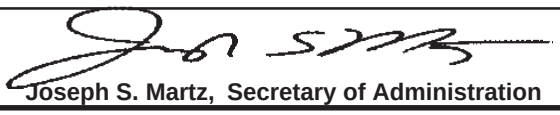
MANAGEMENT DIRECTIVE

205.34
Amended
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

Commonwealth of Pennsylvania Information Technology Acceptable Use Policy

By Direction Of:	Date:
 **Joseph S. Martz, Secretary of Administration**	**March 28, 2007**

This directive establishes policy for the acceptable use of Commonwealth information technology (IT) resources, including of the Internet and electronic mail (E-mail) by Commonwealth workforce members, including employees, contractors, consultants, volunteers and other authorized users (hereinafter referred to as Authorized Users). Marginal dots have been excluded due to major changes.

1. PURPOSE. This policy is established to provide Authorized Users with guidelines for, restrictions upon and standards for acceptable use of Commonwealth IT resources. All Authorized Users must be familiar with this policy and adhere to it.

2. BACKGROUND. The Commonwealth of Pennsylvania has established a complex enterprise network of IT resources that connects agency networks with the Internet and other business partner networks for the purpose of sharing and accessing information in accordance with the mission of the Commonwealth. Commonwealth workforce members, including employees, contractors, consultants, volunteers and other Authorized Users, are expected to use this network and its connected IT resources in accordance with authorized job functions and in accordance with the acceptable use guidelines documented in this directive.

It is the policy of the Commonwealth to ensure that all Authorized Users that have access to Commonwealth IT resources are made aware of and comply with the standards set forth in this directive and in Enclosures 1 and 2. These standards encourage effective use of IT resources and provide a framework to prevent misuse or illegal use of these resources. This directive does not prohibit employees from performing authorized job duties.

3. SCOPE. This directive applies to all Authorized Users in all agencies under the Governor's jurisdiction who have access to Commonwealth IT resources.

4. POLICY.

a. These standards are designed to prevent use that may be illegal, abusive, or which may have an adverse impact on the Commonwealth or its IT resources and to identify permissible and effective uses. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer.

b. The improper use of Commonwealth IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Commonwealth IT resources by contractors or consultants may result in disciplinary action that may include formal action under the terms of the applicable contract or debarment under the Contractor Responsibility program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Commonwealth IT resources.

c. Authorized Users of Commonwealth IT resources should be aware that all records of computer use, Internet use and/or E-mail communication (sent, received, or stored) conducted on Commonwealth IT resources are the property of the Commonwealth. Individual Authorized Users do not control access to such records. At its discretion, executive level or Human Resources staff or their authorized designees may access and review any computer files or data, Internet records or E-mail communications for compliance with the provisions of this directive. Agency heads may determine who may access these records, including, but not limited to, executive level staff, legal staff, human resource management staff, network system administrators, individuals in the Authorized User's chain of command or others, including law enforcement. Files and records of IT resource use may be reviewed at any time and are routinely backed up and stored without the user's knowledge. All physical equipment, intellectual property, information, software, data, files or programs that are provided, stored or otherwise utilized by or on any Commonwealth-provided IT resource is the property of the Commonwealth.

d. All Authorized Users should understand that all electronic communication and access may be traced and/or monitored. Agencies and their designees may use tracking, blocking, and monitoring software to restrict certain access and/or alert information technology staff to certain inappropriate uses. Authorized Users must use passwords and/or encryption in a manner that is consistent with Commonwealth and agency policy. Utilization of special passwords or encryption does not necessarily guarantee the confidentiality of any electronic communication. Authorized Users must keep passwords secure and must not share them with others.

e. The Internet and E-mail are information tools that the Commonwealth has made available on Commonwealth computer resources for Commonwealth business purposes. Where personal use of these resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the Commonwealth, reasonable use of the Internet and/or E-mail for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental. Any personal use which is inconsistent with Commonwealth policy regarding availability or capability of computer equipment, or inappropriate content of communications as defined by this policy, is prohibited.

f. All existing employees must be provided a copy of this policy. All new employees must review this policy during new employee orientation. All non-employee Authorized Users must review this policy prior to their use of Commonwealth IT resources.

g. As acknowledgement of receipt and understanding of this policy, agencies must obtain a signed user agreement in the form of Enclosure 2 from each Authorized User who has been granted access to Commonwealth IT resources. Agencies must obtain a signed user agreement from each new employee prior to granting such employee access to Commonwealth IT resources. Agencies may continue to use existing user agreements for ninety (90) days after the issue date of this Directive, but thereafter agencies may only grant access to Commonwealth IT Resources to Authorized Users who had signed a user agreement in the form of Enclosure 2, unless a waiver of this requirement has been granted by the Office of Administration.

h. Each agency must maintain copies of the agreement signed by each user authorized by the agency. Completed user agreements shall be maintained as part of the employee's Official Personnel Folder. Alternately, users may sign and agencies may store these agreements in an electronic format consistent with *Management Directive 210.12, Electronic Commerce Initiatives and Security, and ITB—SEC006, Commonwealth of Pennsylvania Electronic Signature Policy*. Signed agreements must be accessible to individuals who are authorized to view or use the documents.

i. Technical standards for use of the Commonwealth IT resources will be published in Office of Administration/Office for Information Technology (OA/OIT) "IT Bulletins" that will be available on the OA/OIT Internet site at <http://www.oit.state.pa.us>.

j. Requests for records pertaining to Commonwealth IT resources must be addressed consistent with all laws, directives or policies that would apply to the same information if maintained in a non-electronic format. These requests should be referred to agency legal counsel.

k. This policy supplements and where conflicting, supersedes *Management Directive 205.29, Commonwealth Internet Access.*

l. This policy supersedes any existing IT, Internet and/or E-mail use policy issued by agencies under the Governor's jurisdiction that is inconsistent with this directive, unless specific exemptions are granted by the Secretary of Administration or designee. Approved labor agreements or "side letters" should be read in a manner to effectuate both this policy and any such agreement or letter. In cases where a provision of an approved labor agreement or "side letter" cannot be reconciled with this policy, the labor agreement or side letter will control. Agencies may develop supplemental IT, Internet and/or E-mail policies only with the approval of the Secretary of Administration or designee. Agencies must ensure that Authorized Users with access to Commonwealth IT resources have access to this directive and Enclosures 1 and either Enclosure 2 or Enclosure 3, as appropriate, either electronically or in hard copy. All use of Commonwealth IT resources must conform with Executive Order 1980-18, Code of Conduct, Management Directive 505.7, Personnel Rules, and Commonwealth policies on nondiscrimination and sexual harassment.

ENCLOSURES

1 – Commonwealth Acceptable Use Standards for Information Technology (IT) Resources

2 – Commonwealth Acceptable Use Policy Agreement Commonwealth Employee or Volunteer Form

3 – Commonwealth Acceptable Use Policy Agreement Commonwealth Contractor or Consultant Form

This directive supersedes *Management Directive 205.34*, dated September 12, 2000.

Enclosure 1

COMMONWEALTH ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESOURCES

Each Authorized User must comply with these standards when using the Internet or Commonwealth IT resources.

AUDITING AND REPORTING

The Commonwealth reserves the right to monitor and/or log, with or without notice, all Internet activity, all Internet web site access, all E-Mail and any other communications or data accessed, stored or otherwise used by or on Commonwealth IT resources. Therefore, Authorized Users should have no expectation of privacy in the use of the Commonwealth's IT resources. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer. All physical equipment, intellectual property, information, software, data, files or programs that are provided, stored or otherwise utilized by or on any Commonwealth IT resource is the property of the Commonwealth.

DISCIPLINE

Misuse of Commonwealth IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Commonwealth IT resources by contractors or consultants may result in disciplinary action that may include formal action under the terms of the applicable contract or debarment under the Contractor Responsibility program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Commonwealth IT resources.

GENERAL IT RESOURCE USE

a. As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on Commonwealth systems for which they do not have authorization or explicit consent.

b. Authorized Users may not share their Commonwealth or agency account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes with any other person or Authorized User. Authorized Users are strictly responsible for maintaining the confidentiality of their Commonwealth or agency account(s), passwords, PIN, Security Tokens or similar information or device.

c. Authorized Users may not make unauthorized copies of copyrighted software.

d. Authorized Users may not use non-standard shareware or freeware software without agency IT management approval unless it is on the agency's standard software list.

e. Authorized Users may not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT resource; obtain extra IT Resources beyond those allocated; or circumvent computer security measures.

f. Authorized Users may not use Commonwealth IT resources for personal gain.

g. Authorized Users may not engage in illegal activity in connection with their use of Commonwealth IT Resources, including, but not limited to downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners or any other non-approved programs on Commonwealth IT resources unless they are specifically authorized to do so.

h. Authorized Users may not intentionally access, create, store or transmit material that is generally considered to be inappropriate or personally offensive, including sexually suggestive, pornographic or obscene material.

i. Authorized Users may not utilize unauthorized proprietary and/or commercial Instant Messaging (IM) products on Commonwealth computer resources. Refer to *Management Directive 210.15 – Instant Messaging.*

j. Authorized Users are personally responsible for the security of authorized portable Commonwealth IT resources such as issued laptops, Blackberries and cell phones. Care must be exercised to ensure these devices are not lost, stolen or otherwise accessed in an unauthorized manner.

k. Authorized Users may not store non-public information on IT resources, if those IT resources will be removed from Commonwealth facilities without prior approval from the agency Secretary or designee.

l. Authorized Users may only use encryption methods approved by the Commonwealth to encrypt information.

m. Authorized Users may not use non-Commonwealth or non-approved storage devices or storage facilities without the approval of the agency Secretary or designee.

INTERNET USE

All security policies of the Commonwealth and its agencies, as well as policies of Internet sites being accessed, must be strictly adhered to by Authorized Users.

Software

In connection with Authorized Users' use of and access to Commonwealth IT Resourses:

a. All software used to access the Internet must be part of the agency's standard software suite or approved by the agency IT department. This software must incorporate all vendor provided security patches.

b. All files downloaded from the Internet must be scanned for viruses using the approved Commonwealth distributed software suite and current virus detection software.

c. All software used to access the Internet shall be configured to use an instance of the Commonwealth's standard Internet Access Control & Content Filtering solution.

Expectation of Privacy

a. Authorized Users may not rely on any communications via the Internet using Commonwealth IT Resources being secure, private, or inaccessible, except where appropriate security applications are used, e.g. data encryption.

b. All activity on Commonwealth IT resources is subject to logging and review.

Access Control and Authorization

Agencies should authorize access to the Internet using Commonwealth computer resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access and all possible precautions should be taken to protect passwords. Authorized Users are responsible for activity and communications transmitted under their account.

Incidental Use

a. Use of Commonwealth IT resources is only authorized for personal use on a limited, occasional, and incidental basis and in a manner consistent with this policy.

b. Incidental personal use of Internet access is restricted to Authorized Users; it does not extend to family members or other acquaintances.

c. Access to the Internet from an agency owned, home based computer must adhere to all the same policies that apply to use from within agency facilities. Employees may not allow family members or other non-employees to access agency computer systems.

d. Incidental use must not result in direct costs to the Commonwealth.

e. Incidental use must not interfere with the normal performance of an Authorized User's work duties.

f. No user may send or solicit files, documents or data that may risk legal liability for, or embarrassment to, the Commonwealth.

g. All files and documents located on Commonwealth IT resources, including personal files and documents, are owned by the Commonwealth and may be accessed in accordance with this policy. In addition, it should be understood that such documents may be subject to the Right to Know Law 65 P.S. § 66.1, *et seq.* and other laws that may require the Commonwealth to disclose the content of its IT resources.

Acceptable Use of the Internet

Accepted and encouraged use of the Internet for Authorized Users on Commonwealth IT Resources includes, but is not limited to, the following:

1. Access, research, exchange, or posting of information that relates to the assigned job duties of an Authorized User for carrying out Commonwealth business.

2. Promotion of public awareness in regard to Commonwealth law, agency services, and public policies.

3. Posting of agency information that has been authorized by appropriate management.

E-MAIL USE

Expectation of Privacy

a. When sensitive material is sent electronically via E-mail, it is important to verify that all recipients are authorized to receive such information and to understand that E-mail is not fully secure and/or private, except where appropriate security applications are used, e.g. data encryption.

b. Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.

c. Where it is necessary to transmit Commonwealth proprietary or restricted information beyond the Commonwealth Connect E-mail network, the messages should be protected by encryption. Authorized Users should contact their agency network coordinator or Information Technology Coordinator for assistance if encryption is needed.

d. E-mail messages to be transmitted outside of the United States should comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users should contact their network coordinator or Information Technology Coordinator, who may receive technical assistance from the Office of Administration, Office for Information Technology.

e. The agency head or designee should determine specific agency policy regarding business information which is determined to be too confidential or sensitive to be transmitted via E-mail.

f. All user activity on Commonwealth IT resources is subject to logging and review.

Access Control and Authorization

a. Only Authorized Users may use Commonwealth IT resources to send or view E-mail or access the Commonwealth's E-mail systems.

b. Unauthorized persons may not use the network or Commonwealth equipment to originate E-mail messages or read E-mail messages directed to others.

c. Access Commonwealth E-mail will only be granted to Commonwealth workforce members, including employees, contractors, consultants, volunteers and other authorized users if they agree to abide by all applicable rules of the system, including this policy and its related standards.

d. Unauthorized access of an Authorized User's E-mail files is a breach of security and ethics and is prohibited. An Authorized User may not access the E-mail or account of another Authorized User unless granted permission to do so by the Authorized User. This restriction does not apply to system administrators and management staff in the Authorized User's chain of command who are authorized to access E-mail for legitimate business purposes.

e. In accordance with agency policy, Authorized Users should use password protection to limit access to E-mail files. Authorized Users must safeguard their passwords so that unauthorized users do not have access to their E-mail. Authorized Users are responsible for messages transmitted under their account.

Message Retention

E-mail messages may be subject to Commonwealth and/or agency document retention standards. See *Management Directive 210.5 Records Management* for additional guidelines.

E-mail Security Issues – Worms & Viruses

E-mail and attachments to E-mail increasingly are reported to be sources of computer viruses. All Authorized Users should act in accordance with the latest Information Technology Bulletins regarding containment methods for computer viruses.

Maintaining Professionalism.

Every Authorized User who uses Commonwealth computer resources is responsible for ensuring posted messages are professional and businesslike. As a way to impose personal restraint and professionalism, all employees should assume that whatever they write may at some time be made public. Authorized Users should follow the following guidelines:

1. Be courteous and remember that you are representing the Commonwealth with each E-mail message sent.

2. Review each E-mail message before it is sent and make certain that addresses are correct and appropriate.

3. Consider that each E-mail message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipient of the message.

4. Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration, and speculation which could be misconstrued.

5. Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of E-mail can easily identify different E-mail messages. Avoid subject fields that are vague and general, e.g. "question," "comment," etc.

Electronic Message Distribution, Size and Technical Standards

a. Authorized Users should receive authorization from their chain supervisor before wide scale "broadcasting" an E-mail bulletin to groups of employees.

b. The use of "reply to all" should be avoided unless it is appropriate to respond to all addressees.

c. Authorized Users wishing to send E-mail bulletins to all Commonwealth or agency employees must first obtain authorization from agency management.

d. E-mail messages should be brief, and attachments to E-mail messages should not be overly large. Agency IT staff will inform Authorized Users of limitations on the size of E-mail messages and attachments. The Office for Information Technology periodically will provide technical standards and guidance to agencies through IT Bulletins on the technical capacities of the Commonwealth Connect system and limitations on E-mail message size. Technical standards will be provided in areas such as file size and backup procedures, and will be available on the OA/OIT Internet site at **<http://www.oit.state.pa.us>.**

UNACCEPTABLE USES OF IT RESOURCES

The following are examples of impermissible uses of Commonwealth IT resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:

1. Viewing, accessing, posting or transmitting any material that is generally considered to be personally offensive or inappropriate, including sexually suggestive, pornographic, or obscene materials.

2. Viewing, accessing, posting or transmitting material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups including, but not limited to, protected groups identified in *Executive Order 1996-9, Equal Employment Opportunity.*

3. Conducting personal, for-profit transactions or business or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the Commonwealth.

4. Participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as auctions, games, accessing pornographic or offensive material, or any other activity that is prohibited by directive, policy or law.

5. Attempting to test or bypass the security ("hacking" or "cracking") of computing resources or to alter internal or external computer security systems.

6. Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms or other forms of malware, i.e. malicious software.

7. Promoting, soliciting or participating in any activities that are prohibited by local, state, or federal law or the Commonwealth rules of conduct.

8. Violating or infringing the rights of any other person.

9. Using any other Authorized User's password and/or equipment to conduct unacceptable activities on Commonwealth IT Resources.

10. Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.

11. Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio or video files, as well as trademarks or service marks without the owner's permission.

12. Promoting or participating in any unethical behavior or activities that would bring discredit on the Commonwealth or its agencies.

13. Downloading and/or installing any unapproved software.

14. Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender, or alter a sender's message.

15. Sending or forwarding confidential or sensitive Commonwealth information through non-Commonwealth email accounts. Examples of non-Commonwealth email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers.

16. Sending, forwarding or storing confidential or sensitive Commonwealth information utilizing non-Commonwealth accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.

17. Participating in any other Internet or E-mail use that is deemed inappropriate by the Commonwealth and/or its agencies and is communicated as such to Authorized Users.

Enclosure 2

COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT – COMMONWEALTH EMPLOYEE OR VOLUNTEER

This user agreement does not prohibit employees from performing authorized job duties.

I have read the attached Management Directive _____, "*Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*" and in consideration of the Commonwealth of Pennsylvania making its IT Resources available to me, I agree to abide by the requirements set forth therein. I understand that disciplinary action, up to and including termination, may be taken if I fail to abide by any of the requirements of this agreement. I further understand that my Commonwealth IT resource usage may be monitored at any time and by signing this Agreement, I specifically acknowledge such monitoring. I further understand that if I have any questions regarding this Directive, I am required to ask for clarification from my supervisor or my agency Human Resource representative.

Printed Name: _____

Employee Number: _____

Signature: _____

Date: _____

Agency: _____

Bureau/Facility: _____

Division/Section: _____

Mailing/E-mail Address: _____

Work Phone: _____

Optional Agency Approval: _____

Date: _____

Enclosure 3

COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT – COMMONWEALTH CONTRACTOR OR CONSULTANT

This user agreement does not prohibit contractors or consultants from performing services required by their contract with the Commonwealth.

I have read the attached Management Directive _____, "*Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*" and in consideration of the Commonwealth of Pennsylvania making its IT Resources available to me, I agree to abide by the requirements set forth therein. I understand that the Commonwealth may take appropriate action, including any action specified in my contract with the Commonwealth, as well as under the Commonwealth's Contractor Responsibility Program, if I fail to abide by any of the requirements of this agreement. I further understand that my Commonwealth IT resource usage may be monitored at any time and by signing this Agreement, I specifically acknowledge such monitoring.

Printed Name: _____

Contractor: _____

Signature: _____

Date: _____

Contracting Agency: _____

Bureau/Facility: _____

Division/Section: _____

Mailing/E-mail Address: _____

Work Phone: _____

Optional Agency Approval: _____

Date: _____

Federal ID #: _____

Mailing Address: _____

E-mail address: _____

Work Phone: _____

Signature: _____