MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject:	***Number:***
Commonwealth of Pennsylvania Information Technology Acceptable Use Policy	205.34 Amended
Date:	***By Direction of:***
February 18, 2021	Michael Newsome, Secretary of Administration
Contact Agency: Office of Administration, Office for Information Technology, Telephone 717.787.5440, email: ra-ITCentral@pa.gov	

This directive establishes policy, responsibilities, and procedures for the acceptable use of Information Technology (IT) resources by Authorized Users.

1. PURPOSE. To establish policy, responsibilities, and procedures for the acceptable use of the Commonwealth's IT Resources.

2. SCOPE. This directive applies to all Authorized Users of all departments, boards, commissions, offices, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction.

3. OBJECTIVE. To ensure that all Authorized Users who have access to IT Resources are made aware of and comply with this policy, including the standards set forth herein and in Enclosure 1.

4. DEFINITIONS.

a. Authorized Users. Commonwealth of Pennsylvania employees, contractors, consultants, volunteers, or any other user who has permission to utilize or access the Commonwealth's IT Resources.

b. Commonwealth Data. Any information, records or files, regardless of form, that are owned, managed, processed, generated or stored by the Commonwealth or Authorized Users. Commonwealth Data includes, but is not limited to, data that is intellectual property of the Commonwealth, data that is protected by law, order, regulation, directive or policy and any other sensitive or confidential data that requires security controls and compliance standards.

c. Electronic Communication System. Any method of electronic communication or information system that generates, stores, transmits, or displays Commonwealth Data, including, but not limited to:

(1) The Commonwealth's Metropolitan Area Network (MAN);

(2) Local Area Networks (LANs);

(3) The internet;

(4) News groups;

(5) Bulletin board systems;

(6) Intranets;

(7) Social media;

(8) Blogs;

(9) Computer hardware;

(10) Personal Computer Desktops;

(11) Laptops and Docking Stations;

(12) Software programs;

(13) Applications;

(14) Databases;

(15) Voice mail systems;

(16) Telephones;

(17) Faxes;

(18) Copiers;

(19) Printers or multi-function devices;

(20) Radio;

(21) Cellular and smartphones;

(22) Tablet computers or personal digital assistants;

(23) Electronic mail and messaging systems;

(24) Instant Messaging;

(25) Messaging;

(26) Cloud storage solutions;

(27) USB drives, thumb/flash drives, SD cards;

(28) Video conferencing and transmissions; and

(29) Electromagnetic, photo-electronic, and other electronic media or devices.

d. IT Resources. Equipment or interconnected systems or subsystems of equipment, networks, or services used to receive, input, store, process, manipulate, control, manage, transmit, display and/or output information, including, but not limited to: computers, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, Intranet, email, ancillary equipment, software, firmware, cloud-based services, systems, networks, platforms, plans and data, training materials and documentation and social media websites.

e. Multifactor Authentication. Authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence or factors to an authentication mechanism.

5. POLICY.

a. Authorized Users of IT Resources are required to understand and abide by this directive and the Acceptable Use Standards. These Acceptable Use Standards are designed to prevent use that may be illegal, unlawful, abusive, contrary to policy, or which may have an adverse impact on the Commonwealth or its IT Resources. In addition, these standards identify for Authorized Users the permissible and effective uses of IT Resources. Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer. Enclosure 1, Commonwealth Acceptable Use Standards for IT Resources, sets forth additional information about the permissible scope of usage of IT Resources.

b. Abuse or misuse of IT Resources and Commonwealth Data will have consequences. The improper and/or unauthorized use of IT Resources or Commonwealth Data by Authorized Users may result in disciplinary action, up to and including termination of employment, termination of volunteer status, termination of engagement or other formal action under the terms of the applicable contract or suspension or debarment under the Contractor Responsibility Program as set forth in Management Directive 215.09 Amended, Contractor Responsibility Program, depending on the circumstances of the incident.
When warranted, the Commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse or abuse of IT Resources or Commonwealth Data.

c. Ownership of IT Resources and Commonwealth Data. All Commonwealth Data and IT Resources, including those pertaining to computer use, internet use, email communication, voicemail communication, text messages, online chat, and other electronic communication (whether sent, received, displayed, accessed or stored), as well as the content of such communications, are presumed to be the sole and exclusive property of the Commonwealth. Authorized Users do

not control the access to or the use of such data or records. In addition, Authorized Users have no property or other rights to any or all related physical equipment, hardware, and software applications that are provided in connection with IT Resources.

d. Authorized Users shall have no expectation of privacy when using IT Resources. Authorized Users shall have no expectation of privacy in any IT Resource or in any electronic files, Commonwealth Data, or records stored on or accessed through IT Resources nor should an Authorized User have any expectation of privacy in any communications sent or received via, or stored within, IT Resources.

e. Agency heads may determine who may access IT Resources and Commonwealth Data. At their discretion, executive level or human resources staff or their authorized designees may access IT Resources in any way, including to retrieve, search, trace, audit, monitor and review at any time any files, data, or records whether sent, received, displayed, accessed or stored through IT Resources, as well as, data or records related to IT Resource usage, including internet records, email communications, voicemail communication, text messages, online chat, and other electronic communication, for business purposes, or in order to determine compliance with the provisions of this directive or any other directive, personnel policy or applicable local, state, or federal law.

f. IT Resources are subject to monitoring or other access. All IT Resources and Commonwealth Data, or records, whether sent, received, displayed, accessed or stored on or accessed through IT Resources, may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, or retrieved) with or without notice to the Authorized User.

g. Use of an IT Resource by an Authorized User is deemed to be consent to monitoring. The use of an IT Resource by an Authorized User constitutes consent to monitoring. By using an IT Resource, Authorized Users consent that all activity on that IT Resource is subject to monitoring, tracing, logging, blocking, censoring, auditing, or searching, with or without notice, to examine or retrieve the Authorized User's historical or real-time activity.

h. Authorized Users may not access unauthorized Commonwealth Data and shall take measures to protect the security of Commonwealth Data. Authorized Users may not access Commonwealth Data or IT Resources that they have not been granted access to and shall take measures to protect the security of Commonwealth Data. Authorized Users must use acceptable cybersecurity measures in a manner that is consistent with Commonwealth policy. Use of acceptable cyber security measures does not, however, guarantee the confidentiality of any electronic communication or of any file, Commonwealth Data, or record stored or accessed through IT Resources. Authorized Users must keep confidential any credentials used for authentication and not share them with others. Credentials may include, but are not limited to, passwords, certificates, tokens, Personal Identification Numbers (PINs), knowledge-based

questions/answers, time-based one-time passcodes (TOTP), and other credentials.

i. **IT Resources are intended for business use and shall be used primarily for that purpose.** IT Resources are tools that the Commonwealth has made available for Commonwealth business purposes. Where personal use of IT 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. Any personal use that is inconsistent with Commonwealth policy is prohibited.

j. **IT Resources must never be used in a manner that violates other Commonwealth directives and policies.** All use of IT Resources must conform to all Commonwealth policies, including but not limited to Executive Order 1980-18, Code of Conduct, Management Directive 505.7 Amended, Personnel Rules, and Commonwealth policies on nondiscrimination and prohibition of sexual harassment. Violations of the Commonwealth's policies through IT Resources will be treated in the same manner as other violations.

k. **All Authorized Users must be provided with this directive.** All current Authorized Users must be provided an electronic or hard copy of this policy on an annual basis. All new Authorized Users must review this policy prior to their use of and access to IT Resources.

l. **All Authorized Users must sign an Acknowledgement of Receipt Form.** On an annual basis, agencies must obtain signed user agreements from Authorized Users prior to granting access to IT Resources. Employees or volunteers shall sign Enclosure 2 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form. Contractors and consultants shall sign Enclosure 3 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form.

m. **Each agency must maintain copies of the agreement signed by each Authorized User in that agency.** Completed user agreements shall be maintained as part of the employee's Electronic Official Personnel Folder (E-OPF). Agencies will store these agreements in the electronic format consistent with Management Directive 210.12 Amended, Electronic Commerce Initiatives and Security, and ITP-SEC006, Commonwealth of Pennsylvania Electronic Signature Policy. Signed agreements are accessible to employees and supervisors as well as HR staff with specific roles, who are authorized to view these documents.

n. **Requests for electronic records shall be treated in the same manner as hard records.** Requests for records pertaining to IT Resources shall be addressed consistent with all laws, directives, or policies that would apply to the same records if maintained in a hard

format. All such requests shall be referred to agency legal counsel and/or the Agency Open Records Officer, as appropriate.

o. This amended directive supersedes prior or inconsistent policies. This policy supersedes any existing HR, IT, internet and/or email 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 collective bargaining agreements, side letters or current practices shall be applied in a manner to effectuate both this policy and any such agreement, side letter or current practice. In cases where a provision of an approved collective bargaining agreement, side letter or current practice cannot be reconciled with this policy, the former shall control. Agencies may develop supplemental HR, IT, internet and/or email use policies only with the approval of the Secretary of Administration or designee.

6. RESPONSIBILITIES.

a. Agency shall:

(1) Provide either a hard copy or electronic copy of this directive to Authorized Users.

(2) Ensure that Authorized Users have signed the user agreement.

(3) Maintain a copy of the signed user agreement for each Authorized User.

b. Authorized Users shall:

(1) Understand the permissible scope of usage of IT Resources and Commonwealth Data and comply with this management directive and the applicable enclosure.

(2) Sign the user agreement.

c. Enterprise Information Security Office shall:

(1) Conduct system audits and compliance reviews of adherence to this directive.

(2) Prevent and respond to cybersecurity incidents.

(3) Assist human resources staff in conducting investigations involving the alleged misuse of IT Resources and/or Commonwealth Data.

(4) Assist in Commonwealth Data retrieval and analysis for any records requests.

(5) Provide annual security awareness training in compliance with Management Directive 535.9 Physical and Information Security Awareness Training.

7. RELATED GUIDANCE/REFERENCES. Technical standards and guidance relating to IT Resources and Commonwealth Data usage published by the Office of Administration, Office for Information Technology (OA/OIT), Information Technology Policies (ITPs) must be followed and are available on the OA/OIT website.

This directive replaces in its entirety, Management Directive 205.34, dated March 19, 2020.

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

Enclosure 2 Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form

Enclosure 3 Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form

ENCLOSURE 1

COMMONWEALTH ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESOURCES

Each Authorized User must comply with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and the following Acceptable Use Standards when using IT Resources:

1. AUDITING, MONITORING AND REPORTING

All IT Resources and files, Commonwealth Data, or records, whether sent, received, displayed, accessed or stored on or accessed through IT Resources, may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded) with or without notice to the Authorized User.

All activity may be monitored. Authorized Users should have no expectation of privacy in any files, Commonwealth Data, or records whether sent, received, displayed, accessed or stored 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 access to or auditing and/or monitoring of IT Resources by the Commonwealth.

Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer.

2. DISCIPLINE OR OTHER CONSEQUENCES OF MISUSE

The improper use of IT Resources or Commonwealth Data 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 or Commonwealth Data by contractors or consultants may result in termination of engagement, other action under the terms of the applicable contract, or suspension or debarment under the Contractor Responsibility Program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse of IT Resources.

3. GENERAL IT RESOURCES USE

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

b. Authorized Users are strictly responsible for maintaining the confidentiality of their Commonwealth or agency account(s), passwords, Personal Identification Numbers (PIN), Security Tokens, or similar information or devices used for identification and authorization purposes (such as multi-factor authentication methods).

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

d. Authorized Users may not use non-standard open-source software, shareware, or freeware software (i.e. unauthorized resources) without OA/OIT prior approval generated through established policy exception processes. Authorized Users may not use unauthorized resources on IT Resources to conduct official business.

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 IT security controls.

f. Authorized Users may not use IT Resources to engage in personal, for-profit transactions or business, or to conduct any not-for-profit or 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, and/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 authorized to do so by human resources or law enforcement, in conjunction with the Enterprise Information Security Office (EISO).

h. Authorized Users may not use IT Resources or any unauthorized assets/devices to leverage IT Resources to 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 and mobile IT Resources. This includes securing mobile devices when traveling nationally or internationally. Care must be exercised to ensure these devices are secured and not lost, stolen, or otherwise accessed in an unauthorized manner. Authorized users must report lost or stolen IT Resources to their immediate supervisor upon discovery of lost or stolen IT Resources.

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 shall use Commonwealth-approved Electronic Communication Systems primarily for Commonwealth business.

l. Authorized Users shall use only Commonwealth-approved encryption methods to encrypt Commonwealth Data, as appropriate.

m. Authorized Users shall use only Commonwealth-approved storage solutions.

n. Authorized Users shall only store or transmit Commonwealth content, files, Commonwealth Data or any other type of information on or through an IT Resource that is Commonwealth-provided or Commonwealth-approved.

o. Authorized Users shall not use IT Resources, or personal devices, to record telephone calls or other conversations unless all parties to the conversation consent prior to the recording. Recording an oral conversation without consent from anyone and/or consent from only one party during the conversation is prohibited. Examples of conversations include, but are not limited to, oral discussions, group meetings, online web collaboration meetings, phone calls, conference calls, or group discussions. Someone who violates Pennsylvania law that requires "two-party" consent may also be subject to civil liability and may be subject to discipline, up to and including termination of employment. It is further a violation of the Wiretap Act for a person to disclose or to use the contents of any illegally recorded conversation.

4. INTERNET USE

All security policies of the Commonwealth and its agencies must be strictly adhered to by Authorized Users.

5. SOFTWARE

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

a. All software used to access IT Resources must be part of the agency's standard software suite or approved by the agency IT department and agreed to by the Commonwealth. The terms and conditions for the software must be approved by the Commonwealth. The software must incorporate all vendor-provided security patches.

b. All files downloaded from the internet must be scanned for viruses using the approved Commonwealth standard scanning solution.

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.

6. ACCESS CONTROL AND AUTHORIZATION

Agencies shall authorize access to the internet using IT Resources through the utilization of an Identity and Access Management system. Authorized Users shall be responsible for the protection of their passwords, and IT Resources used for multi-factor authentication. Authorized Users are responsible for activity and communications, including but not limited to email, voicemail, text messages, data, and any other electronic communications transmitted under their account.

7. 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 may be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental. IT Resources may not be used for supplemental employment or to engage in non-Commonwealth personal business ventures.

b. Access to IT Resources that are off-Commonwealth network, such as accessing the internet from an agency owned, home-based computer, must adhere to all the same policies that apply to use from within agency facilities.

c. Authorized Users may not allow family members, other acquaintances, other persons or non-employees to access Commonwealth-provided IT Resources or internet access through 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. Incidental use may not risk legal liability for, or embarrassment to, the Commonwealth.

g. All files and documents located on IT Resources, including personal files and documents, may be accessed and retrieved in accordance with this policy. In addition, it shall be understood that such documents may be subject to disclosure under the Right-to-Know Law, 65 P.S. §§ 67.101—67.3104, and other laws.

8. ACCEPTABLE USE OF THE INTERNET

Acceptable 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.

9. ACCEPTABLE USE OF INSTANT MESSAGING (IM)

a. Authorized Users may use IM software 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 Authorized Users must be part of the determined enterprise standard software solution.

c. IM software shall only be used to conduct Commonwealth 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 210.05, The Commonwealth of Pennsylvania State Records Management Program and Manual 210.09, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule, items G001.021, Transitory Records and G001.025, Transitory Files Confidential*.

10. ACCEPTABLE USE OF SOCIAL MEDIA

a. Social Media platforms may include, but are not limited to, blogs, individual/group chat, discussion boards, wikis, and video/photo sharing sites and professional networking sites. Only authorized Social Media platforms are to be connected to IT Resources and associated with Commonwealth email accounts. Authorized Social Media platforms are to be approved by the Office of Administration prior to access and use.

b. Only Authorized Users who have been granted agency-level approval to do so may utilize authorized external Social Media platforms, and only if the use is directly related to an Authorized User's job responsibilities in accordance with *Management Directive 205.42, Social Media*.

c. Social Media may be used only to conduct Commonwealth business that produces records that have little or no documentary or evidentiary value and that need not be retained for future use. These records are subject to the provisions of *Management Directive 210.05, The Commonwealth of Pennsylvania State Records Management Program and Manual 210.09, The Commonwealth of Pennsylvania General Records Retention* and *Disposition Schedule, items G001.021, Transitory Records and G001.025, Transitory Files Confidential.*

11. ACCEPTABLE USE OF MOBILE TECHNOLOGIES

Authorized Users shall ensure that information on mobile devices is not compromised by:

a. Securing mobile devices from access by unauthorized persons, through the use of locking devices, passwords, or other appropriate protection;

b. Ensuring that unauthorized persons do not view information on the display screen;

c. Refraining from checking devices into airline luggage systems, with hotel porters, or from using other unsupervised handling or storage processes;

d. Securing or maintaining possession of mobile devices at all times; and

e. Immediately reporting a lost or stolen mobile device to their supervisor.

12. ACCEPTABLE USE OF CLOUD-BASED STORAGE SOLUTIONS

a. Cloud-based solutions enable convenient, on-demand network access to a shared pool of configurable computing resources such as digital processing or storage that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud-based solutions are intended for business use and shall be used only for that purpose.

b. Cloud-based solutions contracted by the Commonwealth are considered IT Resources in scope of this Management Directive and must never be used in a manner that does not comply with other Commonwealth issuances and policies, and violations thereof will be treated in the same manner as other violations of policy.

c. All Commonwealth Data located in cloud-based solutions is owned by the Commonwealth and may be accessed and retrieved like any other Commonwealth Data in accordance with this management directive. In addition, it shall be understood that such Commonwealth Data may be subject to requests for disclosure under the Right-to-Know Law, 65 P.S. §§ 67.101—67.3104, and other similar laws.

d. Authorized Users will only access those cloud-based solutions which have been authorized for their use.

e. Authorized Users who obtain a password and ID for a cloud storage solution shall keep that password confidential. Commonwealth policy prohibits the sharing of user IDs, passwords, and other authentication methods obtained for access to network and cloud storage resources.

f. Authorized Users are responsible for the use of their individual cloud-based solution accounts and shall take all reasonable precautions to prevent others from being able to use their account, including, but not limited to, coworkers, friends, or family.

g. Commonwealth policy or procedure shall not be violated via use of a cloud storage solution unless that policy or procedure is itself explicitly waived by OA/OIT.

h. Cloud-based solutions that contain or hold Commonwealth Data are considered IT Resources in scope of this Management Directive and must never be used in a manner that does not comply with other Commonwealth issuances and policies, and violations thereof will be treated in the same manner as other violations of policy.

i. Cloud-based solutions that contain or hold Commonwealth Data may be accessed and retrieved like any other Commonwealth Data in accordance with this management directive. In addition, it shall be understood that such Commonwealth Data may be subject to requests for disclosure under the Right-to-Know Law, 65 P.S. §§ 67.101—67.3104, and other similar laws.

13. EMAIL USE

a. Usage

(1) 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.

(2) Authorized Users shall understand that messages can be quickly and easily copied and may be forwarded inappropriately.

(3) Where it is necessary to transmit Commonwealth proprietary, confidential, sensitive, protected, privileged or pre-requisite required information beyond the Commonwealth email network, the messages shall be protected by encryption. Authorized Users shall contact their agency Information Security Officer (ISO) for assistance if encryption is needed.

(4) Email messages, to be transmitted outside of the United States, shall comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users shall contact their ISO who may receive technical assistance from the Office of Administration, Office for Information Technology (OA/OIT).

(5) The data owner shall determine the data classification regarding business information which is determined to be too confidential or sensitive to be transmitted via email.

(6) The agency head or designee shall determine if data can be shared, and the means by which it can be shared, e.g. transmitted via email, etc. in accordance with the data owner's requirements, e.g. IRS Publication 1075, CJIS policy, HIPAA privacy rules.

(7) Agencies shall not share data owned by a third party without express written consent from the data owner following their requirements, e.g. IRS Publication 1075, CJIS policy, HIPAA privacy rules. Business area staff and OA/OIT shall review all requests for the release of data.

(8) OA/OIT shall coordinate with business area staff, agency management, and OA Legal to determine data sharing requirements. OA/OIT shall assist business area staff in making information sharing/collaboration decisions and document the sharing of data.

(9) Authorized Users shall use email addresses assigned to them primarily for work-related purposes. Authorized Users may not use their Commonwealth e-mail address to register for or subscribe to any product or service that is not work-related.

(10) Authorized Users shall not forward work-related emails, calendar items or documents to their personal or other non-Commonwealth email addresses. In the event that a provision of an approved collective bargaining agreement, side letter or current practice cannot be reconciled with this policy, the former will control.

b. Access Control and Authorization

(1) Only Authorized Users may use IT Resources to send or view email or access the Commonwealth's email systems.

(2) Only after agreement to abide by all applicable rules of the system, including this directive and its related Acceptable Use Standards, shall access to Commonwealth email be granted to Commonwealth employees, contractors, consultants, and volunteers, in their capacity as Authorized Users.

(3) An Authorized User may not access the email or account of another Authorized User. This restriction does not apply to system administrators and management staff in the Authorized User's chain of command, authorized to access email for legitimate business purposes, to effectuate this directive.

(4) In accordance with agency policy, Authorized Users shall use appropriate cyber security measures in accordance with Commonwealth policy to limit access to Commonwealth Data. Authorized Users shall safeguard their cyber security measures so that Unauthorized Users do not have access to their email. Authorized Users are responsible for all messages transmitted and originating under their account.

c. Message Retention

All messages, including email, text messages, IMs and voicemail messages, are subject to the appropriate records retention and disposition schedules and the provisions of *Management Directive 210.05, The Commonwealth of Pennsylvania State Records Management Program.*

d. Email Security

Email and attachments to email are sources of computer security issues. All Authorized Users shall act in accordance with the latest IT Policies and other OA/OIT guidance regarding containment methods for computer viruses and any security alert emails from agency HR or IT.

e. 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 shall assume that whatever they write may at some time be made public. Authorized Users shall follow the following guidelines:

(1) Be courteous and remember that you are representing the Commonwealth with each email message sent.

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

(3) 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.

(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 email can easily identify different email messages.

14. UNACCEPTABLE USES OF IT RESOURCES

The following are examples of unacceptable 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:

a. 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 or threatening activities, including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, offensive material, sexually suggestive, pornographic, or obscene material.

b. 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 2016-04, Equal Employment Opportunity.*

c. Engaging in personal, for-profit transactions or business, supplemental employment activities or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the Commonwealth.

d. 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.

e. Attempting to test or bypass the security of IT Resources or to alter internal or external IT Resource systems or Commonwealth Data.

f. Participating in or promoting the bypass of security through the intentional introduction of computer viruses, worms, malware, ransomware, or other forms of malicious software or malicious code.

g. Promoting, soliciting, or participating in any activities that are prohibited by local, state, or federal law or Commonwealth policy.

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

i. Using any other Authorized User's account and/or equipment to conduct unacceptable activities on IT Resources.

j. Transmitting, using, 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.

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

l. Downloading, distributing, and/or installing any unapproved software.

m. 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.

n. Sending or forwarding Commonwealth Data or records to non-Commonwealth IT resources or through non-Commonwealth email accounts.

o. Sending, forwarding, or storing Commonwealth Data or records utilizing non-Commonwealth IT resources or non-Commonwealth accredited mobile devices.

p. 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.

q. Using or disclosing Commonwealth Data without proper authorization.

r. Authorized Users shall receive authorization from their supervisors before Enterprise-wide-scale "broadcasting" an email bulletin to groups of employees.

s. The use of "reply to all" shall be avoided unless it is appropriate to respond to all addressees. Senders shall utilize "blind carbon copy "BCC" email feature for large audiences to avoid accidental reply to all responses.

t. Authorized Users wishing to send email bulletins to all Commonwealth or agency employees must first obtain authorization from the agency communication director or designee.

15. TELEWORKING REQUIREMENTS

The following is a list of teleworking requirements that Authorized Users shall follow:

a. **Wi-Fi and Public Networks:** Secure your home network with a strong password and use passwords for all devices on your network.

b. **Data Storage:** Keep Commonwealth Data on work devices only.

c. **Physical Security:** Use a strong password or passphrase and lock when your device is unattended. Make sure the device is accounted for when transporting it. Maintain awareness on who has a line of sight to your device while working.

d. **Data:** Follow all record keeping policies. Backup your data to OneDrive or a Commonwealth network shared drive.

e. **Social Media:** Follow all Agency and Commonwealth guidelines on social media. Be aware of misinformation.

f. **Reporting:** Report suspicious activities to OA-SecurityIncidents@pa.gov. Reporting phishing to CWOPA_Spam@pa.gov.

16. TELEWORKING UNACCEPTABLE PRACTICES

The following practices are prohibited during teleworking.

a. **Wi-Fi and Public Networks:** Using public or unsecured networks. Allowing unknown devices to access your network.

b. **Incidental Use:** Using IT Resources for personal use where such use interferes with the efficiency of operations or is 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. Allowing non-employees to use work devices (even for simple tasks) is prohibited.

c. **Physical Security:** Having passwords written down, even in your home. Care must be exercised to ensure devices are secured and not lost, stolen, or otherwise accessed in an unauthorized manner.

d. **Data:** Leaving hard records unsecured and unattended. Using a thumb drive or personal storage devices to store Commonwealth data.

e. **Social Media:** Presenting personal information such as birthdays, addresses or phone numbers. Sharing personal information can lead to account compromise.

f. **Reporting:** Opening potential spam or phishing emails. Do not assume someone else has reported a phishing email.

ENCLOSURE 2

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

This User Agreement does not prohibit employees or volunteers from performing authorized job duties.

I have read the attached *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, and Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources, 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, including electronic communications such as email, voicemail, text messages, and other Commonwealth 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 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 Address: _____

Email 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 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, and Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources, 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, including electronic communications such as email, voicemail, text messages, and other Commonwealth 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.

Printed Name: _____

Contractor/Consultant: _____

Signature: _____

Date: _____

Contracting Agency: _____

Bureau/Facility: _____

Division/Section: _____

Mailing Address: _____

Email Address: _____

Work Phone: _____

Optional Agency Approval: _____

Date: _____

Federal ID #: _____

Mailing Address: _____

Email address: _____

Work Phone: _____