



pennsylvania
OFFICE OF ADMINISTRATION

Testimony

Senate Intergovernmental Operations Committee

**Public Hearing on Use by Public Officials and Employees of
Messaging Apps with Autodeletion Features**

March 24, 2025

Office of Administration

Neil R. Weaver, Secretary

Chairman Coleman, Chairwoman Tartaglione, and members of the Senate Intergovernmental Operations Committee, thank you for the opportunity to provide written testimony for today's hearing.

The Office of Administration (OA) understands the importance of transparency and the appropriate use of technology to create and maintain records, both to comply with laws such as the Right-to-Know Law and the Sunshine Act, and to keep the public trust.

The OA Office for Information Technology (OIT) establishes standards and policies for the acceptable use of Commonwealth technology resources, including mobile devices. These standards and policies apply to all authorized users, which include employees and agencies under the Governor's jurisdiction, as well as any other entity connecting to the Commonwealth network.

As a part of its larger technology governance strategy, OIT employs industry leading Mobile Device Management (MDM) and Mobile Application Management (MAM) tools to prevent the misuse of Commonwealth devices and data.

MDM tools secure, monitor, manage, and support mobile devices. By deploying MDM tools to Commonwealth-issued devices, OIT prevents users from downloading unauthorized applications. Users are also unable to access commercial app stores and may only install applications which have been reviewed and approved for use. OIT reviews and approves enterprise applications for use by all agencies. If an agency has a need for a specific application to conduct business, the Chief Technology Officer and Chief Information Security Officer assigned to the delivery center serving that agency are responsible for reviewing and determining if the request should be approved.

In instances where authorized users are permitted to use privately owned mobile devices to access Commonwealth resources, MAM tools are used to protect Commonwealth data. These

tools prevent the user from copying, printing, and downloading Commonwealth data to a personal mobile device.

A copy of the Commonwealth's Mobile Device Policy is attached to this testimony.

In addition to technical controls, there is also an important human factor to securing and appropriately maintaining Commonwealth assets, including technology, data, and records. Authorized users must understand the rules concerning access to, and appropriate use of, Commonwealth tools and data.

OA conducts multiple training courses to educate authorized users on the protection and acceptable use of data and technology resources. Each year, all authorized users are required to complete Security Awareness and Acceptable Use training. In addition to training on cybersecurity best practices, this course instructs authorized users on their responsibility to use Commonwealth data and technology only for Commonwealth business and provides information and guidance on approved tools and technologies. The training also includes a copy of Management Directive 205.34 Amended - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy. Authorized users are required to acknowledge their understanding of the directive and its requirements at the end of the course.

A copy of Management Directive 205.34 Amended - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy is attached to this testimony.

Records management, retention, and disposition are closely tied with the appropriate use of Commonwealth data and technology; therefore, employees have a duty to understand their records management responsibilities. Management Directive 210.5 Amended - The Commonwealth of Pennsylvania State Records Management Program and Manual 210.1 Amended - The Commonwealth of Pennsylvania Employee Records Management Manual establish records management policies, as well as the agency and employee responsibilities

that accompany those policies. All employees are responsible for identifying the different types of records in their possession and classifying them accordingly. Once classified, employees must manage those records in accordance with the General Records Retention and Disposition Schedule or their Agency-Specific Records Retention and Disposition Schedule.

Copies of Management Directive 210.5 Amended - The Commonwealth of Pennsylvania State Records Management Program and Manual 210.1 Amended - The Commonwealth of Pennsylvania Employee Records Management Manual are attached to this testimony.

Through the combination of these well-established policies, regularly-scheduled employee education and training, and technical guardrails, OA has created a strong framework to ensure that Commonwealth data, records, and resources are used and maintained in accordance with applicable law and the public trust.

At this time, OA is not proposing statutory changes.

Mobile Device Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
September 30, 2025

Supersedes:
ITP-PLT012, ITP-SEC035

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) establishes the accepted practices, responsibilities, and procedures for the use of Mobile Devices that are authorized to leverage Commonwealth IT Resources or networks.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the IT Policy Glossary.

Mobile Devices shall not store or transmit sensitive or non-public information without protective measures approved by the agency Information Security Officer (ISO).

Mobile Devices are prohibited from being connected to public Wi-Fi. Physical protection, access controls, cryptographic techniques, backups, virus protection, and the rules associated with connecting Mobile Devices to networks (excluding all public Wi-Fi, which is prohibited under this policy), and guidance on the use of these devices in public places must be followed on all Mobile Devices. These requirements extend to, and cover, removable/mobile media associated with Mobile Devices.

Mobile Devices connecting directly to the Commonwealth network via carrier cellular network integration shall ensure embedded SIM cards, eSIM cards, or compensating controls such as SIM PINs, or locking of the SIM to the serial number of the device are in place to prevent the use of the SIM in an unauthorized device.

Mobile Devices containing Commonwealth Data shall not be left unattended. Mobile Devices must be secured from access by unauthorized persons, through the use of locking devices, passwords, or other approved protection.

Mobile Devices used for official business shall not be Jailbroken or Rooted. A Commonwealth-issued Mobile Device that is Jailbroken or Rooted is deemed “misuse of IT resources” as defined in *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and personnel may face disciplinary actions due to non-compliance.

The use of Promiscuous Mode from a Mobile Device while attached to the Commonwealth network is prohibited.

Authorized users of Mobile Devices shall ensure all security updates are applied in accordance with the *Patch Management Policy*.

4.1 Required Mobile Device Service Offerings

The following table summarizes the required use of the Mobile Device Management (MDM) and Mobile Application Management (MAM) service offerings from the Office of Administration, Office for Information Technology (OA/IT) for Mobile Devices. Refer to the *Mobile Device Configuration Procedure*, contact RA-OAITPOLICY@pa.gov for requests) for guidance on baseline configurations required for these service offerings.

Device Type	Mobile Device Management (MDM)	Mobile Application Management (MAM)
Commonwealth issued devices	Agencies must leverage OA/IT service offering or obtain and submit an approved exception for an alternative.	Agencies must leverage OA/IT service offering or obtain and submit an approved exception for an alternative.
Privately Owned devices / Bring your own device (BYOD)	Not Applicable	Users with Privately Owned devices shall be required to use MAM for Commonwealth applications to prevent disclosure of Commonwealth Data.

4.2 Commonwealth-Issued Mobile Devices

All Commonwealth-issued Mobile Devices are required to use OA/IT service offerings for device management.

Agencies that do not elect to leverage the OA/IT service offering must have a documented and OA/IT approved alternative approach that includes a security management plan with the approved ITP exception to meet the policy requirements.

4.2.1 Supported Mobile Devices

OA/IT will publish and make accessible via the Telecommunication Management Officer (TMO) SharePoint site a current Mobile Device Certification List of Mobile Devices supported by OA/IT service offerings.

4.2.2 Unsupported Mobile Devices

For Mobile Devices not listed on the Mobile Device Certification List, agencies shall maintain the responsibility for ensuring these devices conform to the minimum security requirements, perform validation testing, and submit a Mobile Device Certification Form to RA-EnterpriseVoiceServices@pa.gov for review before connecting any unsupported Mobile Device to the Commonwealth network or accessing Commonwealth IT Resources.

4.2.3 Interconnected Devices and Wearables

Agencies shall conduct risk assessments of each Mobile Device prior to adding to the supported Mobile Device Certification List. Active cloud connectivity, near field communication (NFC), wireless networking (WLAN), and other communication vectors available will need internal risk profiles completed (contact agency or respective ISO for guidance). Each Mobile Device shall be reviewed for privacy concerns with data that is transferred and/or stored. All applicable end-user license agreements (EULAs) shall be reviewed by legal counsel.

4.3 Mobile Application Management

MAM is used to distribute and manage Mobile Applications. Agencies must utilize the OA/IT service offering or obtain and submit an approved exception for an alternative as outlined in Section 3.1.

4.4 Mobile Applications

Mobile Applications can be developed internally by an agency or developed by an external third-party entity. Applications developed by a third-party entity usually have their own end-user license agreement (EULA) with separate terms and conditions.

A list of third-party applications that have been reviewed and approved by OA/IT for use by all Agencies will be made available on the TMO SharePoint site. All other third-party applications shall be reviewed and approved at the agency level as follows:

- Any agency hosting a third-party developed Mobile Application within its own application repository is responsible to ensure that the application is vetted with appropriate IT, executive, and legal approvals. The agency accepts all financial, security, and legal risks associated with that decision.
- Third-party applications that duplicate capabilities within existing third-party applications previously reviewed and approved by OA/IT are prohibited. Third-party applications the Agency is considering must add functionality that is required and unavailable within the current list of OA/IT reviewed and approved third-party applications.
- The management and approval of third-party applications for installation on Commonwealth-

issued Mobile Devices must be approved by both the Agency CTO and Agency ISO. OA/IT shall maintain agency and business area specific application catalogs within the MAM/MDM primary service offering.

Direct access to consumer app stores by the end user is prohibited on Commonwealth-issued Mobile Devices.

4.5 Mobile Email Management

Agencies requiring access to CWOPA (Exchange) email from Commonwealth-issued or Privately Owned (BYOD) Mobile Devices must use the OA/IT MAM Messaging (secure containerized email) service.

All other email messaging applications not explicitly authorized in this policy are prohibited; including, but not limited to, web mail scrapers, non-Commonwealth- issued Virtual Desktop Interface (VDI) clients, or any other non-Commonwealth-issued messaging applications that access Commonwealth IT Resources.

4.6 Privately Owned Mobile Devices

The use of Privately Owned Devices by Authorized Users to remotely access COPA IT Resources is strictly prohibited. Only under the following extenuating circumstances and only for so long as the extenuating circumstance exists may a Privately Owned Device be utilized to remotely access COPA IT Resources:

- Pandemic, emergency, or disaster scenario requiring the Authorized User to have remote access to COPA IT Resources in order for Commonwealth business to function; or
- Critical systems support during non-Commonwealth business hours requires the Authorized User to have remote access to COPA IT Resources in order for Commonwealth business to function.

Under any other circumstances, the use of Privately Owned Devices by Authorized Users to remotely access COPA IT Resources shall comply with this ITP and only after an approved IT Policy Exception is obtained by the Agency business area may the Authorized User use the Privately Owned Device to remotely access COPA IT Resources. The exception request shall include a timeline or estimated timeframe for the purchase of Commonwealth issued devices to negate the need for the use of Privately Owned Devices.

It is preferable that Commonwealth issued devices are used by Authorized Users for teleworking purposes. If Commonwealth issued devices are not available, the use of Privately Owned Devices must follow the requirements in this ITP, receive an approved IT Policy Exception and a request to procure Commonwealth owned devices must be submitted.

For connectivity details, requests for approval to temporarily use Privately Owned Devices to remotely access COPA IT Resources and steps to modify system configurations on Privately Owned Devices, follow the guidance in the *Connectivity Methods for Remotely Accessing Commonwealth IT Resources Procedure*.

Under no circumstances shall the Commonwealth be responsible to support and/or maintain the

Authorized User's Privately Owned Device and approval to temporarily use the Privately Owned Device shall not imply such a responsibility. Further, the Authorized User shall not be entitled to nor shall the Authorized User receive assistance or reimbursement from the Commonwealth for configuration, installation, maintenance, repair, or replacement of the Authorized User's Privately Owned Devices.

Connecting Privately Owned Devices directly to COPA IT Resources, including agency networks, is strictly prohibited.

When an Authorized User uses a Privately Owned Device to gain Remote Access to COPA IT Resources or COPA applications, the Authorized User must comply with the following criteria outlined below:

- Connection to COPA IT Resources shall be through Virtual Desktop Infrastructure (VDI).
- Anti-Virus (AV) software shall be installed and kept current on the Privately Owned Device. For additional information, please refer to ITP-SEC001 Enterprise Host Security Software Policy for policy regarding anti-virus software.
- Patches and security updates shall be kept current on the Privately Owned Device in accordance with ITP-SYM006 Commonwealth IT Resources Patching Policy. For PCs with a Microsoft operating system, it is recommended that the Microsoft Windows Update feature be configured to automatically receive and install updates.
- Authorized Users shall store and maintain all Commonwealth data on the CoPA managed system or service only. Commonwealth data shall never be saved locally to Privately Owned Device per *Management Directive 205.34 Amended Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.
- Privately Owned Devices used to access COPA IT Resources shall adhere to the same password requirements set forth by the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard*.
- Authorized Users shall access data through the Privately Owned Device only in a manner that is in accordance and compliance with published IT policies and regulatory requirements mandated by your Agency.
- Authorized Users shall report occurrences of cyber security incidents or data breaches on all Privately Owned Devices used to remotely access COPA IT Resources in compliance with the *IT Security Incident Reporting Policy*.
- Public Computers shall not be used to access COPA IT Resources. Using a Public Computer to connect to a COPA IT Resource poses a significant security risk. For instance, a third party may easily capture a user's logon credentials.
- Privately Owned Printers shall not be used to print Commonwealth Data. Only Commonwealth issued printing devices shall be used to print Commonwealth Data.
- A Privately Owned Device that is used to remotely access COPA IT Resources may be seized and/or searched at the Commonwealth's discretion in connection with, but not limited to, a cyber security incident or breach, e-Discovery, Right-to-Know Law, or non-compliance with Commonwealth policies.
- All electronic and hard copy records, data, and files created or maintained in connection with the performance of job duties are the property of the Commonwealth and are subject to applicable confidentiality and retention practices, regardless of where stored or maintained,

and shall be subject to Right-to-Know Law as outlined in *Management Directive 205.36 Amended Right-To-Know Law Compliance*.

- Privately Owned Devices used to remotely access COPA IT Resources may be subject to access and inspection as outlined in *Management Directive 205.34 Amended Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.
- Electronic information that is maintained or stored on a Privately Owned Device that remotely accesses IT Resources shall be collected for purposes of e-Discovery for litigation matters if a determination has been made by Agency Legal Counsel in compliance with the *e-Discovery Technology Standards*.
- Commonwealth issued and Privately Owned Mobile Communication Devices that are being used to conduct Commonwealth business must follow the guidance set forth in this policy.
- OA/IT MAM service offerings or an approved agency alternative mobile security solution is required for Privately Owned Mobile Devices (non-Commonwealth-issued devices).
- Commonwealth applications are prohibited from being installed or utilized on Privately Owned Mobile Devices unless OA/IT service offering for MAM is installed and active on the Mobile Device as outlined in Section 4.1. Agency ISOs shall make final determination on appropriate use of Privately Owned Mobile Devices and the use of Commonwealth applications.
- Connection of a Privately Owned Mobile Device to the Commonwealth or an agency network is strictly prohibited.
- Authorized users shall fully understand that Privately Owned Mobile Devices utilized to access Commonwealth IT Resources may be seized and/or searched at the Commonwealth's discretion in connection with, but not limited to, a cyber security incident, or breach, e-Discovery, Right-to-Know Law, or non-compliance with Commonwealth policies.
- In addition, under no circumstances shall the Commonwealth be responsible to support or maintain the Authorized User's Privately Owned Mobile Device. Approval to utilize a Privately Owned Mobile Device shall not imply such a responsibility. Additionally, the Authorized User shall not be entitled to, nor receive assistance or reimbursement from the Commonwealth for configuration, installation, maintenance, repair or replacement of the Authorized User's Privately Owned Mobile Device.
- It shall only be utilized to conduct personal business and not utilized to conduct Commonwealth business such as, but not limited to, administrative, or job-related activities/duties.

Note: Authorized Users are permitted to access employee resources, such as Employee Self Service (ESS), from their Privately Owned Mobile Device to obtain their own personal data, such as, but not limited to, pay statements, tax forms, benefit and leave information.

5. Contact

Questions or comments may be directed via email to [OA, IT Policy](#).

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document




Management Directive

Commonwealth of Pennsylvania

Governor's Office

Management Directive 205.34 Amended – Commonwealth of Pennsylvania Information Technology Acceptable Use Policy

Date: September 7, 2022

By Direction of: 
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 under the Governor's jurisdiction (hereinafter referred to as "agencies").

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 User.** Commonwealth of Pennsylvania employees, contracted resources, consultants, volunteers, or any other users who have been granted access to and are authorized by the Commonwealth to use Commonwealth 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.
- f. **Video Sharing Service.** An enterprise application or service where Authorized Users can create, upload, view, publish, and share videos.

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 505.07 Amended, Personnel Rules,* and Commonwealth policies on nondiscrimination and prohibition of sexual harassment. Violations of the Commonwealth's policies through the use of IT Resources will be treated in the same manner as other violations.
- k. Authorized Users are to be aware of the dangers associated with driving while using wireless communication devices.** Driving while using wireless communication devices can distract a driver's attention from the primary job of responsible driving. Authorized Users are required to obey all local, state, and federal laws related to the use of wireless communication devices while driving.
- l. 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.
- m. 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.

- n. **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.
- o. **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.
- p. **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 535.09 *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, Information Technology (OA/OIT), via 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 Amended, dated February 18, 2021.

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 Amended, 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, contracting officer or the Pennsylvania Office of State Inspector General (OSIG).

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 Amended, The Commonwealth of Pennsylvania State Records Management Program*

and *Manual 210.09 Amended, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*, specifically 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 Amended, The Commonwealth of Pennsylvania State Records Management Program and Manual 210.09 Amended, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*, specifically items *G001.021, Transitory Records and G001.025, Transitory Files Confidential*.

11. ACCEPTABLE USE OF VIDEO SHARING SERVICES

Authorized Users shall ensure that:

- a. Video Sharing Service applications are only used to conduct Commonwealth business.
- b. Approval is received for the use of Video Sharing Services by the appropriate Agency Head.
- c. Only authorized Video Sharing Services are connected to IT Resources and associated with Commonwealth user accounts.
- d. Authorized Video Sharing Services are to be approved by the appropriate Agency Heads prior to access and use.
- e. Proper access controls and processes are put in place to govern the sharing of videos. If required, encrypt video content so that unauthorized users cannot access or manipulate content.
- f. Consultation with Legal Counsel and/or Privacy Officer in obtaining the owner's permission and approval before transmitting, using, or soliciting any proprietary material such as copyrighted software, publications, audio or video files, as well as trademarks or service marks.
- g. Any content produced, shared and published must not leak intellectual property, sensitive communications, or information/data with the designation of "C" classification as outlined in *ITP-SEC019, Policy and*

Procedures for Protecting Commonwealth Electronic Data.

- h.** Creation of content using a Video Sharing Service that includes Commonwealth content and information that is intended for distribution to the public shall be reviewed and authorized by the appropriate agency personnel and shall comply with *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and *Management Directive 220.1 Amended, Commonwealth Media Services*, prior to distribution.
- i.** All individuals and parties participating in the creation of video streaming content must obtain consent for any and all facilitators who may opt to speak orally or be video recorded during the presentation.

12. RECORDING CONSENT

Authorized Users or third-party presenters shall do the following when meetings, presentations or webinars are being recorded:

- a.** Prior to the Start of the Recording/Webinar:
 - Globally mute all participants
- b.** After the Start of the Recording/Webinar:
 - Indicate that "This session is being recorded. By participating in this session, you are consenting to the recording, retention and use of this session."
- c.** Prior to the Start of any Question-and-Answer Session:
 - Remind the participants that the session is being recorded and by asking a question verbally, they are consenting to the recording, retention and use of their statements as part of the session.
- d.** A Conspicuous Notice shall be Included and Posted during the meeting in a manner that makes it obvious that the meeting, presentation, or webinar is being recorded.

Authorized Users should consult with their Agency legal office with any questions regarding recording or consent to record.

13. 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.

14. 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 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 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 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.

15. EMAIL USE

a. Usage

- i. 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).
- ii. Authorized Users shall understand that messages can be quickly and easily copied and may be forwarded inappropriately.
- iii. 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.
- iv. 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).
- v. 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.
- vi. The agency head or designee shall determine if data can be shared, and the means by which it can be shared (e.g., based on the classification of data or regulation associated with it).
- vii. 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.
- viii. 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.
- ix. 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.
- x. 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

- i. Only Authorized Users may use IT Resources to send or view email or access the Commonwealth's email systems.
- ii. 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.
- iii. 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.
- iv. 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 emails through 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 Amended, 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:

- i. Be courteous and remember that you are representing the Commonwealth with each email message sent.
- ii. Review each email message before it is sent and make certain

that addresses are correct and appropriate. Use spell check before sending.

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

16.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 in any medium 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.

17. 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-RA SecurityIncidents@pa.gov. Report phishing emails by using the Cofense Reporter button in your Outlook ribbon or within additional email options on your Commonwealth issued mobile device.

18. 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 Amended, 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 Amended, 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 #: _____

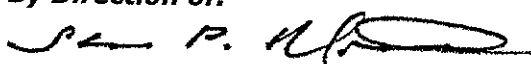
Mailing Address: _____

Email address: _____

Work Phone: _____

MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania Governor's Office

Subject: The Commonwealth of Pennsylvania State Records Management Program	Number: 210.5 Amended
Date: October 31, 2017	By Direction of:  Sharon P. Minnich, Secretary of Administration
Contact Agency: Office of Administration, Office of Continuity and Records Information Management (OCRIM), Telephone 717.783.5055	

This directive establishes policy, responsibilities, and guidance for records management, including records created in electronic messaging systems. This amendment revises the Purpose, Scope, Objectives, Definitions, Policy, and Responsibilities sections. Marginal dots are excluded due to major changes.

- 1. PURPOSE.** To establish policy, responsibilities, and guidance for the State Records Management Program, including paper, electronic records and other formats.
- 2. SCOPE.** Applies to all agencies subject to *The Administrative Code of 1929*, agencies and offices under the Governor's jurisdiction, and entities that store records at the State Records Center (SRC). Other state entities are encouraged to follow this directive.
- 3. OBJECTIVES.** To provide guidance, definition, and documentation of policies to ensure that:
 - a.** All current employees and departing employees are aware of their responsibilities for appropriate records management;
 - b.** All records are identified and scheduled on File Plans and approved records retention and disposition schedules;

- c. All records are managed, retained, and disposed of in conformance with approved records retention and disposition schedules;
- d. Permanent/archival records are identified and transferred to the State Archives as soon as the records are no longer active;
- e. Vital records are properly identified and protected; and
- f. All records are managed efficiently, minimizing the cost of doing government business while assuring access.

4. DEFINITIONS.

- a. **Active Records.** Records used to conduct current operations.
- b. **Agency File Plan.** A tool used by agency employees to manage their records in accordance with general and agency specific records retention and disposition schedules that provides bureau/office guidance to include bureau/office-specific record retention, disposition, record location, media type, and a designated record custodian, to ensure that all agency employees properly manage records under their care and control.
- c. **Agency Open Records Officer (AORO).** The official or employee designated by the agency head to receive and respond to *Right-to-Know Law* (RTKL) requests.
- d. **Agency Records Coordinator.** The employee appointed by the agency head to have agency-wide responsibility for managing and coordinating the agency's records management program. See *Manual 210.7, State Records Management Manual*.
- e. **Agency Records Legal Liaison.** Agency counsel assigned by the Agency Chief Counsel to provide legal guidance to the Agency Records Coordinator and AORO with RTKL responses and to assist with records issues.
- f. **Continuity of Operations (COOP).** Efforts within individual agencies to ensure that their critical functions continue during a wide range of emergencies and disruptions including, for example, localized acts of nature, accidents, and technological or attack-related emergencies. COOP activities include plans and procedures to ensure that critical functions are performed; testing, training, and exercising ensuring a viable COOP capability; managing agency response during a disruption; and continuing and/or resuming agency critical functions throughout a disruption.
- g. **Data.** Symbols or representations of facts, or ideas that can be communicated, interpreted, or processed by manual or automated means, and often associated with electronic data or with statistics or measurements.
- h. **Disposition.** The changing of custody, location, or existence of records including transfer to the SRC; transfer of permanently valuable records to the State Archives; transfer of electronic records to a different storage system; or destruction.

- i. **Disposition Code.** A code used to direct the final disposition of records. Records must be disposed of in accordance with the assigned disposal code listed on approved records retention and disposition schedules. For specific details, refer to *Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*.
- j. **Electronic Messages.** Information that is created, stored, and delivered in an electronic format. Types of electronic messages may include the following: email, text, discussion threads, digital voice mail, blogs, and message boards.
- k. **Electronic Record.** A record created, generated, sent, communicated, received, or stored by electronic means.
- l. **Enterprise Records Management System (ERMS).** The electronic system that the Pennsylvania Historical and Museum Commission (PHMC) uses to manage all commonwealth records retention and disposition schedules.
- m. **Executive Board.** The Executive Board consists of the Governor, as Chairman, and six other heads of departments. It has the power and authority in the administrative and executive functions directed to be performed under provisions of §506 of *The Administrative Code of 1929*.
- n. **Human-Readable Format.** The representation of information that can be read with the human eye and does not require machine (computer) assistance. Printed material, microfilm and microfiche are examples of human readable format. For purposes of this policy, 'human-readable format' also includes any electronic format designated by the PHMC as an appropriate substitute.
- o. **Inactive Records.** Records that are not needed for ongoing agency business or that are accessed relatively infrequently, but whose retention period has not yet expired.
- p. **Information System.** The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.
- q. **Long-term records.** Records that must be maintained for ten years or more.
- r. **Non-records.** Information that does not meet the definition of a record as defined in this Management Directive. These materials relate to non-government business or activities and may include items such as announcements of community events and personal emails. Non-records may also include publications such as trade journals, pamphlets, and reference materials received from outside organizations, conferences, and workshops.
- s. **Official Records.** Records that reflect the position or official business of an agency and that are to be retained by a designated record custodian in accordance with the appropriate records retention and disposition schedule.
- t. **Pennsylvania State Archives.** The Pennsylvania State Archives collects, preserves and makes available for study the permanently-valuable public records of the commonwealth, with particular attention given to the records of state government.

- u. Permanent/Archival Records.** Records appraised by the PHMC as having sufficient historical, administrative, or legal value to warrant continued preservation by the commonwealth.
- v. Preservation of Records.** The process and procedures used to ensure historical records are kept from harm, injury, decay, or destruction while remaining accessible.
- w. Record.** Information, regardless of physical form or characteristics, that document a transaction or activity of an agency and that is created, received, or retained pursuant to law or in connection with a transaction, business or activity of the agency. The term includes a document, paper, letter, map, book, tape, photograph, film or sound recording, information stored or maintained electronically, and a data-processed or image-processed document.
- x. Record Custodian.** Any person having custody, possession, or control of a record.
- y. Record-Keeping Requirements.** The prerequisites needed to manage records regardless of format, throughout the creation, maintenance, and disposition of a record.
- z. Records Legal Hold.** The suspension of ordinary practices and procedures for disposing of records, as necessary, to comply with existing preservation obligations related to actual and reasonably anticipated litigation, government investigation, or audit.
- aa. Records Management.** The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition, in order to achieve adequate and proper documentation of the policies and transactions of the commonwealth for an effective and economical management of agency operations.
- bb. Records Retention and Disposition Schedules.** A comprehensive statement approved by the Executive Board showing retention periods and all actions to be taken with respect to disposition of records. The schedule lists each record series, indicates length of time each series is to be maintained in a prescribed format, and the location where the records are to be stored. There are two types of records schedules used by state agencies to control records: general and agency-specific. General schedules identify record series common to most agencies. Agency-specific schedules identify unique record series created by an agency.
- cc. Record Series.** A group of records that may be treated as a unit for purposes of classification, designation, description, management, or disposition because they relate to a particular subject or function, result from the same activity, have a particular physical form, or because of some other relationship arising out of their creation, receipt, or use.
- dd. Senior Management Employee.** An agency head, deputy secretary or equivalent, chief counsel, bureau director or equivalent and members of boards or commissions.

- ee. Series or Item Number.** A unique number assigned to designate a record series when creating or revising a records retention and disposition schedule.
- ff. State Records Center.** The State Records Center (SRC) is a low-cost, high density, secure storage for semi active and inactive records of state agencies.
- gg. Transitory Records.** Records that have little or no documentary or evidential value and that need not to be set aside for future use; have short term administrative, legal, or fiscal value and should be disposed of once that administrative, legal or fiscal use has expired; or are only useful for a short period of time, perhaps to ensure that a task is completed or to help prepare a final product. For more detail, refer to *Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*.
- hh. Vital Records.** Records needed to support critical functions during a COOP event, to recover full operations following an emergency or disruption, and to protect the legal rights and interests of citizens and government. The two basic categories of vital records are emergency operating records (e.g. plans and directives, orders of succession, delegations of authorities and staffing assignments) and legal and financial records.

5. POLICY.

- a. Employees and Records Management.** All Commonwealth of Pennsylvania employees are to manage records under their care and control on an ongoing basis to ensure proper records management, retention, and disposition.
 - (1) Employee Orientation.** New or transferred employees are to review the policies, responsibilities, and procedures in this Management Directive and *Manual 210.1, The Commonwealth of Pennsylvania Employee Records Management Manual*.
 - (2) Employee Separation.** The departing employee will work with their manager and/or supervisor to verify that the appropriate records remain with the agency, pursuant to records retention and disposition schedules, including email records, and shall do the following:
 - (a)** Consult with the Agency Records Coordinator in determining proper disposition of records;
 - (b)** Ensure that agency records under the control of the departing employee, including emails and other electronic records, are transferred to the control of the supervisor (i.e. moved from the network drive of the employee to the network drive of the supervisor or that paper records are left in the office of the departing employee) or otherwise retained for the successor employee following appropriate records retention and disposition schedules;
 - (c)** Have an agency designated representative review requests for employees to copy records for personal use or to remove non-records in the employee's custody;

- (d) Notify the departing employee of the results of such review and direct what records may be copied and what non-records may be retained by the employee. The employee may appeal the decision of the supervisor to the Agency Chief Counsel or designee; and
- (e) Comply with restrictions on the copying or destruction of records that may be subject to a litigation hold, audit reporting requirements, confidentiality provisions, archival review, or other considerations noted in the appropriate general or agency-specific records retention and disposition schedules.

(3) Separation of Senior Management Employees. Senior Management Employees are to comply with the direction set forth in Section 5(a)(2), above. The following additional measures apply to ensure that records are not inappropriately taken upon departure. The Agency Chief Counsel or a person delegated by the Chief Counsel is to verify in writing both to the agency head and to the General Counsel, or their designees, at least seven business days prior to the departure of any Senior Management Employee, that the employee has been advised as follows:

- (a) That the Senior Management Employee shall provide to the agency head and the General Counsel, or their designees, at least five business days prior to departure, a written summary of any records remaining in the employee's sole possession or control, as of that time, and any records that the employee wishes to retain for personal use after departure;
- (b) That a decision as to which records the Senior Management Employee may retain after departure shall be made by the agency head and General Counsel, or their designees; and
- (c) That the Senior Management Employee shall notify the Agency Chief Counsel of and provide to that office any records either designated as necessary for litigation purposes or that are reasonably likely to be subject to litigation, investigations, subpoenas, or discovery requests.

Note: Managers, supervisors, and employees should refer to *Manual 210.1, The Commonwealth of Pennsylvania Employee Records Management Manual* to ensure adequate knowledge of records management requirements.

- b. **New Record Types.** During the creation of a new document or electronic system that contains agency data and/or records, the agency shall conduct an analysis to determine the format, retention requirements, and value of the record (vital, permanent, non-permanent, etc.) at each stage. Upon completion of the records analysis, new record types should be added to the Agency File Plan and/or to the agency-specific records retention and disposition schedule.

c. Records Maintenance and Use.

- (1) All records, regardless of format, must be identified and maintained in accordance with general and agency-specific records retention and disposition schedules.
- (2) Each email message must be categorized and classified according to its content.
 - (a) Since email is a method or a tool for communicating, a blanket retention for "Email Records" does not exist.
 - (b) Employees should ensure that priority is given to the classification of email messages whose retention periods have not been met and that all others are routinely deleted.
- (3) As part of the normal course of doing business for records management purposes, electronic format(s) may be used in lieu of hard copy. Resulting format(s) must be retained in accordance with general and agency-specific records retention and disposition schedules and provide for the retention of a hard copy as may be required for long-term records.
- (4) Appropriate measures must be taken to maintain confidentiality of records in order to protect the privacy of individuals, employees, taxpayers, clients, or service recipients.
- (5) All retention periods in the general and agency specific records retention and disposition schedules are to reflect at least the minimum legal, fiscal, and administrative (operational) business requirements.
- (6) Electronic records, including electronic messages, designated by the PHMC as having permanent/archival value, shall be maintained in human-readable format, as well as any other media types or format. The creating agency shall retain the records permanently or until such time as they may be scheduled for transfer to the State Archives.
- (7) All commonwealth records must be maintained in such a way that they are readily retrievable, in facilities that provide a suitable environment to protect them from damage, deterioration, and loss, and are in compliance with the applicable records retention and disposition schedules.
- (8) Records, including inactive records, are to be accessible within five business days, to allow for a timely response to any RTKL request.

- d. Inactive Records Storage.** Inactive records must be stored so records are readily retrievable, in facilities that provide a suitable environment to protect them from damage, deterioration, or loss.

(1) **SRC Storage Fees.** Agencies with inactive records stored at the SRC shall pay a storage fee to support the SRC operations and services based on a per box charge. The SRC does not charge additional fees for disposal or retrieval. In instances where records are removed from SRC storage, in accordance with an Executive Board approved records retention and disposition schedule, removal will coincide with SRC's normal disposal cycle. The SRC storage fee shall be payable annually and be based on a computation as follows:

(a) SRC Operating Costs/Service Data (boxes stored) = Annual Service Rate (ASR).

(b) ASR x Agency Usage (boxes stored by each agency) = Agency Billing Amounts.

(2) **SRC Retention.** Agencies with records scheduled for retention at the SRC may not store these records in another location without submitting a records action to amend the retention of the record series.

(3) **Agency Obligations for non-SRC Storage of Inactive Records.** Executive Board approval of an agency records action seeking non-SRC storage shall be contingent upon a demonstration that the storage facility complies with requirements set by the PHMC, which are published on the PHMC web site. The fees for such storage must be lower than fees for storage at the SRC or there must be another compelling reason for using an alternate storage location.

e. Disposition.

(1) Records are to be disposed of according to applicable disposition codes provided by the appropriate records retention and disposition schedule.

Note: Records subject to a records legal hold or that are reasonably likely to be involved in litigation shall not be disposed of without approval from Agency Chief Counsel. Consult with your Agency Records Legal Liaison for direction.

(2) Disposition actions should be appropriate to the media upon which the records reside, agency business needs, record's security classification, and archival value.

(3) Unscheduled records cannot be destroyed until approval is received from the Executive Board and the PHMC.

f. Records Legal Hold. Agencies are to establish and uphold policies and procedures in coordination with the Agency Records Legal Liaison for records legal hold to ensure that the records will not be destroyed or reformatted until the event resulting in the records legal hold has concluded and all appeal periods are exhausted.

(1) Procedures must include the preparation of reports or lists identifying such records and the circulation of this information to all agency employees that may hold the records subject to records legal hold.

- (2) Records involved in a record legal hold must be retained for the duration of the legal action, even if the records exceed the relevant records retention and disposition schedule requirements.
- g. Discovery and Disclosure.** Agencies are to establish and update policies and procedures in coordination with Agency Records Legal Liaison, Agency Records Coordinator, and Agency Chief Information Officer to process discovery and disclosure requests, including RTKL requests, for commonwealth records that include policy and procedures:
- (1) Identifying employee roles in the process.
 - (2) Notifying employees of a records legal hold.
 - (3) Providing for the redaction of sensitive and/or non-public information from records.
- h. Electronic Messaging System.** Records maintained in an electronic messaging system must be managed appropriately based on their content.
- (1) Records created in electronic messaging systems must be retrievable and available for the retention period listed on the appropriate, approved records retention and disposition schedules.
 - (2) Messages in the in-box should be limited to very short term transitory messages with a retention value of three months or less.
 - (3) Messages with a permanent retention, a retention period of ten years or more, or which may be archival (disposal code of 2 or 4) can be printed or maintained according to Section 5(c)(6) in this Management Directive.
- i. State Records Management Performance Program.** The State Records Management Performance Program is to be administered by OCRIM and provide for policy review, assessments tools, and methods for examination of state agency records management programs to ensure state agencies are sufficiently capturing and managing records that document commonwealth business.
- (1) **Review.** OCRIM shall review the State Records Management Program policies and procedures and records retention and disposition schedules to determine the degree to which outcomes defined in the program are met.
 - (2) **Assessment.** Through various survey instruments, on-site interviews, agency file plan review, and agency records management self-assessment results, OCRIM shall assess state agency records management programs for evidence of proficient performance.
 - (3) **Performance Standards.** These standards will be used as the criteria in evaluating proficient performance.
 - (a) Records are maintained and disposed of in accordance with valid records retention and disposition schedules.

- (b) Agency has evidence of internal policies, training, and procedures for managing agency records.
- (c) Records are retrieved in a reasonable amount of time.
- (d) Agency records management programs are managed and planned with the involvement and support of agency heads, senior management, Agency Records Coordinator, Records Legal Liaisons, Agency COOP Manager, and IT Managers and CIOs.

j. Use of Management Directive. This Management Directive should be used in conjunction with *Executive Order 1992-1, Records Management, Administrative Code of 1929, the History Code (Title 37 of Pennsylvania Code)*, other related Management Directives, Manuals, Information Technology Policies and applicable provisions of the *Pennsylvania Right-To-Know-Law, 65 P.S. § 67.101, et seq.*

6. RESPONSIBILITIES.

a. The Secretary of Administration shall issue all directives (i.e. Management Directives, Manuals and General Records Retention and Disposition Schedules) regarding the State Records Management Program.

b. OCRIM shall:

- (1) Administer the State Records Management Program as designated by the Secretary of Administration, by working collaboratively with agencies to draft policies, standards, and procedures to control the creation, use, maintenance, transfer, scanning, preservation, and retention and disposition of records.
- (2) Administer and audit the State Records Management Performance Program.
- (3) Advise the Secretary of Administration on the development of policies and procedures and on the overall administration and evaluation of the State Records Management Program.
- (4) Collaborate with the Executive Director of the PHMC on the development of policies and procedures that may affect the implementation of the State Records Management Program.
- (5) Issue reports, as needed, on the results of the State Records Management Program reviews, including the compliance of specific agencies, and on the overall effectiveness of the State Records Management Program.
- (6) Conduct studies, as needed, pursuant to *Section 527 of The Administrative Code of 1929*, of the accumulation of records in the possession of agencies.

- (7) Serve, in coordination with the Office of Administration, Office for Information Technology (OA/OIT) and the PHMC as a central clearinghouse for information on the State Records Management Program.

c. PHMC shall:

- (1) Work with OCRIM to regularly assess and seek to improve records management procedures, guidelines, and standards.
- (2) Work with agencies on the development of records inventories and recommend appropriate retention periods and disposition to be submitted to the Executive Board.
- (3) Appraise agency records for permanent or historical value and work with agencies to preserve these records. Upon agreement by the agency and the PHMC, transfer records to the State Archives.
- (4) Be responsible for the designation, management, and preservation of records of permanent or historical value.
- (5) Train Agency Records Coordinators and Agency Records Legal Liaisons in records management practices.
- (6) Work with the Office of Administration, Office of Human Resources Management, to develop records management training for state employees other than Agency Records Coordinators and Agency Records Legal Liaisons.
- (7) Administer the Enterprise Records Management System (ERMS).
- (8) Manage the SRC to provide adequate safety, security, and space for storage of inactive commonwealth records, regardless of format. Management of the SRC includes setting fees; administering information systems used to manage or preserve inactive records; training agency employees who interact with such systems; and other activities required to effectively manage inactive records.
- (9) Approve agency storage of inactive commonwealth records at facilities other than the SRC and establish minimum requirements for such facilities.
- (10) Determine the formats for storage of inactive and archival records that are stored by agencies or by the PHMC.

d. The Executive Board shall:

- (1) Review and approve the general and agency-specific records retention and disposition schedules.
- (2) Review and approve requests for microfilming of records.

e. Agency Heads shall:

- (1) Ensure that an agency records management program is established and maintained.
- (2) Appoint an Agency Records Coordinator, according to guidelines provided in *Manual 210.7, State Records Management Manual*, to have agency-wide responsibility for managing and coordinating the agency records management program.
- (3) Provide for all necessary support, staff, and agency authority for the Agency Records Coordinator to carry out designated records management responsibilities.

f. Agencies shall:

- (1) Be responsible for supporting agency employees in developing and adhering to the agency records management program.
 - (a) Delineate record and non-record information within the agency.
 - (b) Outline program responsibilities.
 - (c) Oversee management of agency records.
- (2) Ensure that employees are trained and comply with requirements, policy, and procedures for the State Records Management Program.
- (3) Ensure that electronic records, including electronic messages, are:
 - (a) Organized and maintained in such a manner as to ensure accessibility over time in order to meet business/legal requirements, technology migration requirements, and user expectations.
 - (b) Maintained in such a way to preserve the integrity of electronic records, including electronic messages along with attachment(s) in a safe and secure environment.
 - (c) Retained following an approved commonwealth records retention and disposition schedule; non-records should be deleted immediately and transitory records should be deleted once their short-term business value has ended.
 - (d) Reviewed regularly to determine retention requirements and compliance with disposal codes.
 - (e) Appropriately maintained for those records designated by the PHMC as having permanent/archival value. This shall include provision for maintenance of such records in human-readable format. The creating agency shall retain the records permanently or until such time as they may be scheduled for transfer to the State Archives.


- g. Agency Chief Counsel** shall report to the General Counsel in compliance with the section of this Management Directive regarding departing Senior Management Employees.

7. Related Guidance/References.

- a.** Agency Records Coordinators shall manage commonwealth records using the procedures set forth in *Manual 210.7, State Records Management Manual*.
- b.** Agency Records Coordinators shall manage vital records using the guidelines provided in *Manual 210.8, Vital Records Disaster Planning*.
- c.** Agency employees are to create and maintain their individual records in accordance with procedures and instructions issued through *Manual 210.1, The Commonwealth of Pennsylvania Employee Records Management Manual*.
- d.** Agencies must comply with the RTKL as indicated in *Management Directive 205.36, Right-to-Know Law Compliance*.
- e.** Authorized Users that have access to commonwealth IT Resources must comply with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Use Policy*.
- f.** Agency employees should use this management directive in conjunction with Executive Order 1992-1, Records Management and Sections 506 and 527 of the Administrative Code of 1992.
- g.** For storing long-term records in electronic formats, agencies must follow Guidance for Policy Regarding Agency Long Term Records in Electronic Format and Policy on Preservation of Electronic Records Retained Permanently by an Agency (and Exception to PDF/A).
- h.** Information Technology Policies should be referenced on OA's IT Policy page at <http://www.oa.pa.gov/Policies/Pages/itp.aspx>.

This directive replaces, in its entirety, Management Directive 210.5, dated July 29, 2010.

MANUAL
Commonwealth of Pennsylvania
Governor's Office

Subject: The Commonwealth of Pennsylvania Employee Records Management Manual	Number: Manual 210.1 Amended
By Direction of:  Naomi Wyatt, Secretary of Administration	Date: May 20, 2010
Contact Agency: PA Office of Administration, Office of Enterprise Records Management, Telephone 717-783-5055	

This manual is designed to assist employees in organizing, maintaining, and disposing of records created and used in day-to-day operations.

The authority for this manual is derived from Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.

PA Office of Administration
Office of Enterprise Records Management
613 North Street
Room 311, Finance Building
Harrisburg, PA 17120-0400
Records & Directives
E-mail: OA, Enterprise Records Management
Telephone: 717-783-5055
Fax: 717-787-0776

This manual replaces, in its entirety, Manual 210.1, Guide to Efficient Filing, dated July 21, 1976.

TABLE OF CONTENTS
SECTION ONE: OVERVIEW

1.1 OVERVIEW..... 1

SECTION TWO: KEY DEFINITIONS

2.1 ACTIVE RECORDS..... 2
2.2 AGENCY FILE PLAN 2
2.3 AGENCY RECORDS COORDINATOR..... 2
2.4 AGENCY RECORDS LEGAL LIAISON 2
2.5 AGENCY RECORDS LIAISON(S)..... 2
2.6 CONTINUITY OF OPERATIONS/VITAL RECORDS..... 2
2.7 DISPOSITION 2
2.8 INACTIVE RECORDS..... 2
2.9 NON-RECORDS..... 2
2.10 RECORD 3
2.11 RECORD SERIES..... 3
2.12 RECORDS RETENTION AND DISPOSITION SCHEDULE 3
2.13 TRANSITORY RECORDS..... 3

SECTION THREE: EMPLOYEE RESPONSIBILITIES

3.1 RECORDS RETENTION AND DISPOSITION SCHEDULES 4
3.2 AGENCY FILE PLANS 4
3.3 ELECTRONIC RECORDS AND ELECTRONIC MESSAGING SYSTEMS 5
3.4 RECORDS LEGAL/AUDIT HOLD..... 6
3.5 RECORDS REQUESTED UNDER THE RIGHT-TO-KNOW LAW 6

SECTION FOUR: ADDITIONAL RECORDS MANAGEMENT TOPICS

4.1 CONTINUITY OF OPERATIONS/VITAL RECORDS..... 7
4.2 DEPARTING EMPLOYEES 8

SECTION FIVE: AUTHORITY

SECTION SIX: RESOURCES

SECTION ONE: OVERVIEW

1.1 Overview.

This online manual is intended to assist employees in organizing, maintaining, and disposing of records created and used in day-to-day operations, in accordance with *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*¹.

Information related to the business of an agency is a record and must be retained and disposed of in accordance with approved retention and disposition schedules. All records must be kept for an assigned period of time, which is the retention period. Records must also be disposed of properly, which is the disposition schedule. No record may be disposed of without being on an approved records retention and disposition schedule. Please note that records may be in any format, not just paper.

Each agency has an Agency Records Coordinator and an Agency Records Legal Liaison to assist employees, including field offices, with understanding and implementing the agency records management program. Some agencies may also have Agency Records Liaison(s) to support the Agency Records Coordinator and Agency Records Legal Liaison. If you are unsure about your agency's records management program or records staff, please contact the Pennsylvania Historical Museum Commission at RA-StateRecordsMgmt@pa.gov to obtain the name of your Agency Records Coordinator.

¹ Agency Records Coordinators should refer to *Manual 210.7, State Records Management Manual* for specific responsibilities, procedures and instructions.

SECTION TWO: KEY DEFINITIONS

- 2.1 Active Records.** Records that are used to conduct current operations.
- 2.2 Agency File Plan.** A tool used by employees to manage their records in accordance with the General and/or Agency-Specific Records Retention and Disposition Schedules. The Agency File Plan provides specific guidance to bureaus and offices to ensure that all employees properly manage records under their care and control.
- 2.3 Agency Records Coordinator.** The employee appointed by the agency head to have agency-wide responsibility for managing and coordinating the agency's records management program. See Manual 210.7, State Records Management Manual.
- 2.4 Agency Records Legal Liaison.** The agency attorney designated by the agency Chief Counsel to provide legal guidance to the Agency Open Records Officer and Agency Records Coordinator on the agency's response to a Right-to-Know Law request.
- 2.5 Agency Records Liaison(s).** Employee(s) responsible for assisting the Agency Records Coordinator with managing and coordinating bureau/office records within an agency.
- 2.6 Continuity of Operations/Vital Records.** Records needed to support critical functions during a Continuity of Operations event, to recover full operations following an emergency, and to protect the legal rights and interests of citizens and government. The two basic categories of vital records are emergency operating records (e.g. plans and directives, orders of succession, delegations of authorities and staffing assignments) and legal and financial records.
- 2.7 Disposition.** Disposition occurs when records change custody, location, or cease to exist. Records at the end of their retention period may be sent to the State Archives or be shredded or recycled, depending on the disposition given for those records.
- 2.8 Inactive Records.** Records that are not needed for ongoing agency business or that are accessed relatively infrequently, but whose retention period has not yet expired.
- 2.9 Non-Records.** Information that does not meet the definition of a record. These materials relate to non-state government business or activities and may include items such as announcements of community events and personal e-mails. Non-records may also include publications such as trade journals, pamphlets, and reference materials received from outside organizations, conferences, and workshops. Non-records may be disposed of at the convenience of the agency when they have no more value or use to the agency. The following are examples of non-records:
- blank forms, publications, etc., which are outdated or superseded;
 - preliminary drafts of letters, reports, and memoranda which do not represent significant basic steps in preparation of record documents;

- shorthand notes, stenography tapes, mechanical recordings which have since been transcribed, except where noted on the Agency-Specific Records Retention and Disposition Schedule;
- routing and other interdepartmental forms which do not add any significant material to the activity concerned; and
- form and guide letters, sample letters, form paragraphs, vendor product information packets and brochures.

2.10 Record. Information, regardless of physical form or characteristic, that documents a transaction or activity of an agency and that is created, received or retained pursuant to law or in connection with a transaction, business or activity of the agency. The term includes documents, papers, letters, maps, books, tapes, photographs, film or sound recordings, information stored or maintained electronically, and data- or image-processed documents.

2.11 Record Series. A group of records that may be treated as a unit for purposes of classification, designation, description, management, or disposition because they relate to a particular subject or function, result from the same activity, have a particular physical form, or because of some other relationship arising out of their creation, receipt or use.

2.12 Records Retention and Disposition Schedule. A comprehensive statement approved by the Executive Board showing retention periods and all actions to be taken with respect to disposition of records. The schedule describes the contents of each record series and defines: 1) the length of time each series is to be maintained in a prescribed format, such as paper or electronic; 2) the location where the records are to be stored, and; 3) the final disposition of the records (shredded, deleted or sent to the State Archives). There are two types of records retention and disposition schedules used by state agencies to control records: general and agency-specific. The General Records Retention and Disposition Schedule identifies record series common to most agencies. The Agency-Specific Records Retention and Disposition Schedule identifies unique record series created by an agency.

2.13 Transitory Records. Records that have little or no documentary or evidential value and that need not to be set aside for future use; have short term administrative, legal or fiscal value and should be disposed of once that administrative, legal or fiscal use has expired; or are only useful for a short period of time, perhaps to ensure that a task is completed or to help prepare a final product. For more detail refer to Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule.

Additional definitions are available in Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.

SECTION THREE: EMPLOYEE RESPONSIBILITIES

Employees are responsible for knowing the policy and procedures for maintaining records under their purview. Employees should work with their assigned Agency Records Coordinator, Agency Records Liaison(s), and/or supervisor or manager to ensure that records in any format, including paper and electronic, are maintained and disposed of in accordance with the Agency File Plan.

3.1 Records Retention and Disposition Schedules.

Records retention and disposition are terms used to define the amount of time to retain records and the means of disposing of records. The Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule controls the retention and disposition of records relating to common functions performed by or for most state agencies. It provides uniformity when similar records are found in numerous agencies. The Agency-Specific Records Retention and Disposition Schedule relates to records particular to a specific agency. They are prepared by agencies to control program-specific records not covered by the General Records Retention and Disposition Schedule.

All records are covered by the General and/or Agency-Specific Records Retention and Disposition Schedule. Employees are responsible for managing their records in compliance with the appropriate records retention and disposition schedule items listed on the Agency File Plan. The Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule is located on Pennsylvania Historical Museum Commission's Web site under state records management. The Agency Records Coordinator, Agency Records Liaison(s), and/or supervisor or manager is available to provide guidance and assistance to employees with reading and applying a general records retention and disposition schedule and with managing records under their care and control.

3.2 Agency File Plans.

The Agency File Plan is the primary tool for employees to manage and track state records. The Agency File Plan includes all records series from the General and/or Agency-Specific Records Retention and Disposition Schedules.

Each Agency File Plan is to be kept current by employees in coordination with the Agency Records Coordinator, Agency Records Liaison, and/or supervisor or manager. The Office of Administration's Office of Enterprise Records Management reviews each Agency File Plan every five years. For guidance, assistance, or a sample format of an Agency File Plan, contact your Records Coordinator.

The Agency File Plan should include the following:

- **Record Name.** A title by which the record series is commonly known or referenced;
- **Record Series Description.** A description of the record series that includes enough detail for employees to understand the purpose and use of the record;

- **Record Series Item Number.** This number is the unique identifier listed on the General and/or Agency-Specific Records Retention and Disposition Schedules that identifies the specific record series;
- **Record Format.** Is the same as the media code found on records retention and disposition schedules and denotes the format of the record. For example paper, microfilm, electronic, multi-media (paper and electronic);
- **Record Location.** The site where the record series is maintained. For example: file cabinet in Joe Smith's office, building/room number, or human resources network drive folder;
- **Vital Record.** If a record series is listed on the agency Continuity of Operations plan, then this should be noted in your Agency File Plan;
- **Record, Official Copy or Reference Copy.** Indication of whether it is the official record or simply a copy of the record;
- **Public Access Exemptions.** Designation of exempt and legal justification for any exemption from disclosure under the Right-to-Know Law or other public access;
- **Date of Record.** General date or instructions to trigger the beginning of the retention period. For example: close of contract; end of month; fiscal year; case closed;
- **Retention Period.** The total amount of time that a record is maintained no matter where it is located;
- **Series Cut-off.** Calendar year, fiscal year, and other;
- **Disposition Instructions.** Instructions for what to do with the record series when the retention period is met;
- **Custodian of Record.** The name and related contact information of the employee responsible for the maintenance of the record series.

3.3 Electronic Records and Electronic Messaging Systems.

Electronic records and records from electronic messaging systems (email) are managed in a similar fashion to paper records by using electronic file folders. The retention and disposition of electronic records is based on the content, not format, of the record. The key to electronic records management is consistent filing and naming conventions and managing content upfront, so that non-records are not maintained with records.

Email management includes daily review of email records to dispose of non-records and transitory records, both sent and received, and to keep other electronic records in folders or locations from which they can be readily identified and retrieved. Electronic records should be stored and archived in accordance with the appropriate records retention and disposition schedule.

3.4 Records Legal/Audit Hold.

Records involved in a record legal/audit hold must be retained for the duration of the legal action/audit, even if the record exceeds the relevant records retention and disposition schedule requirements. No records related to known investigations, litigation, or audit holds may be destroyed without the approval of the Agency Records Legal Liaison. If an employee knows that records are involved in litigation or reasonably likely to be involved in litigation, any related records within the control of that employee must be retained and the employee should immediately consult with the Agency Records Coordinator, Agency Records Legal Liaison, Agency Records Liaison(s), and/or supervisor or manager to ensure proper retention and disposition of the records.

3.5 Records Requested Under the Right-to-Know Law.

The Agency Open Records Officer and the Agency Records Legal Liaison are to be consulted with regard to any records implicated in a Right-to-Know Law request. Records that are the subject of a current Right-to-Know Law request must be retained by the agency, even if their records retention and disposition schedule indicates otherwise. These records may not be destroyed during the duration of the active request, the appeal time related to the request, and any subsequent appeal related to the request. Employees should consult with the Agency Records Legal Liaison prior to the disposal of any records that have been requested under the Right-to-Know Law.

SECTION FOUR: ADDITIONAL RECORDS MANAGEMENT TOPICS

4.1 Continuity of Operations/Vital Records.

Vital or essential records are records that protect the legal rights and interests of citizens and government and are needed to continue operations both during and after an emergency. There are two basic categories of vital records:

- a. **Emergency Operating Records.** Records which are needed immediately by fire and safety personnel during the actual emergency and records which are needed by agency management and personnel assigned to disaster recovery efforts. Examples include blueprints, floor plans, special fire hazard records (including Material Safety Data Sheets and Hazardous Substance Survey Forms), utility records, emergency plans and directives, orders of succession, delegations of authority, staffing assignments, vital records inventories, employee telephone lists, contracts including maintenance agreements, lists of alternate location sites, inventories of fixed assets, and five-year plans covering automated technology, both hardware and software.
- b. **Legal and Financial Records.** Records which are needed by agency staff to continue mandated operations and services during and after the actual emergency and in order to preserve the legal and financial rights and interests of the agency and the individuals directly affected by its activities. Examples include forms used to provide services, insurance records, minutes, receipt and expenditure records, property and investment records, budgets, payroll and retirement records, articles of incorporation, current lists of clients, permits, and licensing records.

Employees in coordination with the Agency Records Coordinator, Agency Records Liaison(s), and/or supervisor or manager may be requested to identify vital records for the agency Continuity of Operations plan. It is important to remember that:

- Many records are considered important, however only a small percentage of the records are vital. In order for a record to be vital, it must be essential to emergency operations and to the organization's continuance, or be difficult or impossible to replace.
- Although records designated as permanent are often vital, the length of time a record is retained does not necessarily mean that the record is vital.
- Vital records may be in any format or medium. Original copies of the records are not necessary. It is the information, not the medium that is most important.

In addition to identifying records, employees may be asked to recommend ways in which vital records can best be protected to ensure that they are available in the event of a disaster. Three methods of protecting vital records are: duplication and dispersal, on-site storage, and off-site storage.

1. Duplication and Dispersal. Vital records can be protected by distributing duplicate copies created in paper, microfilm, or electronic format to locations other than the agency's primary office space. During the regular course of business, duplicates of vital records are often routinely distributed to other buildings or field offices. The duplicate records should be designated as vital records; maintained in the proper condition, and retained for the same length of time as the official record.

2. On-Site Storage. Vital records can be protected by storing on-site in fire-resistant vaults, safes, or file cabinets. Such equipment is rated according to the maximum number of hours of exposure to fire and maximum temperature at which they will protect records.

NOTE: The major disadvantage to on-site storage of vital records is the potential for total or near total destruction or contamination of a single facility in the event of a disaster.

3. Off-Site Storage. Vital records can be protected by storing them off-site if the reference rate is low, thereby eliminating the costs of duplication. An off-site storage facility should be located close enough for easy retrieval and updating of the records but far enough away from the primary space as to be unaffected by an area-wide disaster. Since these would constitute the original records, it is imperative that the storage facility has the proper environmental conditions and security systems in place.

For further guidance and resources, employees, through their supervisor or manager, should contact their Agency Records Coordinator.

4.2 Departing Employees.

Departing employees should notify their supervisor or manager as soon as possible after they become aware of separation or submit a resignation letter, to ensure that records are not inappropriately copied and taken; that others can access records that were formerly controlled by the employee; that records are not lost or inappropriately destroyed, and that the employee does not have access to agency records after the employee has departed. For Senior Management Staff, follow guidelines contained in Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.

SECTION FIVE: AUTHORITY

Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program guides the creation, use, maintenance and disposition of records. The program ensures that agencies subject to the *Administrative Code of 1929*, agencies under the Governor's jurisdiction, and entities that use the State Records Center apply policies and activities in a consistent manner that enables effective and transparent operations.

The Pennsylvania Office of Administration's Office of Enterprise Records Management manages and issues the Commonwealth of Pennsylvania's state records management directives, manuals and Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule; audits agency compliance and chairs the State Records Committee.

The Pennsylvania Historical and Museum Commission implements the Commonwealth of Pennsylvania's State Records Management Program and operates the State Records Center and the State Archives.

SECTION SIX: RESOURCES

[How to Read a Records Retention and Disposition Schedule – General Use](#)

[Applying Records Retention and Disposition](#)

[Sample File Plan Format](#)

[Email Management](#)

[Creating Electronic File Folders](#)

[Filing and Naming Electronic Records](#)

[Separation Guidelines \(separation from agency or state employment\)](#)

[Records Management Inventory: Employee Separation](#)

[Form for Agency Chief Counsel Regarding Departure of Senior Management Employees](#)