COMMONWEALTH ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESOURCES

Each authorized user must comply with these standards when using the internet or IT resources as defined in *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

AUDITING, MONITORING AND REPORTING

All files, data or records stored on or accessed through IT resources and all records related to IT usage including internet records and electronic mail (email) communications may be searched, traced, audited and/or monitored, with or without notice to the authorized user. This includes, but is not limited to, all internet activity, all internet website access and all email, voice mail and text messages. Agencies and their designees may use tracking, blocking, logging and monitoring software to investigate IT resource usage, restrict certain access and/or alert IT staff to certain inappropriate uses.

Authorized users, therefore, should have no expectation of privacy in any files, data or records stored on or accessed through IT resources, nor should they have any expectation of privacy in any electronic communication sent or received via, or stored within, IT resources. By using IT resources, the user authorizes any such access to or auditing and/or monitoring of IT resources by the commonwealth.

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.

DISCIPLINE OR OTHER CONSEQUENCES OF MISUSE

The improper use of IT resources by employees or volunteers may result in disciplinary action, up to and including termination of employment or volunteer status, depending on the circumstances of the incident. The improper use of IT resources by contractors or consultants may result in disciplinary action that may include termination of engagement, other 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 misuse of IT resources.

GENERAL IT RESOURCES 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 devices.

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 IT resources to engage in personal, for-profit transactions or business, or to conduct any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.

g. Authorized users may not engage in illegal activity in connection with their use of 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 IT resources, unless they are specifically authorized to do so.

h. Authorized users may not access, create, store, transmit, post or view material that is generally considered to be inappropriate or personally offensive or which may be construed as discriminatory or harassing, including sexually suggestive, pornographic or obscene material.

i. Authorized users are personally responsible for the security of authorized portable IT resources. Care must be exercised to ensure these devices are not lost, stolen or otherwise accessed in an unauthorized manner.

j. Authorized users may not store non-public information on IT resources, if those IT resources may be removed from commonwealth facilities without prior approval from the agency Secretary or designee.

k. Authorized users may only use encryption methods approved by the commonwealth to encrypt information. Authorized users may not rely on any business communications via the internet using IT resources being secure, private, or inaccessible, even where appropriate security applications are used, e.g. data encryption.

l. 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 websites being accessed, must be strictly adhered to by authorized users.

Software

In connection with authorized users' use of and access to IT resources:

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 and Content Filtering solution.

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, including but not limited to email, voice mail, text messages, data and any other electronic communications transmitted under their account.

Incidental Use

a. IT resources are communication tools that the commonwealth has made available 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 for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional and incidental.

b. Incidental personal use of internet access is restricted to authorized users; it does not extend to family members, other acquaintances or any other persons.

c. Access to IT resources that are home-based, e.g., accessing the internet from an agency owned, home based computer or laptop, 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 home-based IT resources.

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 IT resources, including personal files and documents, are generally owned by the commonwealth and may be accessed and retrieved in accordance with this policy. In addition, it should be understood that such documents may be subject to requests for disclosure under the *Right to Know Law, 65 P.S. §§ 67.101*, and other similar laws.

Acceptable Use of the Internet

Accepted and encouraged use of the internet for authorized users on IT resources includes, but is not limited to, the following:

a. Access, research, exchange or posting of information that relates to the assigned job duties of an authorized user for carrying out commonwealth business.

b. Promotion of public awareness in regard to commonwealth law, agency services and public policies.

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

- **Acceptable use of Instant Messaging (IM)**

a. Only authorized users who have been granted agency level approval to utilize IM technology may use IM software, and they may use it only to communicate internally across the commonwealth MAN in a manner directly related to an authorized user's job responsibilities.

b. IM software that is utilized by commonwealth authorized users must be part of the determined enterprise standard software solution.

c. IM software is only to be used to conduct state business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These records are subject to the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program* and *Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule*, items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

- **Acceptable use of Web 2.0 Technologies/Tools**

a. Web 2.0 Technologies or tools may include but are not limited to blogs, RSS, discussion boards, social networking, wikis, video sharing sites, AJAX, mashups and folksonomies (social tagging).

b. Only authorized users who have been granted agency level approval to do so may utilize Web 2.0 tools, and only if the use is directly related to an authorized user's job responsibilities.

c. Web 2.0 Technologies or tools are only to be used to conduct state business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These records are subject to the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program* and *Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule*, items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

EMAIL USE

Expectation of Privacy

a. When sensitive material is sent electronically via email, it is important to verify that all recipients are authorized to receive such information and to understand that email 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 email network, the messages should be protected by encryption. Authorized users should contact their agency Network Coordinator or IT Coordinator for assistance if encryption is needed.

d. Email 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 ITC oordinator, who may receive technical assistance from the Office of Administration, Office for Information Technology (OA/OIT).

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 email.

f. All user activity and electronic communication, including the contents of such communication, including but not limited to, email, voicemail, text messages and data, on IT resources is subject to tracking, blocking, logging, auditing, monitoring, accessing, retrieving and reviewing, as described more fully in this directive.

Access Control and Authorization

a. Only authorized users may use IT resources to send or view email or access the commonwealth's email systems.

b. Unauthorized persons may not use the network or commonwealth equipment to originate email messages or read email messages directed to others.

c. Access to commonwealth email will only be granted to commonwealth employees, contractors, consultants, volunteers, in their capacity as authorized users, if they agree to abide by all applicable rules of the system, including this directive and its related standards.

d. An authorized user may not access the email or account of another authorized user unless granted permission to do so by the authorized user. Unauthorized access of an authorized user's email files is a breach of security and ethics and is prohibited. This restriction does not apply to system administrators and management staff in the authorized user's chain of command who are authorized to access email for legitimate business purposes, to effectuate *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

e. In accordance with agency policy, authorized users should use password protection to limit access to email files. Authorized users must safeguard their passwords so that unauthorized users do not have access to their email. Authorized users are responsible for all messages transmitted and originating under their account.

Message Retention

All messages, including email, text messages, and voice messages, are subject to the appropriate records retention and disposition schedules and the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*.

Email Security Issues, Worms and Viruses

Email and attachments to email increasingly are reported to be sources of computer viruses. All authorized users should act in accordance with the latest IT Bulletins regarding containment methods for computer viruses.

Maintaining Professionalism

Every authorized user who uses IT resources is responsible for ensuring posted messages and other electronic communications are professional and businesslike. As a way to impose personal restraint and professionalism, all authorized users should assume that whatever they write may at some time be made public. Authorized users should follow the following guidelines:

Be courteous and remember that you are representing the commonwealth with each email message sent.

Review each email message before it is sent and make certain that addresses are correct and appropriate. Use spell check before sending.

Consider that each email 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 recipients of the message.

Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration and speculation which could be misconstrued. Remember that intonation and inflection are lost in email.

Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of email can easily identify different email 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 supervisors before wide scale "broadcasting" an email 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 email bulletins to all commonwealth or agency employees must first obtain authorization from agency management.

d. Email messages should be brief, and attachments to email messages should not be overly large. Agency IT staff will inform authorized users of limitations on the size of email messages and attachments. OA/OIT periodically will provide technical standards and guidance to agencies through IT Bulletins on the technical capacities of the commonwealth Connect System and limitations on email 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 website at http://www.oit.state.pa.us.

UNACCEPTABLE USES OF IT RESOURCES

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

Accessing, creating, storing, transmitting, posting or viewing material that is generally considered to be inappropriate or personally offensive or which may be construed as harassing, including sexually suggestive, pornographic or obscene material.

Accessing, creating, storing, transmitting, posting or viewing 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 2003-10, Equal Employment Opportunity*.

Engaging in personal, for-profit transactions or business, or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.

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

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

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

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

Violating or infringing the rights of any other person.

Using any other authorized user's password and/or equipment to conduct unacceptable activities on IT resources.

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

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.

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

Downloading and/or installing any unapproved software.

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.

Sending or forwarding confidential or sensitive commonwealth information through non-commonwealth email or webmail accounts. Examples of non-commonwealth email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, Gmail and email provided by other internet service providers.

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, Blackberry devices, two-way pagers and cellular telephones.

Participating in any other internet or email use that is deemed inappropriate by the commonwealth and/or its agencies and is communicated as such to authorized users.

PENNSYLVANIA GAMING CONTROL BOARD IT RESOURCE ACCEPTABLE USE EMPLOYEE ACKNOWLEDGMENT FORM

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

I have read the attached Commonwealth Acceptable Use Standards for Information Technology (IT) Resources, and in consideration of the Commonwealth of Pennsylvania and the Pennsylvania Gaming Control Board (PGCB) 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.

I further understand that my IT resource usage, including electronic communications such as email, voice mail, text messages and other data and records, may be accessed and monitored at any time, with or without advance notice to me. By signing this agreement, I specifically acknowledge and consent to such access and monitoring.

I further understand that if I have any questions regarding the outlined standards and expectations, I am required to ask for clarification from my supervisor or the PGCB Director of Human Resources.

Printed name: _____

Employee number: _____

Signature: _____

Date: _____

Bureau: _____

Email address: _____