pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Commonwealth of PA System Logon Banner and Screensaver Requirements

ITP Number	Effective Date
ITP-SEC012	May 26, 2006
Category	**Supersedes**
Security	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	July 2022

1. Purpose

This Information Technology Policy (ITP) defines logon banner and screensaver requirements that shall be displayed on an Authorized User's computer system (laptop, desktop, etc.).

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Objective

To establish requirements for deploying a logon banner and screensaver for computers connecting to the Commonwealth's network.

4. Policy

Logon banners provide a definitive warning that network intrusion is illegal and provide Authorized Users with their obligations and responsibilities relating to their use of the Commonwealth's computer network. Thus, Authorized Users of the computer network can be held accountable for their actions since they have reviewed the logon banner warnings prior to logging into the computer network.

Screensavers provide helpful tips and tricks to Authorized Users regarding security awareness. These reminders act to reinforcement the annual security awareness training.

4.1 Logon Banners

Agencies shall use logon banners for all Authorized Users' computers that have the capability to display logon banners intended for logging into the Commonwealth network.

This policy does not apply to Commonwealth applications or other system logins (both public and internal).

Agencies may develop their own logon banners; however, every banner shall meet the following minimum requirements (NOTE: if not technically feasible to display an electronic login banner, a printed banner shall be placed on the workstation):

- Banners shall be displayed prior to log on or prior to use of the system.
- The Authorized User must be able to acknowledge the banner before access to the system is granted.
- Identifying information such as operating system, system configuration, or other internal matters are not to be provided on the banner until the user is authenticated. Identifying information may divulge confidentialinformation.
- The banner shall specify that the system is used for authorized use(s) only.
- Any deviation from the below required banner language must be approved by agency legal counsel prior to use.
- The logon banner shall specify that all activity may be monitored, and the user is to have no expectation of privacy. Anyone using the system expressly consents to monitoring.
- The banner shall specify that the Commonwealth is a two-party consent state when it comes to recording of conversations.
- A reference to the Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Agencies may use the following banner or compose their own if the banner meets the previously stated minimum requirements:

"This is an actively monitored computer system for authorized use only. Unauthorized access is prohibited. By using any Commonwealth IT Resources, including this system, the user acknowledges and agrees to comply with Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*. Unauthorized or improper use of this system may result in administrative disciplinary action, and/or civil charges or criminal penalties.

All activity may be monitored. Authorized Users should have no expectation of privacy in any files, data, or records stored on or accessed through IT Resources, nor should they have any expectation of privacy in any electronic communication sent or received via, or stored within, IT Resources. By using IT Resources, the user authorizes access to or auditing and/or monitoring of IT Resources by the Commonwealth."

Pennsylvania law requires "two-party" consent before a conversation may be recorded. This means that both parties involved in a conversation must give their consent to the recording of the conversation prior to recording it. If there are more than two people in the conversation, all parties must consent prior to any recording of the conversation. The recording of another person or persons, without their prior consent, is a violation of Pennsylvania's Wiretap Act and is a third-degree felony. Someone who violates the Wiretap Act 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.

4.2 Screensavers

All Commonwealth computers connecting to Commonwealth networks shall display a security awareness screensaver when the computer is in a resting mode or after ten (10) minutes of inactivity.

This screensaver is supplied and maintained by the Office of Administration. Two System Center Configuration Manager (SCCM) packages containing the screensaver and necessary settings to implement will be supplied to each agency for implementation.

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP.

5.2 Third-party vendors, licensors, contractors, or suppliers providing services to the Commonwealth must comply with the requirements outlined in this ITP and OPD-SEC000B *Security Policy Requirements for Third Party Vendors.*

6. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-ACC001 *Information Technology Digital Accessibility Policy*
- ITP-SEC000 *Information Security Policy*
- OPD-SEC000B *Security Requirements for Third Party Vendors*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	05/26/2006	Base Policy	N/A
Revision	03/16/2007	Policy Refresh	N/A
Revision	04/02/2014	ITP Reformat	N/A
Revision	02/25/2015	Added Definitions section Revised the required banner language Added Section 7 Exemption section Clarified language throughout	N/A
Revision	05/30/2019	Removed Definitions section in place for online glossary Updated Exemption and Publication section boilerplate language	N/A

Revision	09/26/2019	Revised ITP title Added screensaver guidance	Revised IT Policy Redline <09/26/2019>
Revision	6/26/2020	Added links to online glossary Added publication version control boilerplate language Removed COPPAR from Exemption section	Revised IT Policy Redline <6/26/2020>
Revision	07/12/2021	• Added offices to scope • Added third party vendors to Scope and Responsibilities Section • Added Responsibilities Section • Update policy references/links	Revised IT Policy Redline <07/12/2021>