

2. Scope

The scope of this policy covers the use of all VMI information systems (to include desktops, laptops, PDAs, and tablets), and applies to all cadets, Institute employees (to include faculty, staff, and classified employees), and all other users of VMI information systems.

3. Expectation of Privacy

All users of VMI-owned systems, or personally-owned systems connected to the VMI network have no expectation of privacy. This includes any files residing on VMI hardware, or information moving across VMI's network. VMI may monitor, inspect, store, or disclose any activity, electronic communication, or record on its network, and IT systems, include, but are not limited to, network traffic; application and data access; keystrokes; user commands; email and Internet usage; and message and data content may be accessed and monitored, for any legitimate purpose, whenever it is deemed necessary.

All users are not to disable, tamper with, or sabotage features, processes, and software which prevent, or detect fraud, or other policy or legal violations such as, but not limited to, logging, and monitoring software, servers, and devices on VMI systems and infrastructure.

4. General Guidelines

The following general guidelines apply to the use of all VMI information systems:

- a. Access to computer systems owned, or operated by VMI and the VMI network is granted subject to VMI rules, regulations and policies, as well as local, state, and federal laws, to include all cyber-bullying laws designed to prevent harassment and/or illegal discriminatory acts. All users must abide by these standards and applicable regulations. Violations of these policies may result in loss of access privileges as well as additional appropriate discipline. In addition, VMI considers violations of the following guidelines to be serious, and reserves the right to copy and/or examine any files or information resident on VMI systems related to any potential violation of this policy or any other VMI policy, rule, or regulation. All offenders may be prosecuted.

Cadets and all employees, using personally owned computers, tablet and smart phones to perform VMI-related work, are required to have antivirus software installed on their devices with up to date malware detection software and files.

- b. Cadets must patch their systems in accordance with directives from the IT department. Directives include but are not limited to patching systems as soon as is feasible after a software update or patch has been released. If the updates can be automatically performed, then updates must be checked for, downloaded and installed no less than monthly. This includes operating systems such as Windows, IOS and Linux, as well as application software such as Adobe products, and Microsoft Office. It also includes web browsers like Internet Explorer and Firefox.
- c. All users of VMI information systems will use only legal versions of copyrighted software and ensure that they are in compliance with any and all vendor license agreements for that software.

## 5. E-mail Guidelines

When using the VMI e-mail system:

- a. Use only the VMI e-mail system (@vmi.edu or @mail.vmi.edu) for all official VMI business email messaging.
- b. Bulk e-mails to cadets, cadet classes, faculty, employees or administrative staff must be approved in advance by an authorized approval authority. Once approved, the message must identify the source of the approval (e.g., "This message has been approved by the Dean of the Faculty"). The following officers or their designees may approve bulk e-mail messages:
  - i. Athletic Director
  - ii. Athletic Chief of Staff
  - iii. Chief of Staff
  - iv. Commandant
  - v. Deputy Superintendent-Finance, Administration & Support
  - vi. Dean of the Faculty
  - vii. Director of Communications and Marketing
  - viii. Director of Information Technology
  - ix. Inspector General
  - x. Director of the Center for Leadership and Ethics
  - xi. Cadet First Class President (can approve e-mails to the "Cadet" e-mail group)
  - xii. Cadet Honor Court President (can approve e-mails to the "Cadet" e-mail group)
  - xiii. other cadet class presidents (can only approve messages to their particular class)
- c. Minimize personal use of VMI e-mail (this includes using your VMI e-mail address as your point of contact for items published in the VMI Post Peddler).
- d. Do not give the appearance that you represent VMI when you do not.
- e. Do not make it appear that VMI endorses any individual, organization, or activity, when it does not.

- f. Do not use the VMI e-mail system or the VMI network to send SPAM, unsolicited bulk email or IM (Instant Messages), or electronic “chain letters.”
- g. Do not use mail or message services to harass or intimidate another person. In accordance with The Code of Virginia § 2.2-603.G, any instances of harassment or intimidation must be reported to the Commonwealth.
- h. Do not release personal, private, or sensitive information, which includes but is not limited to, protected personal identity information, health records and insurance information, student information, credit card or financial information, without express permission of the information owner, or VMI custodian to outside parties except with appropriate authorization and as required by law.

## 6. Network Use Guidelines

When using the VMI network and electronic resources and infrastructure:

- a. If your computer becomes infected with a virus or any malicious software, it must be immediately disconnected from the network until the infection has been removed by a member of the IT staff. If it is connected by a network cable unplug the cable, for wireless devices disable the wireless network connection.
- b. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting resources (including public computer time, disk space, and/or printer paper).
- c. Do not use any files, systems, or data that are not your own unless you have permission.
- d. Do not use server storage space (e.g., your M: drive or O: drive) to store personally-owned music, games, pictures, movies, videos, or executable files (those with a .exe file extension). This storage space is available for VMI business-related documents and coursework only.
- e. Unauthorized extending of the network (e.g., connecting a personally-owned bridge or wireless router to the network) is strictly prohibited.

## 7. User Account Security Guidelines

The following guidelines apply to user account security:

- a. Use only those computer accounts that you are authorized to use. Viewing or entering data into a system using someone else’s credentials, or taking the Security Awareness test for someone else is strictly prohibited.
- b. Protect your account credentials (username and password) from unauthorized use. Users are responsible, and may be held accountable, for all activities performed using their credentials.
- c. Do not allow any third-party organization to use your VMI account credentials.
- d. Passwords used to access the VMI network, including devices used to access that network, or resources on the network, are required by state regulation to adhere to the following minimum standards for complexity:
  - i. When technology permits, passwords must be at least eight characters in length; and

- ii. Utilize at least three of the following four:
  - 1. Special characters,
  - 2. Alphabetical characters,
  - 3. Numerical characters,
  - 4. Combination of upper- and lower-case letters.
- e. Password protected screen savers are set to activate after 15 minutes of inactivity. Disabling these screen savers or changing their settings is strictly prohibited.
- f. Never physically leave a computer on the VMI network unattended without first locking that computer.
- g. Remember: no member of the VMI Information Technology Department will ever ask for your password, nor should you allow anyone else to know it. Be aware of your surroundings and potential shoulder surfing or someone looking over your shoulder.

## 8. Removable Media Guidelines

The following safeguards protect sensitive data stored on removable media (CDs, DVDs, tapes, external hard drives, USB drives, and other removable and portable devices, such as smart phones, tablets, laptops, and notebook computers that have storage and are portable):

- a. Users should avoid storage of sensitive data on removable media whenever possible.
- b. When there is no reasonable alternative to storing sensitive data on removable media, only the minimum data necessary to accomplish the required task can be stored there.
- c. When sensitive data is stored on removable media, the cryptography must be compliant with the current Federal Information Processing Standards 140 (FIPS 140).
- d. Sensitive data stored on removable media must also be stored on a secure network file share, or as a part of the original system from which it was derived or copied (example: Colleague) for the following reasons:
  - i. This process ensures a secure backup of the data is kept.
  - ii. In the event of a privacy disclosure due to a lost or stolen removable device, a copy of the data is needed to determine to whom notification should be sent.
- e. Removable media must always be physically secured.
- f. When removable media is no longer needed, proper disposal techniques must be employed (contact IT for information on how to properly dispose of old media).
- g. If removable media that contains sensitive data is lost or stolen, the user must contact their supervisor and the Information Technology Help Desk immediately (and within 24 hours of the incident) so that necessary steps can be taken to limit damage and liability.

## 9. Data Destruction Guidelines

- a. When equipment such as computers, mobile phones, removable media, large printers, and copy machines, scanners, fax machines, multifunction devices, tablets, or other devices with storage are being disposed of or returned to their parent companies, the Information Technology Department must be notified prior to disposal so that any on-board storage can be properly erased.

## 10. Proper Use of the VMI Phone System

- a. The VMI Phone System is provided to conduct VMI business only. Personal calls are to be kept to a minimum.
- b. Any personal call on the VMI Phone System that will generate a toll should be done using a calling card so VMI is not charged for the call.

## 11. Prohibited Uses of the VMI Network

VMI employees, cadets, and all users of the VMI network and electronic infrastructure, including IT staff, will NOT:

- a. Use computer programs to decode passwords or access control information.
- b. Perform application, systems, and network assessment and vulnerability scans, including port scan, and protocol scans on the VMI network and attached devices, except with written authorization from the Information Technology Security Officer and approval from the Director of Information Technology.
- c. Engage in any activity that might be harmful to systems or information stored therein, such as disrupting services, or damaging files.
- d. Knowingly create, install, navigate to, store, execute, transmit, print, or display any content that may be, or contain malicious software, virus, trojans, backdoors, logic bombs, spyware, adware, malware, grayware, key loggers or any other software or device that may cause harm or loss to systems and information on Institute systems, or devices that access Institute infrastructure, systems, or information,
- e. Knowingly attempt to “crash” or make unavailable any system on the VMI network, with malicious intent.
- f. Use VMI systems for any commercial or business purpose, or personal monetary gain.
- g. Make, transmit, store or use illegal copies of copyrighted materials, including software, music, movies and other media on VMI systems and over VMI networks.
- h. Search for, access, or copy directories, programs, files, or data that are not your own, without authorization from the Director of Information Technology.
- i. Navigate to, store, process, transmit, print, or display obscene (as that term has been constitutionally defined <http://legal-dictionary.thefreedictionary.com/obscene>), indecent, or lewd material, or any other material that would violate any VMI and other policies, state and federal laws, See number 13 for details regarding exception process.
- j. Attempt to bypass, disable, or remove a security mechanism applied by VMI IT administrators. This includes altering or bypassing access controls, file security, administrative accounts, content filtering or other access on or with VMI-owned computers, infrastructure and user accounts.
- k. Interfere with or intrude upon communications such as e-mail, instant messages, limited-access web sites, and phone conversations of others without authorization.

- l. Tamper with VMI computer software configurations, to include networking, security controls, removing or modifying software as configured, installing personally-owned software, and installing and/or using personally-owned encryption software.
- m. Tamper with VMI computer hardware configurations, to include removing parts from a computer, installing and/or using personally-owned encryption hardware, disabling any network connections, or installing personally-owned computer hardware internally or externally.
- n. Mount a network server without permission from the Director of Information Technology.
- o. Fraudulently communicate any message sent under an assumed name or modified address, or with the intent to obscure the origin of the communication.
- p. Create, modify, execute or retransmit any computer program or instruction intended to obscure the true identity of the sender of e-mail or other electronic messages.
- q. Engage in any other activity that is potentially harmful to the VMI network, infrastructure, or the data contained therein.

12. External Guidelines

- a. In addition to the requirements set forth here, VMI employees (to include faculty, staff, and classified employees) must also adhere to the Department of Human Resource Management Policy 1.75, "Use of Internet and Electronic Communications Systems" located at <http://www.vmi.edu/workarea/showcontent.aspx?id=3661>.

13. Exception Process for Restricted Content.

- a. To request an exception, complete and submit the IT Web Content Policy Exception Agreement included at the end of this document. All applications will be kept on a secured network share.

FOR THE SUPERINTENDENT:

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

DIST: E, Cadets

OPR: IT

## IT Web Content Policy Exception Agreement

I, \_\_\_\_\_, a user of the Virginia Military Institute information  
Print Requestor Name

infrastructure request access to content indicated by marking the box in front of the choice below :

- as described in Virginia Statute Sections 2.2-2827, included below or as may be updated in the future; (The statute is included later in this document for reference.)
- that may be considered malicious.

And, I agree:

1. Only to access the content described below for the purposes stated in the justification item 4 below.
2. In the event, that I may have or suspect that, I may have become infected with malicious software, virus, et cetera, I will immediately disconnect the computer and unplug it if appropriate, from the network and notify the Help Desk and the Information Technology Security Officer and provide as much detail as possible.
3. Not to delete, clear, or remove the browser history or obfuscate or impede the investigation related to potential malware infection.
4. To provide the bona fide, agency-approved research project or other agency-approved undertaking that justifies this access in the space below. If you are currently denied access to a specific site, list it below.

---

---

---

---

---

I understand that violating any of the above provisions may cause my system and/or content access to be revoked without notice. I understand that the access will be valid for one year, at which time I must reapply.

\_\_\_\_\_  
Requestor Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
User ID, if known

\_\_\_\_\_  
Print Department Name

\_\_\_\_\_  
Authorizer Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Authorizer Name

\_\_\_\_\_  
Information Technology Security Officer  
Signature

\_\_\_\_\_  
Date

## IT Web Content Policy Exception Agreement

\_\_\_\_\_  
Superintendent, or designee Signature  
Required for access to sexually explicit content

\_\_\_\_\_  
Date

### **Description of the information requested on this form.**

This section provides a brief description of the information requested. Once the Requestor has completed the form, they must forward it to the approver for their signature and then to the Information Technology Security Officer.

Print Requestor Name - Print name of the person requesting access in the space above  
Print Requestor Name.

Item 4 - In the blank lines under item 4 print the reason access is needed. Be very specific.

Requestor Signature and Date – Signature of person requesting access and indicate the date signed.

User ID - Print the account ID or log on name access is to be granted to. The user's account used to perform the duties this access is required for.

Print Department Name - Print the name of the Department associated with the use of this content in the space above  
Print Department Name.

Authorizer Signature and Date – Institute Executive, or their designee signature indicating their approval and the date signed.

Print Authorizer Name –Print the name of the person who approves this access request and signed this form.

Information Technology Security Officer Signature – the Information Technology Officer's signature and date signed.

Please do not hesitate to contact the Information Technology Security Officer at [iso@vmi.edu](mailto:iso@vmi.edu) if you have any questions or call 540-464-7725.

## IT Web Content Policy Exception Agreement

§ 2.2-2827<sup>1</sup>. Restrictions on state employee access to information infrastructure.

A. For the purpose of this section:

"Agency" means any agency, authority, board, department, division, commission, institution, public institution of higher education, bureau, or like governmental entity of the Commonwealth, except the Department of State Police.

"Information infrastructure" means telecommunications, cable, and computer networks and includes the Internet, the World Wide Web, Usenet, bulletin board systems, on-line systems, and telephone networks.

"Sexually explicit content" means (i) any description of or (ii) any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § [18.2-390](#), sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § [18.2-390](#), coprophilia, urophilia, or fetishism.

B. Except to the extent required in conjunction with a bona fide, agency-approved research project or other agency-approved undertaking, no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content. Agency approvals shall be given in writing by agency heads, and any such approvals shall be available to the public under the provisions of the Virginia Freedom of Information Act (§ [2.2-3700](#)).

C. All agencies shall immediately furnish their current employees copies of this section's provisions, and shall furnish all new employees copies of this section concurrent with authorizing them to use agency computers.

---

<sup>1</sup> <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2827>