pennsylvania
OFFICE OF ADMINISTRATION

EBR, Office of Information Technology Policy SEC-000

Name:	Security Planning Policy
Effective Date:	November 2018
Category:	Security
Version:	1.1

1. Purpose:

This policy creates a prescriptive set of processes, procedures, and training, aligned with applicable Governor's Office of Administration (OA) and the Employment Banking and Revenue (EBR) Information Technology (IT) security policies and standards. This policy establishes the minimum requirements for the EBR Office of Information Technology (OIT) to plan IT security, which will help protect information, including Federal Tax Information (FTI), from unauthorized access and improper disclosure in compliance with safeguards and requirements defined by the Internal Revenue Service (IRS) and the Social Security Administration (SSA). This policy is intended to meet the control requirements outlined in IRS Publication 1075, the National Institute of Standards and Technology (NIST) NIST critical controls: CA-1, CA-2, CA-3, PL-1, PL-2, PL-3, PL-4, PL-6, and SC-1 Per SP 800-53 R4, as well as additional OA IT policies and controls.

2. Background:

The IT System Security Plan (SSP) at EBR is intended to facilitate the effective implementation of the processes necessary to meet IT system security requirements as stipulated by federal and state policies. The SSP ensures the business needs are being met in a secure manner.

An SSP is crucial to the development of a service, system, or application. An SSP shall be in place to address organizational policies, procedures, security testing, rules of behavior, contingency plans, architecture and network diagrams, and requirements for security reviews.

The SSP supports the system development life cycle (SDLC) and shall be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. The SSP provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

The SSP supports the risk management process by providing both the business and IT the necessary information to make risk based decisions about applications and systems.

EBR OIT employs access controls based on the risk appetite of the approving authority, data owner and system owner, to specify how access to data is managed.

3. Scope:

This policy applies to all EBR employees, business partners, contractors, temporary personnel, agents, and vendors, (hereinafter referred to as "EBR Users"); as well as EBR

systems that have been designated as Mission Critical Applications (MCA) or contain data classified as sensitive.

4. Policy:

A. Planning

OIT with oversight from the Information Security Office (ISO), shall establish and manage an overall information security program for the protection of EBR computers, networks, and information assets to ensure that the integrity, confidentiality, and availability of information used is not compromised.

OIT shall provide security requirements for the development of new application systems, and assure the consistent implementation of controls for information systems throughout the organization in accordance with all state and federal laws, and requirements, as well as the Governor's Office of Administration's (OA) standards and policies.

EBR OIT shall align with NIST cybersecurity framework v1.1 and shall apply the NIST 800-53 security controls, develop and document policies, and practices with business requirements to support the missions of EBR.

OIT shall classify all systems and the data processed and stored by that system in accordance with Federal Information Processing Standard Publication 199 (FIPS 199) per EBR policies: ADM-000, SEC-001, SEC-012, SYM-005 and OA policies ITP-SEC019, ITP-SEC020, ITP-SEC031.

OIT shall perform a risk analysis to determine the level of and complexity of controls required to ensure the confidentiality, integrity, and availability of EBR data, in accordance with FIPS 199 security impact level.

OIT shall select controls from NIST critical controls based on the data owner requirements, e.g. IRS Publication 1075, risk, and business requirements.

OIT shall protect information used to conduct the business of EBR from unauthorized disclosure, use, modification, or destruction in accordance with industry best practices and in compliance with federal and state laws and regulations, including but not limited to IRS, SSA, and accepted security standards.

OIT shall plan and coordinate security-related activities affecting these information systems.

The Delivery Center Chief Information Security Officer (CISO) will serve as the primary point of contact to the Delivery Center Chief Information Officer (CIO) for all information technology security matters.

The CIO, CISO, System Owner, and Office of Chief Counsel shall review data sharing agreements and trust relationships between EBR and any business partner or contracted resource owning, operating, or maintaining external information systems connected to

EBR systems. Data sharing agreements shall consist of documentation for each connection, including the data classification, interface characteristics, security requirements, data owner, and the nature of the information communicated.

B. System Owners

All system owners (SO) of sensitive systems shall produce an SSP for their system, including systems that use Commercial-Off-The-Shelf (COTS) applications.

All SO shall document interconnections to other systems including those within the same agency, other agencies within the Commonwealth or other federal entities in the SSP.

All SO shall ensure data security in all environments, including the identification and protection of any sensitive data processed or stored in non-production environments.

All SO shall ensure the proper level of security controls are implemented.

SOs with OIT shall implement Role Based Access Controls (RBAC) to grant and restrict access to sensitive data.

All SOs and authorizing officials shall establish the risk appetite statement for their application/system and furnish this to OIT for risk analysis purposes.

All SOs shall establish within the SSP a user's expected behavior with regard to sensitive information and information system usage, as well as the controls to address user behavior. SOs and delivery center CISO shall modify the contents of the SSP to meet requirements of the data owner and business.

C. Reviews

The Delivery Center CISO shall annually review the SSP, Disaster Recovery (DR), Continuity of Operations (COOP), and Commonwealth of PA Procurement and Architectural Review (COPPAR) documents with the SO as part of the ITIL IT Service Continuity Management and ITIL IT Security Management plans.

The Information Security office, SO, and Authorizing official shall review changes to the SSP, and DR plans annually or upon significant changes to the system.

COTS application administrators shall produce an SSP for their product and ensure it integrates with the application SSP and agency SSP.

OIT shall review architectural changes, version changes, and enhancements to the system as part of change and release management processes for impact to the SSP. Per System Development Life Cycle policy.

OIT shall implement a risk management methodology and incorporate it with EBR's IT Infrastructure Library (ITIL) processes.

OIT shall make plans for appropriate action when loss, damage, or breach of confidentiality occurs per security incident response policy.

OIT shall update the SSP as part of the IT Service Continuity Management process.

OIT shall assess security alerts and threats and apply compensating controls based on the risk management methodology.

5. Responsibilities:

A. EBR User responsibilities:

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

B. EBR management responsibilities:

- Comply with all EBR policies and ensure EBR users comply with the policies; and
- Adhere to this policy and any published procedures regarding security planning.

6. References:

EBR Policy Definitions Document

ITP-SEC005 - Commonwealth Application Certification and Accreditation

ITP SEC016 - Commonwealth of Pennsylvania - Information Security Officer Policy

ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data

ITP-SEC020 - Encryption Standards for Data at Rest

ITP-SEC031 - Encryption Standards for Data in Transit

NIST Special Publications

FIPS Publications

7. Version Control:

Version	Date	Purpose
1.0	02/2009	Base Document template
1.1	11/2018	Format and Content Revision for EBR