



West Virginia State Privacy Program Strategic Plan 2018 - 2020

Mission

In furtherance of Executive Order No. 3-17, the purpose of the West Virginia State Privacy Program (WVSPP) is to appropriately protect the privacy of personally identifiable information (PII), including protected health information (PHI), federal tax information (FTI) and payment card industry information (PCI), collected and maintained by state agencies, through governance, risk management and compliance.

Roles and Responsibilities

Privacy is a shared responsibility across all departments and programs. Under the leadership of the West Virginia Board of Risk & Insurance Management (BRIM) Executive Director, the State Privacy Office (SPO) leads the WVSPP and the West Virginia Privacy Management Team (PMT). The PMT is an integral component of the program and is comprised of privacy officers and subject matter experts from across the Executive Branch.

The SPO sets team goals, with the PMT's participation and consensus, to accomplish the program's mission. Expertise from outside of the PMT is sought when needed. Workgroups may be formed with PMT members as well as others, with subject matter expertise, authority or resources to accomplish specific deliverables. Therefore, a team goal is often accomplished through collaboration with leadership from a variety of agencies. A new product, policy or program is then presented to the PMT and the Governor's cabinet for implementation across the Executive Branch.

Mission Statement Objectives

The WVSPP adopts the American Institute of Certified Public Accountants' (AICPA) Privacy Maturity Model. Based upon a review of program maturity and importance, over the next three years, the WVSPP will focus on improving the maturity of the following elements:

1. Infrastructure and systems management.

- a. AICPA criterion: The organization's¹ policies require that any acquisition of information-related products or services, as well as its system-development life cycle, address privacy.

Action (1): WV Executive Branch will *require* the completion of a Privacy Impact Assessment that evaluates privacy implications when developing or procuring any new technologies or systems that handle or collect PII.

- b. AICPA criterion: The organization has detailed checklists and procedures, and has assigned personnel, for ensuring the design, acquisition, development, and implementation of information-related products and services are compliant with relevant privacy policies.

Action (2): WV Executive Branch will implement a Privacy by Design (PbD) program. PbD is an approach to systems engineering which takes privacy into account throughout the whole engineering process.

2. Privacy incident management. AICPA criterion: Because of its rigorous response process, the organization has resolved all known privacy incidents within 30 days for at least the past year.

Action (3): BRIM will implement an automated incident management system to reduce risk and simplify compliance with data breach law.

3. Risk assessment.

- a. AICPA criterion: The organization's policies require that any acquisition of information-related products or services, as well as its system-development life cycle, address privacy.

Action (4): WV Executive Branch will *require* the completion of a Privacy Impact Assessment that evaluates privacy implications when developing or procuring any new technologies or systems that handle or collect PII. (*See, Action (1)*).

- b. AICPA criterion: The organization has detailed checklists and procedures, and has assigned personnel, for ensuring the design, acquisition, development, and implementation of information-related products and services are compliant with relevant privacy policies.

Action (5): WV Executive Branch will implement a vendor management program, addressing risk assessment, appropriate privacy and security contract terms and assurance.

¹ Organization refers to the appropriate governmental unit.

4. Policy documentation. AICPA criterion: The organization's privacy policies address all 8 privacy principles and are displayed on their relevant websites.

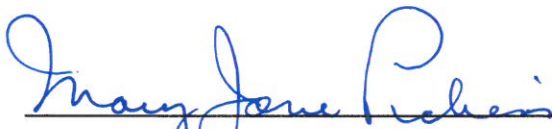
Action (6): BRIM will update and revise Executive Branch Privacy Policies and audit a representative sampling of agency privacy notices.

5. Privacy awareness and training. AICPA criterion: The organization annually communicates its privacy policies to all of its personnel that encounter personal information.

Action (7): BRIM will update HIPAA awareness training module.

Review

The SPO will review and report on progress on this plan on an annual basis to the Governor, prior to the first day of each calendar year, in accordance with Executive Order Number 3-17.



Mary Jane Rickens
Executive Director

11-30-17

Date

West Virginia Board of Risk & Insurance Management