Information Technology Policy
Commonwealth of Pennsylvania
Governor's Office of Administration/Office for Information Technology

ITP Number:	**ITP-BUS003**	
ITP Title:	**Emergency Telework Policy**	
Issued by:	**Deputy Secretary for Information Technology**	
Date Issued: November 20, 2009		**Date Revised: October 25, 2010**
Domain:	**Business**	
Discipline:	**Continuity of Government**	
Technology Area:	**Teleworking**	
Revision History Date:	**Description:**	
10/25/2010	**ITP Refresh**	

Abstract:

The purpose of this Information Technology Policy (ITP) document is to provide technology standards for teleworking in congruence with Management Directive 505.33, "Working from Home during Emergencies Including a Pandemic Influenza Event," and agency Continuity of Government (CoG) plans.

In the aftermath of the events of September 11, 2001, Commonwealth agencies need to consider the full range of possibilities related to how and where their work is accomplished in order to implement CoG planning. Through the use of alternate remote locations such as telecenters, employees who were displaced because of the terrorist attacks and subsequent anthrax problems were able to continue working. Employees were able to use laptop computers, cell phones, and other technologies from remote locations.

More tasks can increasingly be completed at alternate remote locations, especially with the introduction of Web portals and a service-oriented architecture, the ability to access Commonwealth data and applications, and the availability of Web conferencing services for virtual meetings and collaboration. The Commonwealth presently owns technology that allows teleworking employees to use personal computers (PC) to securely access programs and files from the employee's main office.

Teleworking in an emergency situation requires foresight and planning with standards and policies in place that will ensure that employees can effectively work at a remote location with equivalent capabilities and safeguards, just as if they are working at their own office.

General:

This ITP applies to all departments, boards, commissions and councils under the governor's jurisdiction. Agencies not under the governor's jurisdiction are strongly encouraged to follow this policy.

Policy:
Agency Emergency Telework Plans are to be done in compliance with Management Directive 505.33. Agency Emergency Telework plans are to be incorporated into agency CoG plans.

Agencies are to complete the *Emergency Telework Security/IT Checklist* in OPD-BUS003A, and file this attachment with their Agency Security Officer.

Agencies are reminded that all technology policies and standards still apply during Emergency Telework situations unless superseded by Executive Order. Policies that are particularly relevant to Emergency Telework include the following:

Policy	Relevance to Telework
ITP-SYM009 *Commonwealth of Pennsylvania Data Cleansing Policy*	Teleworkers are to ensure that data stored on electronic media is permanently deleted and unrecoverable before the media is disposed of or reused.
ITP-PLT011 *Mobile Device Policy and Standards*	Establishes policy for mobile devices such as Personal Digital Assistants (PDA) or Tablet PCs that are used outside the office for collection and/or remote access of data and applications.
ITP-PLT012 *Use of Privately Owned PCs to Access CoPA Resources*	Addresses the acceptable safeguards for the use of privately owned computers to access the Commonwealth of PA network.
ITP-APP004 *Collaboration Technology Standards*	The Commonwealth has established standards for real time Web conferencing to conduct remote meetings.
ITP-SEC024. *Information Technology Security Incident Reporting Policy* ITP-SEC024A. *IT Incident Reporting Procedures and Form*	Agencies are to put in place processes for ensuring that all users of agency systems are aware of the procedures and the importance of reporting security incidents, threats, or malfunctions that may have an impact on the security of agency information.
Privacy Act of 1974 Health Insurance Portability and Accountability Act (HIPAA)	Personnel are reminded to abide by the same information security policies and procedures (e.g., Commonwealth, industry, and federal) regardless of where they are conducting Commonwealth business.

Refresh Schedule:

All standards identified in this ITP are to be subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee.

Exemption from This Policy:

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Community of Practice Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required. Contact your agency CoP Planner for further details or assistance.

Publication Version Control It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov. Questions regarding this publication are to be directed to ra-itcentral@pa.gov.

Policy Supplements:

OPD-BUS003A Emergency Telework Security/IT Checklist

References:

MD 505.33: Working from Home During Emergencies Including a Pandemic Influenza Event
ITP-APP004: Collaboration Technology Standards
ITP-SYM006: Desktop and Server Patching Policy
ITP-SYM009: Commonwealth of Pennsylvania Data Cleansing Policy
ITP-PLT011: Mobile Device Policy and Standards
ITP-PLT012: Use of Privately Owned PCs to Access CoPA Resources
ITP-SEC001: Enterprise Host Security Suite Software Standards
ITP-SEC007: Minimum Standards for User IDs and Passwords
ITP-SEC024: Information Technology Security Incident Reporting Policy