

September 12, 2002

FROM: John Nickerson, Acting Director of Finance and Administration
Military Department, State of Maryland

TO: All personnel Utilizing State Internet and email Services

SUBJECT: Information Technology Policy Letter #1 for email and Internet Usage

E-mail Security and Usage

Purpose

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers and to promote the appropriate use of e-mail, in supporting State business

Scope

This policy applies to Military Department employees and covers e-mail located on the department's personal computers and servers if these systems are under the jurisdiction and/or ownership of the Military Department. The policy applies to stand-alone personal computers with dial-up modems as well as those attached to networks. Authority for this policy may be referenced in the Annotated Code of Maryland, State Finance and Procurement Article, Sections 3-401 to 3-413 a copy of which is on file in the Information Technology Section.

Responsibilities

As defined below, the Military Department's IT Section is responsible for electronic mail security has been designated as such in order to establish a clear line of authority and responsibility.

1. Information Technology must establish e-mail security policies and standards and provide technical guidance on e-mail security to all Military Department staff.
2. IT staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Monitoring will involve industry software designed to monitor and filter objectionable e-mail content. Program directors must ensure that their staffs are in compliance with the personal computer security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to e-mail security.

3. The Military Department's program directors must ensure that: Employees under their supervision implement e-mail security measures as defined in this document.

Contact point

Questions about this policy may be directed to the IT Manager

Disciplinary process

Violation of these policies may subject employees to disciplinary procedures up to and including termination.

Specific policy

State property. As a productivity enhancement tool, the Military Department encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the State of Maryland, and are not the property of users of the electronic communications services.

Authorized usage. The Military Department's electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

1. It does not consume more than a trivial amount of resources.
2. It does not interfere with staff productivity.
3. It does not preempt any business activity.
4. It does not contain verbiage or pictures that are morally offensive, objectionable or obscene in nature.
5. IT does not create or promote actions involving fraud or defamation.

Users are forbidden from using state electronic communications systems for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the Information Technician Department. Employees are reminded that the use of state resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Default privileges. Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software.

User separation. These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user Ids and associated passwords to isolate the communications of different users. But fax machines that do not have separate mailboxes for different recipients need not support such user separation. All Military Department staff have unique usernames and passwords to access the e-mail system.

User accountability. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess.

No default protection. Employees are reminded that the Military Department electronic communications systems are not encrypted by default.

Respecting privacy rights. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. The Military Department's network is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, the Military Department also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

No guaranteed message privacy. The Military Department's network cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

Regular message monitoring. It is the policy of the Military Department to require IT personnel to periodically monitor the content of electronic communications. The content of electronic communications and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, proper usage, and investigative activities. Users should structure their electronic communications in recognition of the fact that the IT personnel will from time to time examine the content of electronic communications.

Statistical data. Consistent with generally accepted business practice, the Military Department's IT Section collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, Information Technology (IT) staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

Incidental disclosure. It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (Director of Finance and Administration, IT Manager etc.).

Message forwarding. Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Military Department sensitive information must not be forwarded to any outside party without the prior approval of the IT Section. Blanket forwarding of messages to parties outside the Military Department is prohibited unless the prior permission of the IT Manager has been obtained.

Purging electronic messages. Messages that are no longer needed for business purposes must be periodically purged by users and removed from their personal electronic message storage areas. After a certain period—generally three months—electronic messages should be backed up to a separate data storage media (tape, disk, CD-ROM, etc.) and deleted from personal computers

Not only will this increase scarce storage space; it will also simplify record management and related activities.

Internet Security and Usage Policy

Purpose

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection and usage of state information and equipment by Internet and intranet connections and to promote the appropriate use of Intranet and the Internet in supporting State business. Authority for this policy may be referenced in the Annotated Code of Maryland, State Finance and Procurement Article, Sections 3-401 to 3-413 a copy of which is on file in the Information Technology Section.

Scope

This policy applies to all employees, contract, consultants, temporaries, and other users at the Military Department, including those users affiliated with third parties who access the Military Department's computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by the state of Maryland.

Responsibilities

As defined below, IT staff members responsible for Internet security and usage have been designated in order to establish a clear line of authority and responsibility.

- a) Information Technology must establish Internet security and usage policies as well as standards and provide technical guidance on PC security and usage to all staff. The IT department must also organize a computer emergency response team (CERT) to respond to virus infestations, hacker intrusions, and similar events.
- b) IT staff must monitor compliance with Internet security and usage requirements, including hardware, software, and data safeguards. Monitoring will involve industry software designed to monitor and filter objectionable Internet access. Program directors must ensure that their staffs are in compliance with the Internet security and usage policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to Internet security and usage.

- c) IT staff must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
- d) IT staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- e) IT staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.
- f) Military Department program directors must ensure that:
 - 1) Employees under their supervision implement security measures as defined in this document.
 - 2) Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
 - 3) Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all Military Department documents that address information security.
 - 4) Employees and contract personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
 - 5) Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.
- g) Users of Military Department Network Internet connections must:
 - 1) Know and apply the appropriate Military Department policies and practices pertaining to Internet security.
 - 2) Not permit any unauthorized individual to obtain access to the Department's Internet connections.
 - 3) Not use or permit the use of any unauthorized device in connection with the Department's personal computers.
 - 4) Not use Department Internet resources (software/hardware or data) for other than authorized company purposes.
 - 5) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
 - 6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
 - 7) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
 - 8) Report to the It Manager or IT staff any incident that appears to compromise the security of the Department's information resources. These include missing data, virus infestations, and unexplained transactions.
 - 9) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
 - 10) Obtain supervisor authorization for any uploading or downloading of information to or from the Department's multi-user information systems if this activity is outside the scope of normal business activities.
 - 11) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their program director.

Contact point

Questions about this policy may be directed to the IT Manager.

Disciplinary process

Violation of these policies may subject employees to disciplinary procedures up to and including termination.

Specific policy

All information traveling over the Military Department computer networks that has not been specifically identified as the property of other parties will be treated as though it is a state asset. It is the policy of the Military Department to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of Military Department to protect information belonging to third parties that has been entrusted to the Department in confidence as well as in accordance with applicable contracts, state and industry standards.

Introduction

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes the Military Department's official policy regarding Internet security. It applies to all individuals who use the Internet with Military Department computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with the Military Department.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the Information Technology Manager. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

Information movement

All software downloaded from non-state government sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with state information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal state information (see the following section).

Users must not place Military Department material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the IT Section has first approved the posting of these materials.

In more general terms, Military Department internal information should not be placed in any location, on machines connected to the Department's internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writeable (common/public) directories on the Military Department's Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with the Department's business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

Information protection

Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, Military Department secret, proprietary, or private information must not be sent over the Internet.

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services should be used with caution over the Internet when in readable form. Currently the Military Department does not use any type of encryption.

Exchanges of software and/or data between the Military Department and any third party may not proceed unless a written agreement has first been signed and approval obtained from the IT Section. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

The Military Department strongly supports strict adherence to software vendors' license agreements. When at work, or when department computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Military Department work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

Expectation of privacy

Personnel using Military Department information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.

At any time and without prior notice, the Information Technology Section reserves the right to examine e-mail, personal file directories, and other information stored on state computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Military Department information systems.

Resource usage

Information Technology management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should normally be done on personal, not company, time. Likewise, games, news groups, and other non-business activities must be performed on personal, not company, time.

Use of state computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is preempted by the personal use. Extended use of these resources requires prior written approval by the IT Manager.

Public representations

Staff will not be involved in bulletin board discussions, chat sessions, and other offerings on the Internet unless specifically authorized by the state of Maryland.

Staff must not publicly disclose internal Military Department information via the Internet that may adversely affect the Department's public image

Reporting security problems

If sensitive Military Department information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IT Manager must be notified immediately.

If any unauthorized use of Military Department information systems has taken place, or is suspected of taking place, the IT Manager must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the IT Manager must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Signature

By signing below, I agree to the following terms:

- (i) I have received and read a copy of the Military Department's Information Technology Policy Letter #1 for email and Internet usage and understand and agree to same.
- (ii) I understand and agree that if I leave the military Department's employment for any reason, I shall immediately notify the Information Technology Section to be removed from Internet and email facilities.

Employee Signature _____

Employee Name _____

Employee Title _____

Date _____

Department/Location _____

Please sign and return immediately to the Information Technology Department.