pennsylvania
OFFICE OF ADMINISTRATION

EBR, Office of Information Technology Policy APP-000

Name:	Systems Development Life Cycle
Effective Date:	December 2018
Category:	Application
Version:	1.0

1. Purpose:

This policy establishes a well-defined Systems Development Life Cycle (SDLC) framework; related software application development methodologies; and tools that are essential components in the management, development, and delivery of software applications and systems to support the Employment Banking & Revenue (EBR) delivery center business needs. This policy provides direction for systems and software developed in-house and the use of commercial off-the-shelf (COTS) applications. This policy documents the implementation of Information Technology Policy (ITP) ITP-SEC005. This policy also fulfills the requirements of Internal Revenue Service (IRS) Publication 1075 safeguards and requirements defined by the Social Security Administration (SSA). This policy documents the implementation of the National Institute of Standards and Technology (NIST) Security Controls: AC-5, AC-6, CM-9, RA-2, RA-3 & SA-3 Per SP 800-53 R4.

2. Background:

This policy is published under the general authority of the Governor's Office of Administration/Office of Information Technology (OA/OIT).

The SDLC complements the NIST risk management framework by providing a sample roadmap for integrating security functionality and assurance into the SDLC. These security considerations are relevant to both new and legacy systems, and should be applied and documented to ensure security controls are in place and functioning effectively to provide adequate protections for the information and the information system.

Software development or application development is considered a subset of this SDLC process.

3. Scope:

This policy applies to all employees within all bureaus, divisions, boards, commissions, councils, and agencies supported by the Employment Banking and Revenue (EBR) delivery center. This includes any contracted employees in the service of EBR (hereinafter referred to collectively as "EBR Users").

4. Policy:

Agency program area management shall meet with OIT project management to initiate any project related to the development of new or significant changes to existing systems and software applications and create a project team.

EBR, Office of Information Technology Policy APP-000

EBR OIT shall establish project teams consisting of project management, architecture, security, operations, business relationship management, contracted resources, program area staff, and other resources, as necessary. Each project team shall establish controls including cost, accountability, schedule, and success criteria for their project.

EBR OIT shall identify SDLC methodology to be used for all new development and maintenance phases.

The System Owner (SO), in conjunction with the business and Information Security Office (ISO) shall establish the minimum controls to be implemented based on the system security plan per SEC-000.

All project and system development efforts shall adhere to NIST Security Controls, based on data classification and FIPS-199 security impact level.

EBR ISO shall provide documentation of compliance with and gaps in NIST security controls. EBR OIT shall maintain these documents with the service design package (SDP).

EBR OIT shall comply with data classification requirements of ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data.

The SO shall ensure each release complies with requirements from the release management and security management processes. Public facing applications must comply with (CA)^2 requirements OA ITP-SEC005.

The SO shall ensure that no release is promoted to production without having successfully passed static analysis security testing (SAST).

The SO shall ensure the Application Inventory has been updated with the initial release and subsequent updates.

EBR OIT shall ensure that all development efforts implement the least privilege security model, and role based access (RBAC).

EBR OIT shall ensure that all access, roles, and permissions are in compliance with all access control policies.

EBR OIT shall ensure that all systems are architected to ensure separation of duties. No staff having elevated roles and permissions to the development or testing environments shall have access to the production environment. All application and program access paths utilized in development or testing, other than the formal user access paths, must be deleted or disabled before software is moved into production.

EBR OIT shall maintain documentation requirements throughout all phases of the SDLC plan.

The SO shall document and implement records retention and disposition schedules in compliance with MD 210.5 and MD 210.9.

All systems development efforts shall be developed in accordance with the EBR SDLC plan.

All systems utilizing COTS products shall be developed in accordance with the applicable phases of the EBR SDLC plan.

All software developed in-house shall be developed in accordance with the EBR SDLC plan.

All systems shall be architected with a minimum of separate development, test, and production environments. Additional environments must be identified as part of the SDP.

EBR OIT shall document system records in accordance with PLT-004 Inventory of Authorized & Unauthorized Hardware & Software.

EBR OIT shall document baseline management in accordance with SYM-002 Configuration Management Policy.

The SO shall document changes following the EBR change management policy.

The SO shall comply with the EBR release management policy.

EBR OIT shall review the SDLC plan annually and update the plan every three years.

5. Responsibilities:

A. EBR User responsibilities:

- Comply with all EBR policies, OA ITPs, management directives, executive orders and laws; and
- Report any violations of policies promptly to the EBR Chief Information Security Office at LI, OIT-EBRCISO.

B. EBR management responsibilities:

- Comply with all EBR policies, OA ITPS, management directives, executive orders and laws; and
- Ensure EBR users comply with the policies; and
- Adhere to this policy and any published procedures regarding application and system development.

6. References:

EBR Policy Definitions Document

PLT-004 Inventory of Authorized & Unauthorized Hardware & Software

SEC-000 System Security Plan Policy

SYM-002 Configuration Management Policy

ITP-SEC005 Commonwealth Application Certification and Accreditation

ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data

MD 205.34 Commonwealth of Pennsylvania IT Acceptable Use Policy

MD 210.5 Commonwealth of Pennsylvania State Records Management Program

MD 210.9 Commonwealth of Pennsylvania General Records Retention and Disposition Schedule

7. Version Control:

Version	Date	Purpose
.01	02/2009	Base Document
1.0	12/2018	Updated for EBR delivery center