COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **User Access Management**	Number: **STD-ENSS033**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of: James A Weaver James Weaver, Dir of Div of Tech Engineering
Date Revised:	

Abstract:

This standard provides guidance to the department's application development teams on use of department's standard IAM systems for integration with the custom applications. The department IAM solutions include:

- CA SiteMinder
- CA Identity Manager
- CA SOA Security Manager
- IBM Tivoli Identity Manager (ITIM)
- Microsoft Active Directory (AD)

General:

The User Access Management Solutions Standard applies to the Department of Public Welfare (DPW or "Department") Identity and Access Management (IAM) systems used to manage, authenticate and authorize users onto department systems and applications. The requirements outlined in this document provide guidelines on which IAM system should be used under what circumstances.

Standard:

CA SiteMinder

CA SiteMinder is used by the department to manage and maintain user's access, based on enterprise user roles[2] or as approved by the Chief Information Security Officer (CISO), to web resources such as web pages and application specific web services. The department's web applications and application web services shall use CA SiteMinder for user authentication and authorization. The department's application team shall work with the security account administration team to integrate the application with CA SiteMinder.

CA SiteMinder provides user session tokes that are used to maintain and manage user's access The user sessions shall adhere to the department session management policy[1], including:

- Inactivity timeout varies on the DPW applications; default inactivity timeout of 15 minutes on user desktops
- Secure Sockets Layer (SSL) v3 or Transport Layer Security (TLS) session encryption
- SSL/TLS enabled HTTP-only session cookies

The user roles are provisioned using the CA SiteMinder administration interface. The application user accounts shall be managed only by the security account administration team, Chief Information Security Officer (CISO) or department designated business partner delegated administrator. The department's web applications shall use CA SiteMinder to protect its web resources.

CA Identity Manager

The department uses CA Identity Manager to provision and de-provision citizen user and DPW business partner privileges/permissions to department web applications. The CA Identity Manager solution provides backend connection functionality to the department's Microsoft Active Directory, the department's authoritative user account repository.

The department's security account administration team should be involved throughout the Software Development Management (SDM) process to integrate the CA Identity Manager solution with user access management on department web applications.

The department's security account administration team has established several instances of CA Identity Manager to support the department's application requirements. Using these instances, the program office administrators and the corresponding business partner delegated administrators manage the designated user base.

In addition, the department shall use the CA Identity Manager for establishing internet facing citizen user and business partner self-service solutions such as user profile update, password reset and security hint Q/A.

CA SOA Security Manager

The respective department user account administration teams shall implement CA SOA Security Manager to maintain user access to the department enterprise web services – designed for consumption by more than one application and hosted in the department's Service Oriented Architecture (SOA) environment. Please refer to the department standard on services security[3] for additional details on the management and of web services within the department.

The CA SOA security manager also uses user roles to manage access to the protected web services. The user roles are provisioned using the CA SOA security manager administration interface and managed by the department's security account administration team only.

IBM Tivoli Identity Manager (ITIM)

The department's security administration team uses ITIM to provision and de-provision application/system access for Commonwealth employee/contractor user accounts. The ITIM solution shall also be used to assign user roles to DPW mainframe systems.

The ITIM solution provides backend connection functionality to the department's Microsoft Active Directory, the department's authoritative user account repository. The department shall use ITIM for enterprise wide Commonwealth user self-service solutions such as Desktop Password Reset Application (DPRA). As per the department's IAM policy[1], ITIM is used to disable temporary or emergency user accounts after 48 hours of inactivity.

Exemptions from this Standard:

There will be no exemptions to this standard.

References:

1. POL-SEC012: User Identity and Access Management Policy
2. DPW Enterprise Role Based Access Standard
3. DPW Services Security Standard

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	User Access Management	Clifton Van Scyoc