COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **DPW Information Security and Privacy Policies**	Number: **POL-SEC003**
Domain: **Security**	Category:
Date Issued: **05/09/2011**	Issued By Direction Of:
Date Revised: **11/07/2013**	Sandra Patterson, CIO Bureau of Information Systems

Table of Contents

Document History

Version	Date	Author	Status	Notes
1.0	05/09/2011	Tom Zarb	Draft	Initial creation
1.1	11/07/2013	Clifton Van Scyoc	Baseline	Revised version

1 Introduction

1.1 Background

The Department of Public Welfare (DPW) is dedicated to protecting the information entrusted to it. Information and information systems are vital assets that play a central role in the provision of DPW services. As threats to DPW's information resources continue to increase, the need for effective management of the associated risks also increases.

1.2 Purpose

This policy establishes the minimum security requirements for protecting Department of Public Welfare (DPW) information resources and provides overall direction for DPW's Information Security Program.

Additional key objectives of the *DPW Information Security and Privacy Policy* and DPW's security program are to:

- protect citizen data, both electronic and non-electronic, entrusted to DPW;
- implement measures to protect DPW information from unauthorized modification, destruction and disclosure, whether accidental or intentional; and maintain the authenticity, integrity and availability of DPW information;
- communicate the responsibilities for the protection of DPW information;
- establish and maintain a secure and robust IT infrastructure;
- preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure;
- promote and increase the awareness of information security throughout DPW; and
- Efficiently and cost-effectively manage the risk of security exposure or compromise within DPW systems.

1.3 Scope

This policy applies to all DPW units. All users of the Department's information technology (IT) resources are required to adhere to this policy, and as applicable, the supporting information security policies, standards and procedures.

This policy provides the department's view of information security considerations. It addresses technical security controls, as well as the management and operational requirements for information security; and it addresses the associated security roles and responsibilities. This policy addresses maintaining the confidentiality, integrity and availability of information processed, used, stored and transmitted on DPW information systems; as well as authentication of users and non-repudiation of transactions. In addition to IT assets that process, use, store, transmit or monitor DPW information; this policy covers IT facilities and off-site data storage, computing, telecommunications and applications-related services purchased from other state agencies or commercial entities; and Internet-related applications and connectivity.

DPW information security policy is based on federal and state laws, regulations, leading information security practices (e.g., National Institute of Standards and Technology [NIST] Special Publications on information security) and Commonwealth of Pennsylvania Information Technology Bulletins (ITBs).

1.4 Compliance

All DPW employees, interns, volunteers and contractors are responsible for understanding and complying with this *DPW Information Security and Privacy Policy*, and as applicable, the supporting supplementary policies, standards, and procedures. Those who intentionally violate these policies, standards, and procedures may receive disciplinary action, as mandated by the Department. Outsourced processing and storage facilities, including vendors, partnerships and alliances, will be monitored and reviewed to ensure compliance with DPW policies.

1.5 Exemptions

Any exemptions to this policy must be approved by the CISO.

1.6 Policy Review and Update

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

1.7 Acronyms

Table 1. Acronyms

Acronym	Definition
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CoPA	Commonwealth of Pennsylvania
DPW	Department of Public Welfare
IT	Information Technology
ITB	Information Technology Bulletins
NIST	National Institute of Standards and Technology
OA/OIT	Office of Administration / Office for Information Technology

2 Risk Management

The overall objective of any security related endeavor is appropriate risk management. It is impossible to eliminate all risk. Security measures are implemented to cost-effectively mitigate risk to acceptable levels, and all security decisions should be made with risk management in mind.

DPW information resources require security commensurate with its value, criticality and sensitivity. When information is transferred either internally or externally to DPW information systems and networks, it must be protected from origin to destination. Availability of information systems and data resources must be maintained to ensure continued service to citizens and continuity of operations.

2.1 Threats and Vulnerabilities

DPW information resources are vulnerable to many threats that must be considered when making risk management decisions. Shown below is a representative listing of the types of threats that DPW information resources are exposed to.

Table 2. Threat Sources

Human Intentional	Human Unintentional	Structural	Environmental
• Fraud and theft • Malicious intruder • Industrial espionage • Malicious code • Nation-state espionage • Terrorism • Intentional circumvention • of security • Disregard for procedures • Disgruntled employee	• Errors and omissions • Untrained users • Programming errors • Configuration errors	• Physical environment • Network anomaly • Software anomaly • Power anomaly	• Fire • Wind • Water • Snow/Ice • Lightning

2.2 Security Principles

The basic security principles are to ensure the confidentiality, integrity and availability of information and information resources, as well provide for the authenticity and non-repudiation of transactions and information exchanges.

- **Confidentiality** means that information deemed sensitive or confidential is protected and unavailable to those who do not have the necessary approvals to access or view it.
- **Integrity** means that information is correct and is protected from corruption and unauthorized modification. It also means that programs, applications, procedures and systems function as intended.
- **Availability** means that access to information and information systems is not denied to authorized users, and information systems can appropriately resist attacks and recover from failures.
- **Authenticity** means that the originator of a message or transaction can be readily and correctly identified.
- **Non-repudiation** means that the recipient of a message or transaction is unable to deny receipt.

Security is an enabler critical to the success of technology initiatives and should not be viewed as a deterrent or obstacle.

2.3 Information Security

As a fundamental enabler of DPW's mission, information security encompasses many disciplines, including computer security, network security, communications security and physical security. The overall goal of information security is to protect and defend information and information systems. Disruptions in today's environment are not preventable all of the time; therefore, while prevention is ideal, detection is essential. Therefore, information security activities include information protection, event detection, and appropriate response and restoration of information and services.

2.4 Privacy

Congress passed the E-Government Act of 2002 to encourage the use of Web-based applications by government agencies as a means of enhancing the quality, effectiveness and efficiency of government operations. The Commonwealth has similarly encouraged use of the Internet as a key communication tool. Partially due to this trend, public concern regarding the disclosure of personal information has increased. To combat this, federal and state legislation has emerged over the last several years that address safeguarding electronic information in a variety of business areas, including health, business, identity and public safety.

Within this context, DPW has implemented policies and standards that address its commitment to protecting the personal information entrusted to it; while adhering to applicable federal and state privacy and security mandates. DPW's privacy policy and standards address protection of personal information in both electronic and non-electronic form.

2.5 Legal/Regulatory Requirements

Proper use of DPW information and information systems is governed by a diverse set of security and privacy legal and regulatory requirements including the key ones listed below. To obtain a complete list of applicable legal and regulatory requirements, please contact the CISO.

- Protected Health Information (PHI)
    - Health Information Portability and Accountability Act (HIPAA) Omnibus Final Rule 2013
- Federal Taxpayer Information (FTI)
    - Internal Revenue Service publication 1075 (IRS 1075)
- Personally Identifiable Information
    - Children's Online Privacy Protection Act of 1998 (COPPA)
    - Family Educational Rights and Privacy Act of 1974 (FERPA)
    - Pennsylvania Breach of Personal Information Notification Act (BPINA) of 2005, SB 712
    - Pennsylvania SSN Obfuscation Law of 2009, SB 601
    - Tax Information Security Guidelines for Federal, State and Local Agencies, Publication 1075, Internal Revenue Service

- Real ID Act of 2005
- Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement (CMS) v1.0, (August, 2012)
- Social Security Administration (SSA) Security Requirements Defined by the SSA Agreement with the Department of Public Welfare, Commonwealth of PA
    - System Design Plan (SDP) Requirements defined by SSA in the "Electronic Information Exchange Security Requirements and Procedures version 6.0" (April 2012)

- Public Safety Information
    - Pennsylvania Criminal History Record Information Act of 1980 (CHRIA), 18 Pa. C.S.A Section 9101 et seq.
- General Information
    - Commonwealth of Pennsylvania Electronic Information Privacy Policy (ITB-PRV001)
    - Federal Privacy Act of 1974
    - Pennsylvania House Resolution 351 (2005)
- Other
    - Americans with Disabilities Act (ADA), (March 15, 2011)
    - DPW IT Security Incident Reporting Policy (POL_ENSS002)
    - Federal Driver's Privacy Protection Act of 1994

2.6 NIST 800-53 Security Control Catalog

NIST Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems* defines eighteen families of security controls. These controls are the management, operational, and technical safeguards (or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. NIST SP 800-53 is the primary source of recommended security controls for federal information systems, and has been adopted by DPW for developing its information security policy and standards.

3 Roles and Responsibilities

Information security requires the active support and ongoing participation of DPW employees and contractors. It requires support from the executive level and universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with the development, implementation, operation, use and maintenance of DPW information systems.

Implementation, acceptance and maintenance of adequate system and network security is a shared responsibility of senior management, portfolio managers, program offices, security and system administrators, supporting and using organizations, technology providers and users. DPW personnel are responsible for evaluating the level of risk associated with any particular information system and implementing adequate security controls to reduce the risk to an acceptable level. The following are specific roles and responsibilities.

3.1 Chief Information Security Officer (CISO)

Per industry best practice and ITB-SEC016, *Commonwealth of Pennsylvania – Information Security Officer Policy*, each CoPA agency must appoint an Information Security Officer. ITB-SEC016 establishes the following minimum associated responsibilities:

- Determine the sensitivity of data created and/or processed within the organization and establish and/or define appropriate controls and acceptable levels of risk.
- Ensure appropriate organizational security procedures and standards are developed to support the information security policy. The Information Security Officer is responsible for coordinating the implementation of information security measures and providing management assurance that the organization complies with legislative, contractual, and Commonwealth policy requirements regarding information security.

Additional primary responsibilities are:

- Protect information and information systems throughout DPW.
- Develop and implementing the *DPW Information Security and Privacy Policy*, and the supporting policies, standards and procedures. Review the *DPW Information Security and Privacy Policy*, and supporting documents, a minimum annually, and update the documents as needed.
- Implement a Security Awareness and Training Program, to facilitate enforcement of this policy.
- Implement programs and processes to address new requirements and issues, as needed.
- Coordinate with the Office of Information Technology (OIT) and other Commonwealth agencies as needed.

3.2 Chief Risk Officer (CRO)

Per industry best practice and NIST reference (NIST Special Publication 800-39, Appendix D, Roles and Responsibilities) each CoPA agency must appoint a Chief Risk Officer or risk executives and establish the following minimum associated responsibilities:

- Define process and approve procedures to assess and mitigate the agency risks.
- Develop a global risk management program, ensuring that DPW maintains adequate operational risks, and that DPW is in full compliance with state laws, regulations and internal policies and procedures.
- Establish and communicate DPW's risk appetite, risk management philosophy and implement an appropriate infrastructure of policies, processes and personnel, reports and systems for managing and monitoring risks.
- Coordinate with the Office of Information Technology (OIT) and other Commonwealth agencies as needed.

3.3 Chief Privacy Officer (CPO)

Per industry best practice, NIST reference (NIST Special Publication 800-100, Chapter 2, 2.2.3.5 Related Roles) and ITB-PRV002, *Electronic Information Privacy Officer*, each CoPA agency must appoint a Chief Privacy Officer or risk executives and establish the following minimum associated responsibilities:

- Enforcing the Commonwealth Privacy Policy as defined in ITB-PRV001, *CoPA Electronic Information Privacy Policy*.
- Ensuring that all applicable federal, state, and other mandates specific to electronic privacy concerns that pertain to the agency areas are met and enforced in accordance with ITB-PRV001.
- Reporting annually to OA/OIT on the agency's compliance with ITB-PRV001.
- Defining the categories of electronic information and categories of users to be identified for the agency in accordance with ITB-PRV001.
- Developing, in conjunction with the agency's human resources department, the agency electronic information confidentiality agreement as defined in ITB PRV001 and ensuring its use.
- Notifying the Commonwealth CTO and/or OA/OIT EI Privacy Officer of concerns regarding the agency's compliance with either the Commonwealth electronic information Privacy Policy or other state/federal business-related privacy directives.

4 DPW Information Security and Privacy Policy Infrastructure

This document is supported by a documentation infrastructure that includes supplementary policies, standards and procedures. Depicted in Figure 1, below, is the DPW Information Security Policy and supporting documents, including supplementary **policies.** Each supplementary policy (e.g. *User Identity and Access Management Policy*) is supported by one or more **standards** (e.g. *Account Management Standard*), establishing detailed requirements for implementing the policy. From these standards, **procedures** (e.g. *Account Management Procedures*) are developed to address how policy requirements are to be implemented.

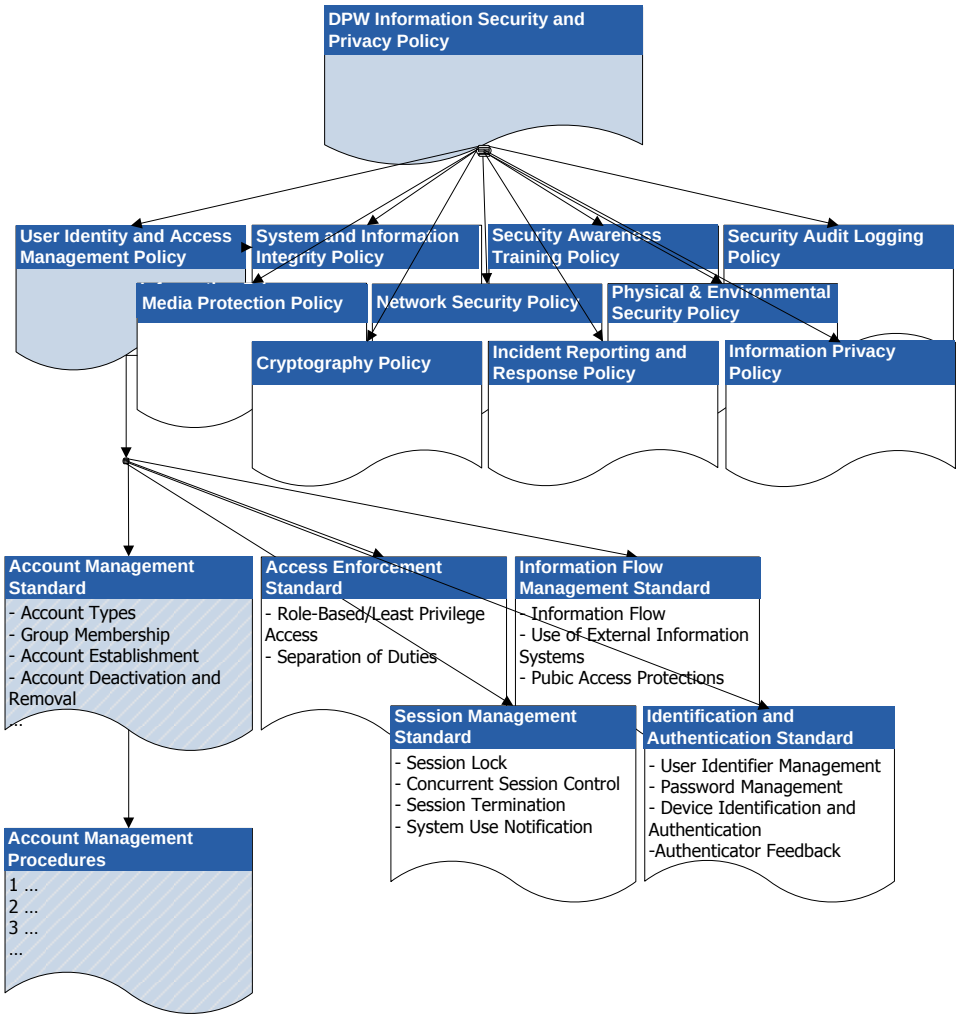
Figure 1. DPW Information Security and Privacy Policy Infrastructure (Example: User Identity and Access Management Policy)

Overarching Policy
- Addresses 'why'
- Outlines specific organization-wide requirements that must be met

Issue-Specific Policies
- Addresses 'why'
- Outlines specific requirements that must be met

Standards
- Addresses 'what' must be done to implement policy
- Consists of issue-specific requirements for addressing specific objectives

Procedures
- Addresses 'how' policy is to be implemented
- Step-by-step actions and decisions to be performed to accomplish a requirement or objective.



The supplementary policies that support this overarching *DPW Information Security Policy* may be accessed from the 'Security Domain' webpage on DPW's Bureau of Information System's website, http://bis/pgm/h-net%20standards/1.0%20security/securitytoc.asp. The *DPW Information Security and Privacy Policy* is supported by the supplementary information security policies listed below. Also identified are the standards referenced within each of the supplementary policies.

Table 3. Supplementary Information Security Policies

Supplementary Policy	Policy Description	Related Standard(s)
Cryptography Policy	Addresses the use of cryptography for protecting information.	• Cryptography Standard
Incident Reporting and Response Policy	Addresses effective response to security incidents.	• Incident Response Plan
Information Privacy Policy	Addresses compliance with federal, state and departmental privacy laws, regulations and requirements.	
Media Protection Policy	Addresses protection of media containing sensitive information.	• Media Protection Standard
Network Security Policy	Addresses protection of information transmitted or received by DPW information systems.	• Information Flow Enforcement Standard • Secure DNS Standard • Partitioning and Virtualization Standard
Physical and Environmental Security Policy	Addresses implementation of physical and environmental safeguards to adequately protect DPW personnel, property and information resources from unauthorized physical intrusion and other physical threats.	• Physical Security Standard • Environmental Security Standard
Security Audit Logging Policy	Addresses maintenance of a record of system application and user activity, to facilitate detection of security violations, performance problems and application flaws.	• Audit Log Management Standard • Audit Review, Analysis, and Reporting Standard
Security Awareness Training Policy	Addresses educating users; thereby reducing errors and omissions, reducing fraud and unauthorized activity, increasing user accountability and motivation, and increasing knowledge of how to perform tasks securely.	
System and Information Integrity Policy	Addresses protection of information assets from malicious code; and identification and correction of information system flaws.	• System Integrity Standard • Information Integrity Standard
User Identity and Access Management Policy	Addresses requirements for authenticating users and controlling access to DPW information systems.	• Access Enforcement • Account Management • Session Management • System Use Notification • Identifier Management • Organizational Users • Non-Organizational Users • Device Identification and Authentication
Maintenance Personnel &	Addresses requirements for the maintenance and review of maintenance personnel to DPW	• Access Enforcement

Vendor Access,	applications and related network resources.	
Configuration Management)	Addresses requirements for managing risks associated with the configuration of information resources.	• Infrastructure Vulnerability Standard