VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 50) 3 March 2023

Acceptable Use of VMI Information Systems

1. Purpose

The purpose of the Acceptable Use of VMI Information Systems policy is to establish user awareness regarding the standards for actions that are and are not permitted on VMI information systems and network. VMI information systems and network are designed to enhance educational research and facilitate administrative processes.

2. Scope

The scope of this policy covers the use of all VMI information systems (to include desktops, laptops, smartphones, tablets, and cloud-based applications such as Box and Canvas). The policy applies to all cadets, Institute employees, and other users of VMI information systems.

3. Expectation of Privacy

All users of VMI maintained systems, or personal systems connected to the VMI network have no expectation of privacy. This includes files residing on VMI hardware, or information moving across the VMI network. The IT Department may monitor, inspect, store, or disclose any activity, electronic communication, or record on the VMI network. Monitored activities include, but are not limited to, network traffic; application usage, data access; keystrokes; and user commands. Email, Internet usage, Box, and Canvas, message and data content may be accessed and monitored, at any time whether suspicion is, or is not, warranted.

Users are not to disable, tamper, or sabotage features, processes, and software designed to prevent, or detect fraud, policy, or legal violations. This includes, but is not limited to, logging, and monitoring software, servers, or hardware devices on VMI maintained systems.

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 is granted subject to rules, regulations, and policies, as well as local, state, and federal law. These policies include cyber-bullying laws designed to prevent harassment, illegal, or discriminatory acts. All users must abide by these standards and applicable regulations. Violations of applicable policies may result in loss of access privileges as well as further disciplinary actions. VMI considers violations of the following guidelines to be serious and reserves the right to copy and/or examine files or information residing on VMI systems related to any potential violation of this policy or other rules, or regulations. Offenders may be prosecuted.

b. Cadets and employees, using personal computers, tablets, and mobile phones to perform VMI-related work, are required to have current and updated antivirus and malware software installed.
c. Cadets must patch their systems as soon as possible after a software update has been released. For software that is automatically downloaded, cadet computers must be configured to perform an automatic download a minimum of once a month. Software with automatic update capabilities includes Windows, Mac OSX, and Linux operating systems, as well as application software such as Adobe, Microsoft Office, Internet Explorer, and Firefox.
d. All users of VMI information systems will use legal versions of copyrighted software and comply with any and all vendor license agreements.

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. Chief Diversity Officer
    xi. Director of the Center for Leadership and Ethics
    xii. Cadet First Class President (can approve e-mails to the “Cadet” e-mail group)
    xiii. Cadet Honor Court President (can approve e-mails to the “Cadet” e-mail group)
    xiv. 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 the VMI e-mail system to email sensitive information.

h. If a VMI employee has received sensitive information via email, the VMI employee should not process the request and notify the sender to use a more secure method to transfer the sensitive data.
i. Do not use e-mail or message services to harass or intimidate another person. In accordance with the Code of Virginia §18.2-152.7:1, any person, with the intent to coerce, intimidate, or harass any person, using a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or making any suggestion or proposal of an obscene nature, or threatening any illegal or immoral act, is guilty of a Class 1 misdemeanor.
j. 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.
k. The auto forwarding of email to external accounts is prohibited.

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 and powered down. Notify the IT Help Desk immediately upon powering down the computer. 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.
d. Do not store sensitive data on the M:, O:, T: or P: drives. Departments must contact IT to request encrypted network accessible file storage of sensitive data.
e. Do not use server storage space on the M: or O: drives to store music, games, pictures, movies, videos, or executable files (those with an .exe file extension). The M: and O: drives are intended for VMI business-related documents and coursework.
f. Unauthorized extending of the network (e.g., connecting a personally owned bridge or wireless router) is prohibited and strictly enforced.

7. Computer Software and Cloud Based Services

a. Users must only use software approved by Procurement Services and IT on VMI owned
b. or managed systems.
c. All VMI data must be saved to approved storage applications. Approved VMI file storage areas consist of internal network drives, Box, Canvas, and Terminal 4 content manager.
d. Any computer software installed on any system that stores/processes VMI data in the cloud must undergo an IT security review.

e. Users must use software in compliance with all vendor requirements and agreements.

8. User Account Security Guidelines

The following guidelines apply to user account security:

a. Use only your individually authorized computer accounts. Viewing or entering data into a system using the credentials of other individuals is 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 for PC's, tablets and mobile phones accessing the VMI network, and resources, are required by state regulation to adhere to the following minimum standards for complexity:
    i. Must be at least twelve characters in length;
    ii. If password has fewer than 16 characters, it must utilize all of the following:
        1. At least one special character
        2. At least one alphabetical character
        3. At least one numerical character
        4. Combination of upper- and lower-case letters
        5. Cannot contain dictionary words;
    iii. Cannot contain your username;
    iv. Cannot be the same as any of your last ten passwords;
    v. Cannot contain a sequence of 5 or more characters from a standard keyboard (ex.: "asdfg" or "gfdsa").
e. Password protected screen savers are to be set for activation after 30 minutes of inactivity. Disabling screen savers or changing the activation settings is prohibited.
f. Never physically leave a computer on the VMI network unattended without first locking it using the Ctrl-Alt-Del key combination.
g. Remember: the VMI Information Technology Department will never ask for your password. Do not disclose your password to anyone. Whenever typing your password, practice situational awareness of your surroundings and potential shoulder surfing.
h. Use of shared accounts is prohibited on IT managed / owned systems. Exception: This prohibition does not apply to non-networked or systems residing on a guest network.

9. Removable Media Guidelines

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

a. Users are prohibited from storing sensitive data on removable media.
b. When there is no reasonable alternative to storing sensitive data on removable media, only the minimum data necessary to accomplish the required task may

be stored.

c. When sensitive data is stored on removable media, the cryptography must be compliant with the current Federal Information Processing Standards 140-2 (FIPS 140-2).
d. The VMI Help Desk can provide encrypted USB flash drives for sensitive data.
e. 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 maintained.
    ii. In the event of a privacy disclosure because of a lost or stolen removable device, a copy of the data is needed to determine where notification should be sent.
f. Removable media must always be physically secured.
g. 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).
h. If removable media containing ~~s~~sensitive data is lost or stolen, the user must contact their supervisor and the Information Technology Help Desk immediately to identify the tasks required to limit damage and liability.
i. If removable media is found, turn in the device to the Information Technology Help Desk.

10. Data Destruction Guidelines

a. When equipment such as computers, mobile phones, removable media, large printers, and copy machines, scanners, faxes, multifunction equipment, tablets, or other devices with storage capabilities are in the disposal process, the Information Technology Department must be notified prior to erase on-board storage.

11. 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.

12. 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 scans of applications, systems, network assessments, vulnerabilities, ports, protocols, or services on the VMI network. Network or equipment scans require written authorization and approval from the VMI ISO and Director of Information Technology.
c. Engage in any activity that might be harmful to VMI systems or information stored therein (harmful activity is any activity which impacts the confidentiality, availability, or integrity of VMI systems or information stored therein).

d. Knowingly create, install, navigate to, store, execute, transmit, print, or display content that may be, or contain malicious software. This includes viruses, trojans, backdoors, logic bombs, spyware, adware, malware, grayware, key loggers or any other malicious software or device that may cause harm or loss to systems and information on Institute systems.
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 defined at http://legal- dictionary.thefreedictionary.com/obscene), indecent, or lewd material, or any other material that would violate VMI and other policies, state and federal laws, See number 13 for details regarding an 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 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.
r. Do not enter card holder data on devices connected to the VMI wireless network unless that device utilizes point to point encryption.

13. External Guidelines

a. In addition to the requirements set forth, 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" DHRM Policy 1.75.

b. VMI employees are required to observe the restrictions on access to web content as defined in The Code of Virginia Title 2.2 – Administration of Government Chapter 28 General Provisions § 2.2-2827.

§ 2.2-2827[1]. 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.

[1] http://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2 -2827/

14. Sensitive Data

Sensitive data must be protected from unauthorized access and unauthorized disclosure and must be encrypted, via NIST approved cryptographic methods, while at rest and during transmission. The following seven elements are defined as sensitive:

a. Social Security Number
b. Debit Card Number

c. Credit Card Number
d. Bank Account Number
e. Driver's License Number
f. Passport Number
g. Military ID

See Appendix 1: Information Security and Privacy Data Management and Usage Policy

15. Exception Process for Restricted Content.
To request an exception, to access restricted web content, complete and submit the IT Web Content Policy Exception Agreement (VMI IT FORM IT-25). Exception applications are available from the VMI ISO.

16. Formal Sanctions for Violations
Violations of this policy will be addressed in accordance with relevant VMI and Commonwealth of Virginia policies. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

FOR THE SUPERINTENDENT:

John M. Young
Lieutenant Colonel, Virginia Militia
Chief of Staff

DIST: E, Cadets

OPR: IT

Appendix 1

Information Security and Privacy Data Management and Usage Policy

Purpose

The purpose of this policy is to establish and maintain an effective security program which promotes information security and ensures the security of VMI's databases and data communications from unauthorized uses, intrusions, or other security threats and to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure VMI develops, disseminates, and updates the Information Security Program Policy. This policy and procedure establish the minimum requirements for the Information Security Program Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 1.4 Information Security Program.

Policy Statement

VMI's information technology resources are protected by a series of policies, standards, procedures, and controls. In conjunction with the Information Technology Contingency Management Plan, FERPA, and HIPAA, all security programs will be updated to ensure integration with all contingency plans. A complete list of General Orders is at http://www.vmi.edu/GeneralOrders.

Procedures

Data Sensitivity and Classification

Virginia Military Institute is strongly committed to maintaining the security and privacy of confidential personal information and other data it collects or stores. It expects all those who store such information to treat these data with the utmost care to protect the privacy and legal rights of the University community.

The ISO will meet annually with data owners to classify data being held in IT systems.

VMI establishes four data classifications: high risk data, moderate risk data, internal use data, and public data. VMI's data classifications map to ITRM Standard SEC501-11 in the following manner: High Risk data as high sensitivity; Moderate Risk and Internal Use data as moderate sensitivity; Public data as low sensitivity. High Risk / high sensitivity is treated as "sensitive" with respect to any security control enhancement for sensitive systems prescribed by SEC501. Listed in the table that follows are examples of data within each classification:

Data Classification	Data Type	Examples:
High Risk Data	***Student Records –High Risk***	*Any data that contains the following elements*:
	Financial Records –High Risk	
	Human Resources –High Risk	*Social Security Number*
	Student Financial	

	Aid Records – GLBA Confidential	*Military ID number* *Federal ID* *Credit card number* *Debit card number* *Bank account number* *Driver's license number* *Passport number* Any personal information that can lead to identity theft if exposed, e.g., Social Security numbers, passport numbers, driver's license numbers, financial account numbers
Internal Use Data	***Student Records – FERPA Confidential*** ***Financial Records –Internal Use*** ***Human Resources –Internal Use*** ***User/Computer Account – Internal Use*** ***DNS – Internal Use***	*Internal use is the classification for all data that is not explicitly defined as high-risk data and may be held from release under FOIA.* *Examples:* Colleague ID numbers FERPA-protected student information not covered by the definition of high-risk data; excluding directory information Data that may be withheld from release under the Virginia Freedom of Information Act (FOIA) Are not public records
		Moderate risk data is classified as a public record in accordance with the Virginia Freedom of Information Act (FOIA) but is not intentionally made public (see the definition of public data). For a complete list, see Code of Virginia § 2.2-3700 Virginia Freedom of Information Act.

		Moderate Risk data does not contain any High-Risk Data elements.
Moderate Risk Data	***Financial Records –Moderate Risk***	
	Human Resources – Moderate risk	*Examples:*
	Email – Moderate Risk	Salary information
	VMI End user documents – Moderate Risk	Contracts
		Personnel and financial information not covered by the definition of high-risk data, but not intended to be made public Specific email correspondence not otherwise protected by a FOIA exemption
Public Data	***Student Records – Open Access***	Public data is intentionally made available to the public Examples: Data intended for a public web site Public press release Public marketing information FERPA directory information

Data Handling Requirements

Data Classification	Data Handling Requirement
High Risk Data	In addition to or in place of requirements for Moderate Risk data: 1. Periodic vulnerability assessment of systems and / or processes used to handle the data is required. 2. Data may not be emailed in an unencrypted form. 3. Data must be stored encrypted on approved VMI owned /managed systems. 4. Data must not be stored on individual's workstation, laptop, or external hard drive.
Moderate Risk Data / Internal Use Data	1. Electronic access to data must be password protected at all times, password used to protect the data must meet VITA standards. 2. Third party and external services used to handle data must be reviewed by the VMI Information Security Office for security and privacy practices. 3. Not permitted on storage external to VMI (e.g., cloud vendors like Drop Box, Google Drive, or any other third-party hosts) unless using a VMI-contracted service.
Public Data	No explicit requirements.