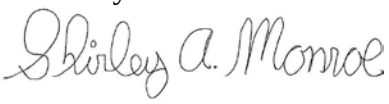
COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **User and Access Certification Standard**	Number: **STD-ENSS025**
Domain: **Security**	Category:
Date Issued: **05/17/2011**	Issued By Direction Of:  Shirley A. Monroe, Dir of Div of Technical Engineering
Date Revised: **08/09/13**	

Abstract:
The purpose of this standard is to describe the Department of Public Welfare (DPW) minimum expectation on user and access certification. The rise in data loss due to inappropriate access has led to various laws, regulations and standards that require periodic user and access certification. To help address inappropriate/excess access and data loss, regulations and standards require that in addition to preventive controls, detective controls also be used. User and access certification can be used as a detective control to identify unauthorized access and reduce exposure by implementing appropriate processes and controls.

General:
This standard provides the minimum required to perform user and access certification for achieving compliance with regulatory requirements and other DPW policies.

Scope
This standard is applicable to DPW employees, contractors, business partners for the DPW application(s) that they have access to.

Standard:
Both a user's information and the access rights that a user has been granted for DPW applications must be certified on a periodic basis (defined by Certification Frequency). The user information and access rights include:

- User information – User information certification entails certifying that the user is a valid user and information about that user is correct such as application access rights, address and email address.

Roles and Responsibilities

DPW CISO Office
DPWs CISO office will provide the program area a list of users and their corresponding access rights per application on a yearly basis.

Certifier – DPW employees and contractors
DPW employees who are authorized representatives of the Program Office are authorized to be a certifier of DPW employee and contractor's user information and access rights. For example, a Program Office Administrator can be an authorized certifier.

Certifier – Business Partner users
Authorized Business Partner Administrators who have the responsibility to approve access rights to business partner users, may certify the user information and access rights of business partner users within their organization. Business Partner Administrators must be certified by a DPW employee who is an authorized representative for the Program Office.

Certifiers must be able to make a determination on whether a user's information is correct and whether the user has been granted appropriate access on DPW applications. Delegation of certification responsibility is prohibited. Transfer of certification responsibility is an exception to the standard.

Certification Frequency
Certification on all applications shall be performed on an annual basis by each Program Office. The completion of the certification exercise must be completed within 60 days after the Program Office receives the list of users and application access.

The submission of the documented results must also be provided to DPW CISO within 60 days of the certification exercise start date. If the results are not provided back to the DPW CISO office, access to the specific application will be removed.

Review on all information system accounts shall be performed at least once every one-hundred-eighty (180) days and recertified.

Certification Remediation
Remediation actions required as a result of the certifications must be performed within 30 days of the completion of the annual certification cycle.

Remediation actions shall be performed on temporary accounts that are no longer required, accounts of terminated or transferred users and/or accounts with a period of inactivity of more than one hundred eighty (180) days.

Certification and Remediation Evidence Retention
Record of certification and remediation performed must be captured and retained for a period of three (3) years by DPW CISO office. When possible, these records should be captured electronically. The certifications actions for each user should be captured and at the minimum the following information must be retained for that certification.

- Certification ID (Unique Sequence Number)
- Date certification request was created

- User name and User Account name
- Application access/roles and attributes
- User type such as DPW employee, contractor, business partner user and business partner administrator
- Certified action at user level (approved, rejected)
    - If rejected, document the user information that needs to change
- Certification date
- Certifier name

Corresponding to each certification request that was processed, the following information regarding remediation must be retained DPWs CISO office.

- Certification ID
- Remediation ID
- Name of person who performed the remediation
- Date remediated
- Details of remediation performed
- Program Office representative who reviewed and returned the certification information

It is the Certifier's responsibility to return all certification results and corresponding remediation actions to DPWs CISO office

Standard Violations

Violations of this Standard are to be documented and escalated to the DPW CISO for tracking and remediation.

Exemptions from this Standard:

Any Program Office that is unable to comply with this standard must discuss any exemption request with the Department's CISO.

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
08/09/2013	6.1	Reviewed and updated	Mathieu Saury