

VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 50)

13 July 2010

Appropriate Use of VMI Information Systems Policy

Access to computer systems and networks owned or operated by Virginia Military Institute impose certain responsibilities and obligations on users. Access is granted subject to VMI rules, regulations and policies, as well as local, state, and federal laws. Appropriate use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and freedom from intimidation and harassment. The purposes of VMI's information systems and the VMI local area network are to enhance educational and research work and to facilitate administrative processes. All users must abide by these standards and expectations. Violations may result in loss of access privileges in addition to appropriate discipline and legal action taken against you.

In making appropriate use of resources one must:

1. Follow security Best Practices "set forth as Appendix A to this document for safeguarding access and use of VMI network/email/Colleague accounts. These safeguards are required at any computer at VMI, whether in an office, in a lab, in a Barracks room, or in a wireless mode of operation. Account holders who do not follow the security Best Practices assume responsibility, and may be held accountable, for any and all actions which originate from their accounts, even if they are unaware of the activity.
2. Use only those computer accounts or facilities that you are authorized to use.
3. Protect your user-id from unauthorized use. Users are responsible, and will be held accountable, for all activities of their user-id or system.
4. Access only files and data that are your own, that are publicly available, or to which your access has been authorized.
5. Use only legal versions of copyrighted software and in compliance with vendor license requirements.
6. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, wasting computer time, disk space, printer paper, and other related resources.
7. Bulk electronic mailings to Cadets, Cadet Classes, Faculty, Employees or AdminStaff must be approved in advance. 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 email messages:
 - a) Athletic Director
 - b) Athletic Chief of Staff
 - c) Chief of Staff
 - d) Commandant

- e) Deputy Superintendent-Finance, Administration & Support
 - f) Deputy Superintendent-Dean of the Faculty
 - g) Director of Communications and Marketing
 - h) Director of Information Technology
 - i) Inspector General
 - j) Director of the Center for Leadership and Ethics
 - k) In addition to this list class Presidents may approve email messages for "class business" (i.e. Ring Figure, class meetings, etc.) for their class only. The First Class President and the Honor Court President may send email messages to the "Cadet" email group.
8. Minimize use of VMI email for personal use including contact information in Post Peddler. One should obtain a commercial email account for this purpose. Gmail, Yahoo, hotmail, and other sources are available for free email accounts. However, all email traffic on the VMI network, regardless of to what account it is directed, is subject to review and inspection by the Institute at any time and for any legitimate purpose.
9. Use only the VMI email system (@vmi.edu or @mail.vmi.edu) for all official VMI business email messaging.

In making appropriate use of resources one must NOT:

- 1. Use a user-id or Colleague number other than your own.
- 2. Use server directory storage space (drives M, O, P, T, etc) to store personal music, games, pictures, movies, videos, or any type of executables (.exe). This storage space is available for VMI business and course work only. This personal data should be stored on the user's C: drive and the user is responsible for backing up this personal data.
- 3. Use any files, systems or data, not your own, without permission.
- 4. Use computer programs to decode passwords or access control information.
- 5. Port scan and/or protocol scan (see appendix B).
- 6. Attempt to circumvent or subvert system security measures including any restrictions associated with your account.
- 7. Engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- 8. Willfully install spyware, adware, malware, gray ware, or key loggers on any system on the VMI network.
- 9. Attempt to modify system facilities or attempt to crash any system.
- 10. Use VMI systems for any commercial or business purpose or for personal monetary gain.
- 11. Make, transmit, store or use illegal copies of copyrighted materials, including software, music, movies and other media on VMI systems or over VMI networks.
- 12. Search for, access, or copy directories, programs, files, or data not your own, without authorization.
- 13. Bypass, disable, or remove a security mechanism applied by VMI system or network administrators. This includes altering file security, administrative accounts or access on VMI owned systems.

14. Give the appearance that you represent VMI when you do not.
15. Make it appear that VMI endorses any individual, organization, or activity, when it does not.
16. Use someone else's account credentials to complete a task. For example, taking the Security Awareness test for someone else; viewing or entering data into a system under someone else's login ID.
17. Allow any third party or organization to use your accounts, network ID, or passwords
18. Interfere with or intrude upon communications such as email, IM (Instant Messages), limited-access web sites, and phone conversations of others.
19. Use mail or messaging services to harass or intimidate another person.
20. Circulate or forward electronic "chain" letters (see appendix B). Create, modify, execute or retransmit any computer program or instruction intended to obscure the true identity of the sender of electronic mail or electronic messages, collectively referred to as "Messages," including, but not limited to, forgery of Messages and/or alteration of system and/or user data used to identify the sender of Messages.
21. Use the VMI communication systems to send SPAM or unsolicited bulk email or IM (Instant Messages) (see appendix B). Transmit, print or display obscene, indecent, lewd or lascivious material.
22. Tamper with VMI computer hardware and software configurations to include networking, security controls, removing parts from a computer, removing or modifying software as configured, installing personally owned software, installing and or using proprietary encryption hardware or software, extending the physical network connections beyond the installed level, disabling a network connection, or installing personally owned computer hardware externally or internally to a VMI system.
23. Mount a network server without permission from the Director of Information Technology.
24. Engage in any use of the VMI system that does not comply with these guidelines presented herein.
25. Cadets, and any employee using a personal computer to perform VMI related work, are required to install Antivirus software from the Information Technology web page <http://www.vmi.edu/antivirus> configure it so that, and verify that, the virus definition updates are scheduled daily.
26. All users are required to apply software patches as required by the Information Technology department. Note, VMI owned faculty, staff, and lab computers are patched by the IT department.
27. Users must not allow an infected computer to be connected to the network until the infection is removed.
28. Cadet computers are required to have the same name as their network login name, preceded by their class year (Example: 2008D0eJH).

No Expectation of Privacy

Users have no expectation of privacy in any files or information residing on VMI hardware or moving across VMI's network or in any activity that takes place on any VMI information system. VMI may monitor, inspect, store, or disclose any electronic communication or record on or transversing its network or systems for any legitimate purpose whenever it is deemed necessary. Virginia Military Institute considers violation of the foregoing guidelines to be serious, and reserves the right to copy and examine any files or information resident on VMI systems allegedly related to this or any other VMI policy, rule or regulation. Offenders also may possibly be prosecuted under laws including (but not limited to), The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, The Virginia Computer Crimes Act, and the Electronic Communications Privacy Act. Access to the text of these laws is available through the Reference Department of Preston Library.

Social Networking

Social networking sites such as Facebook and MySpace have become a tool for staying connected to friends and family and communicating and networking among people with similar interests.

Information posted online, including pictures and text, may become very difficult to completely remove from the internet even after deleting the material. Material may become the property of these sites once they are posted. Potential employers and graduate school admissions perform background checks by searching these sites.

The information you post can be used by others to steal your identity, for stalking, or other criminal activity putting your physical safety in danger. Be cautious of posting personal information. Your full name, address, birthday, pictures, hometown or even plans for the day can all be used to your disadvantage.

State and federal law also apply in using these social networking sites. Copyright infringement, defamation, invasion of privacy, obscenity, pornography, sexually explicit materials, sexual harassment, and stalking are common legal concerns. Users violating these laws may be subject to civil and criminal fines or imprisonment.

Digital Copyright Compliance

Downloading, copying and sharing material, such as music, movies, games, and applications, for which the copyright holder has not given you rights is both against the law and VMI policy. Read the VMI Digital Copyright Compliance Policy (www.vmi.edu/DCCP).

GENERAL ORDER NUMBER 50, 13 July 2010, Page Five

Department of Human Resource Management Policy 1.75

Non cadets must adhere to the Department of Human Resource Management Policy 1.75, "Use of Internet and Electronic Communications Systems" found on the VMI web at <http://www.vmi.edu/workarea/showcontent.aspx?id=3661>.

FOR THE SUPERINTENDENT:

Jeffrey H. Curtis
Colonel, USAF (Ret.)
Chief of Staff

DIST: E, Cadets

OPR: IT

Appendix A: Security Best Practices

1. Users should never:
 - a. Disclose their password to anyone or ask another to disclose their password.
 - b. Leave a public or lab computer on which they are logged on unattended.
 - c. Release personal information about others to outside parties except under the special circumstances described in VMI policies.
 - d. Use mail or message services to harass or intimidate another person. In accordance with [The Code of Virginia § 2.2-603.G](#) this violation must be reported to the state.
2. Users who wish to leave their computer unattended must either log off or lock the computer.
3. Password protected screen savers should be used at all times. Screen savers should activate after no more than 20 minutes of inactivity.
4. Use complex passwords (see appendix B).
5. The following safeguards should be observed to protected sensitive data (see appendix B) stored on removable media (see appendix B):
 - 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, it must be the minimum data necessary to accomplish the required task.
 - c. Sensitive data stored on removable media must be protected by VMI approved encryption methods (see appendix B).
 - 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).
 - i. Storing Sensitive data on a file share or the original system ensures secure backup of the data.
 - ii. In the event of a privacy disclosure (see appendix B), 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.
 - g. If removable media is lost or stolen, the user must contact their supervisor and the Information Technology Help Desk immediately so that necessary steps can be taken to limit damage and liability of an inappropriate disclosure.
6. When depositing of equipment or when returning leased equipment to include but not limited to computers, mobile phones, removable media, large printers, and copy machines, the device must be checked by the Information Technology department for any memory storage capability. If memory is found, the memory will be either erased or encrypted.
7. Land line telephones are provided to conduct VMI business. Personal calls are to be kept to a minimum. Any personal call generating a toll should be done using a personal calling card so as not to have VMI charged for the call.

Appendix B: Definitions

A privacy disclosure: Sensitive data that has been released to individuals, groups, or organizations, that could become available to unauthorized users.

Bulk electronic mailings: Includes any unsolicited electronic communication including email, IM (Instant Messages), and calendar solicitations for meetings that is sent to 20 or more users. Mass electronic messaging is an unsolicited communication.

Chain letters: A letter sent to a number of people asking each recipient to send copies with the same request to a specified number of others. The circulation of a chain letter increases in geometrical progression as long as the instructions are followed by all recipients.

Encryption: The reversible transformation of data from the original to a difficult-to-interpret format as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity.

SPAM or Unsolicited Bulk Email: A message is SPAM only if it is both unsolicited AND bulk. Unsolicited email is normal email--examples: first contact enquiries, sales enquiries. Bulk email is normal email--examples: subscriber newsletters, customer communications, discussion lists. An electronic message is "SPAM" if the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients AND the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent.

Port: A port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, Hypertext Transfer Protocol, have ports with pre-assigned numbers. These are known as "well-known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA).

Port scan and/or protocol scan: A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides.

Removable media: CDs, DVDs, magnetic tapes, floppy disks, external hard drives, universal serial bus (USB) drives (also known as memory sticks, jump drives and thumb drives) and any other storage media intended for data portability separate from the system on which it originated.

Sensitive data: Data with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, security-related data such as passwords, data containing personal information such as medical records, social security numbers, or other data which if available to unauthorized users, may harm an individual, group, or the Institute.

Complex passwords: A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A complex password consists of at least eight characters that are a combination of upper and lower case letters and numbers. Complex passwords also cannot contain words that can be found in any dictionary or parts of the user's own name.

VMI approved encryption methods: The method of data encryption approved as acceptable by the Information Technology Department. The methodology and approved storage devices will change from time to time as technology advances are made in this area.