COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE, AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Maintenance Personnel & Vendor Access**	Number: **POL-SEC013**
Domain: **Security**	Category:
Date Issued: **07/12/2013**	Issued By Direction Of:
Date Revised:	 Sandy K. Patterson, CIO Bureau of Information Systems

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes minimum requirements for the maintenance and review of maintenance personnel for the Department of Public Welfare (DPW) applications and related network resources, in support of maintenance and diagnostic activities. This policy also addresses compliance with related DPW, Commonwealth of Pennsylvania (CoPA) and federal requirements.

Maintenance personnel and vendor access consists of establishing mechanisms ensuring that any DPW personnel or contractors performing maintenance or diagnostic activities on the information system have required proper access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance.

1.2 Scope

All DPW employees, contractors and other stakeholders are responsible for understanding and complying with this policy. Maintenance personnel and vendor access include CoPA personnel contractors or any other stakeholders having access authorizations to perform maintenance on the information system.

1.3 Compliance

All DPW employees, contractors and other stakeholders are expected to be familiar with and comply with this policy. Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

1.4 Exemptions

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.5 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 Maintenance Personnel

Maintenance personnel relate to the protection of the confidentiality, integrity and availability of DPW information systems and DPW information as it gives access authorizations to individuals to conduct maintenance or diagnostic activities.

DPW Policy

a. DPW shall establish procedures for maintenance personnel authorization and maintain a list of authorized personnel and /or organization.
b. Authorized personnel performing maintenance activities on the information system shall have required appropriate access authorizations or be escorted by designated DPW personnel (system owners) with authorizations deemed necessary to supervise the maintenance.
c. Prior to initiating any maintenance or diagnostic activities by personnel who do not have access authorizations, clearances or formal access approvals, all volatile information storage components within DPW information system shall be sanitized and all nonvolatile storage media shall be removed or physically disconnected from the system.
d. DPW system owners shall enforce security procedures for the DPW IT systems. In the event a DPW information system component cannot be sanitized before performing maintenance or diagnostic activities,
e. DPW system owners shall ensure that personnel performing maintenance and diagnostic activities on

DPW Policy

an information system processing, storing, or transmitting classified information are background checked and cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.

f. Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on an information system are fully documented within a Memorandum of Agreement.

3 Controlled Maintenance

Controlled maintenance is the enforcement of a set of rules that govern the monitoring of maintenance activities. Effective maintenance management is critical to controlling and securing access to protected information.

DPW Policy

a. DPW system owners shall schedule, document, perform and review records of any maintenance activities performed on the information system providing an accurate picture of all maintenance and repair actions, needed, in process and completed.

b. All DPW maintenance activities performed on site or remotely shall be controlled.

c. Removals of DPW information system components shall always be approved by a DPW designated official and sanitized to prevent leak of confidential information.

d. DPW system owners shall, at a minimum, record maintenance activities that include the following:
   (a) Date and time
   (b) Name of the individual performing the maintenance;
   (c) Name of escort, if necessary;
   (d) Description of the maintenance performed; and
   (e) List of equipment removed or replaced (including identification numbers, if applicable).

g. DPW system owners shall verify implementation and functioning of appropriate system security controls after maintenance activities are conducted.

4 Maintenance Tools

The management of information system maintenance tools includes identifying how the organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

DPW Policy

a. Prior entering into a facility, DPW system owners shall inspect the maintenance for incorrect or inappropriate modifications.

b. DPW system owners shall ensure the use of information system maintenance tools and remotely executed maintenance and diagnostic activities are approved, controlled, and routinely monitored.

c. DPW system owners shall check all media containing maintenance diagnostic and test programs for malicious code before being used in the information system.

d. DPW system owners shall prevent the unauthorized removal of maintenance equipment by one of the following:
   - Verifying that there is no organizational information contained on the equipment;
   - Sanitizing or destroying the equipment;
   - Retaining the equipment within the facility; or

DPW Policy

- Obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

e. DPW shall employ centralized mechanisms to restrict the use of maintenance tools to authorized personnel only.

5 Remote Maintenance

This policy provides guidance for remote maintenance and diagnostic activities that are performed through a network; either an external network or an internal network.

DPW Policy

a. DPW system owners shall audit remote maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

b. DPW shall document the installation and use of remote maintenance and diagnostic connections in the information system security plan:
   - DPW shall require that remote maintenance and diagnostic services are performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
   - DPW Information system shall remove the component to be serviced from the information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

c. DPW shall protect remote maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:
   - Physically separated communications paths; or
   - Logically separated communications paths based upon encryption.

d. DPW shall require that:
   - The CISO shall periodically be notified by maintenance personnel when remote maintenance is planned (i.e., date/time); and
   - Remote maintenance shall be approved by a designated organizational official with specific information security/information system knowledge.

e. DPW shall employ cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.

f. DPW shall employ remote disconnect verification at the termination of remote maintenance and diagnostic sessions.

6 Appendix

6.1 Supporting DPW Policies

Document	Type
POL-SEC006 – Media Protection Policy	DPW Policy
NIST Special Publication 800-53 Revision 3	NIST Standard

Document	Type
POL-SEC008 – Physical and Environmental security Policy	DPW Policy
POL-SEC012 - User Identity and Access Management Policy	DPW Policy

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
07/18/2013	1.0	Initial Creation	Mathieu Saury
09/12/2014	1.0	Reviewed Content, No Changes	Marvin Ingram-Ambrisco