# STATE OF WEST VIRGINIA
## DEPARTMENT OF ADMINISTRATION
## BOARD OF RISK AND INSURANCE MANAGEMENT

Mark D. Scott
Cabinet Secretary

Melody Duke
Executive Director
Melody.A.Duke@wv.gov


January 5, 2023

Mr. Brian Abraham, Chief of Staff
Office of the Governor
State Capitol
1900 Kanawha Blvd. E
Charleston, WV 25305

Dear Mr. Abraham:

On behalf of the West Virginia Board of Risk and Insurance Management, I am pleased to submit to Governor Justice and to you our annual report on West Virginia's Privacy Program. The report is divided into three sections covering accountability, risk management, and compliance.

The State Privacy Office (SPO) reevaluated and renewed its strategic plan for 2022 – 2025 with a continued focus on how to effectively manage and grow a statewide privacy program. Technology is increasingly important for the expanding need and future growth of West Virginia's State Privacy Office. Our goal is to operate efficiently and remain a small office, while continually expanding our services to support more state entities. This can only be accomplished through the use of technology. Therefore, BRIM and the SPO will be re-doubling efforts, working with WV Office of Technology, to purchase and establish privacy technology solutions that will be effective and efficient. Through accountability measures, privacy risk management and legal compliance, we continue to mature and grow the state's privacy program and accomplishments with no growth in size of the State Privacy Office.

Maintaining our citizens' and employees' privacy is a priority for all of us at the Board of Risk and Insurance Management and the State Privacy Office. This requires a variety of ongoing proactive efforts, along with focused management of privacy incidents to protect the state's valuable data assets, which is our ultimate goal. Thank you for your continued support toward this mutual effort

Should you have any questions, please contact Chief Privacy Officer Ashley Summitt at 304-766-2646 X 20232.

Very truly yours,
Melody Duke
Melody Duke
Executive Director

MD/ldm
Enclosure


1124 Smith Street, Suite 4300
Charleston, West Virginia 25301
www.brim.wv.gov

(304) 766-2646
(304) 558-6004 FAX
(800) 345-4669 TOLL FREE WV


# WEST VIRGINIA

# STATE PRIVACY OFFICE

# 2022 Annual Report

**JANUARY 2023**

Ashley Summitt, Chief Privacy Officer
Lori Tarr, Deputy Chief Privacy Officer
Lora Reynolds, Administrative Assistant

# Membership of the 2022 Privacy Management Team (PMT)

**Board of Risk and Insurance Management, State Privacy Office (a unit of BRIM):**

- BRIM – Melody Duke (Executive Director)
- BRIM – Robert Fisher (Deputy Director/Department Privacy Officer)
- State Privacy Office – Ashley Summitt (Chief Privacy Officer)
- State Privacy Office – Lori Tarr (Deputy Chief Privacy Officer)
- State Privacy Office – Lora Reynolds (Administrative Assistant)

**Executive Branch, Department Privacy Officers (DPO), Agency Privacy Officers (APO):**

- Governor's Office – Samantha Willis (DPO), Felicia Swecker (APO)
- Bureau of Senior Services – Lee Knabenshue (DPO)
- Department of Administration –Tom Miller (DPO HIPAA), Misty Peal (Non-HIPAA)
  - Cabinet Secretary's Office – Misty Peal (DPO)
  - Cyber Security Office – Danielle Cox (Chief Information Security Officer)
  - Office of Technology –Jennelle Jones (General Counsel)
  - PEIA – Tom Miller (HIPAA Privacy Officer) and Bill Hicks (General Counsel)
  - Division of Personnel – Wendy Mays (APO)
- Department of Arts, Culture and History – Kristopher Bowyer (DPO)
- Department of Commerce – Tia Shannon (DPO)
  - Workforce WV – David Dyer (APO)
  - Division of Rehabilitation Services – Aaron Johnson , Candice Ward (DPO)
- Department of Environmental Protection – Neil Chakrabarty (DPO)
- Department of Economic Development - Steve Meester , Tia Shannon (DPO)
- Department of Health and Human Resources – Chris Snyder (DPO)
  - Represents Bureau of Public Health–Claire Winterholler (Assistant Attorney General)
- Department of Homeland Security– Jamie Chambers {2022}, Brandolyn Felton-Ernest (DPO)
- Department of Revenue – Allen Prunty , Heather Samples (DPO)
- Department of Tourism - Erica Whitney , Krysten Wolfe (DPO)
- Department of Transportation – Jill Dunn (DPO)
  - Division of Highways – Rebecca McDonald (APO)
  - Division of Motor Vehicles – Jennifer Pierson (APO)
- Department of Veterans Assistance – Julie Reed (DPO)
- Chapter 30 Licensing Boards –Sue Painter (Privacy Liaison)
- West Virginia National Guard - Mountaineer Academy North - VACANT
- West Virginia National Guard - Mountaineer Academy South - Deborah Gipson, (APO)

**Representing Other Constitutional Officers and Higher Education:**

- State Auditor's Office – Michael Nusbaum (DPO)
- Department of Education – Georgia Hughes-Webb (DPO)
- State Treasurer's Office – Brian Bailey (DPO), Lisa Rutherford (APO)
- West Virginia Supreme Court of Appeals - Pat Moats (Privacy Officer)
- West Virginia School of Osteopathic Medicine - Jeffrey Shawver (DPO), Deborah Bogan (APO)
- West Virginia University – Amanda Griffith (DPO)
- West Virginia University – Stacie Honaker (Health Sciences Center Risk Mgr. / DPO)
- West Virginia Higher Education Policy Commission/West Virginia Community and Technical College System – Melanie Baker (DPO), Shelley DeLuca (DPO), Dr. Zornitsa Georgieva (DPO)

- Marshall Health – Buffy Hammers (DPO), Cindy Shrout (APO)
- wvOASIS – Richard Dolin (DPO)

## INTRODUCTION

Under the direction of the Executive Director of the Board of Risk and Insurance Management (BRIM), the State Privacy Office (SPO) manages the executive branch's Privacy Program (Program) and leads the Privacy Management Team (PMT). The SPO consists of the Chief Privacy Officer (CPO), the Deputy Chief Privacy Officer (DCPO), and an Administrative Assistant.


The PMT consists of:

- leadership at BRIM;
- the State Privacy Office;
- privacy officers from each department and many agencies, higher education, other state constitutional officers, and other branches of state government; and
- the Chief Information Security Officer (CISO).

The SPO and the PMT efforts may be described in three broad functions: accountability; risk management; and, compliance. The goal is to protect the personally identifiable information (PII) of the state's citizens and workforce. PII includes other subcategories of information such as Protected Health Information (PHI), Federal Tax Information (FTI), and Payment Card Industry (PCI) information.

## Six Guiding Principles for the State Privacy Program

These six guiding principles are foundational to any privacy program and are used as the basis for the West Virginia Executive Branch Privacy Policies and guide the State Privacy Office in all aspects of our program.

- *Accountability* – assigned roles and responsibilities to assure application of privacy principles to PII.
- *Notice* – openness regarding the authority for collecting PII; the purpose of the collection; the location of the entity maintaining the PII; with whom the PII may be shared and why; rights an individual has in PII; and the entity's policies, procedures, standards, and practices with regard to PII.
- *Minimum Necessary and Limited Use* – collection, use and disclosure of PII should be limited to the entity's legal authority and purpose, as set forth in an entity's Notice, and Minimum Necessary PII the entity needs to perform the defined legally permitted task.

- *Consent and Authorization* – an entity's collection of PII should be contingent upon first obtaining an individual's consent to collection. An entity does not collect, use, or disclose PII in a manner inconsistent with its Notice, unless it has first obtained the individual's permission for the use or disclosure.
- *Individual Rights/Individual Participation* – when possible, an entity relies first on the PII it collects directly from the individual. An individual should be afforded the ability to access and copy the PII an entity acquired or maintains, request an amendment of the information an entity maintains and, if such amendment is not undertaken, request that the information be notated. Entities shall provide appropriate means of individual redress which include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.
- *Security Safeguards* – an entity implements the appropriate management, operational and technical controls to preserve the privacy, confidentiality, integrity and availability of PII.

## ACCOUNTABILITY

State leadership is committed to proactive accountable management of information security and privacy. The foundational policy of the Privacy Program is the Accountability Policy. This requires each department to have one or more privacy officers designated to ensure application of the executive branch privacy policies and procedures, and to provide training to the departments' workforce. Having staff dedicated to the task of data privacy is intrinsic to holding ourselves accountable to our citizens and workforce.

Fundamental to the process of preparing new privacy officers is our office's privacy officer orientation process. This training reviews the organization of the Privacy Program, the important role it plays in the protection of the state's data, privacy policies, and incident management. It also reviews the privacy impact assessment, online privacy training of the workforce, privacy resources, and many other aspects of the privacy officer role.

The number of new privacy officer orientations conducted in 2022 was 29. This was a significant increase from 2021, when there were 10 orientations. With retirements and the Privacy Office's efforts to secure privacy officers for previously non-represented agencies, we anticipated that 2022 would be back at 2019 orientation levels (20), but we greatly exceeded that expectation. In light of this increase in orientation needs and our small staff size, we are investigating recording our orientation in modules which can be provided to new privacy officers to review on their own, with a follow-up meeting for any remaining questions. This would provide a more efficient process for all, and provides a resource for reference at later times.

The commitment to privacy by West Virginia's leadership is underscored by an annual proclamation of Data Privacy Day, which is an internationally recognized day each January 28th. The proclamation encourages observance of Data Privacy Day by government officials, representatives, educators, schools, and citizens. Each year the SPO holds a West Virginia Data Privacy Day event to raise awareness and provide additional training to all executive branch

departmental privacy officers. The training activities for the 2022 Data Privacy Day event were conducted virtually due to the Covid pandemic. Because of the use of the virtual format, the event was opened to both departmental and agency privacy officers alike as a means to provide a training benefit to agency privacy officers. The 2022 Data Privacy Day event was a discussion of the techniques of investigation of privacy incidents, complete with two table-top exercises in break-out rooms, led by a privacy incident expert in this field.

In addition to its focus on the future and advancing the Privacy Program, the SPO also continued to promote accountability and fulfill its management role by:

- Leading the quarterly PMT meetings, which provide a forum for training and information sharing, legislative updates, consensus building, security updates, and open dialogue among PMT members. The SPO sets the agendas for each meeting, providing speakers and experts in the relevant fields. Since the format of the PMT has been virtual meetings since the pandemic began, PMT meetings have included more agency privacy officers. This format change has resulted in more attendance by privacy officers that are not located in the Charleston area which has been a positive outcome.

- In 2022, discussions and training were based on current privacy and security issues and on members' requests and included:

    - Data Privacy Day - Privacy incident investigations and exercises.
    - Human Resource, Privacy and Security- table-top exercise.
    - Privacy and Security Training tutorial.
    - Privacy Impact Assessment Review
    - Cybersecurity Current Trends, Incident Response
    - Advanced Privacy Officer Training

- On October 17-19, 2022 a Privacy Retreat was held at Canaan Valley Resort State Park. Forty-two (42) departmental and agency privacy officers attended this in-person event to hear experts in the cybersecurity field discuss "What Every Privacy Officer Should Know About Cybersecurity." Participants, who were members of the West Virginia State Bar, received 8 hours of CLE training from participation in the retreat.

## Risk Management

Mitigating organizational risk is accomplished through the selection of appropriate privacy controls established through organization-wide assessment and understanding of distinct mission/business and operational needs. According to the National Institute of Standards and Technology, "The risk-based approach...considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations."[1]

[1] Dept. of Commerce. NIST. "Risk Management." Created November 2016, Updated November 2022.. https://csrc.nist.gov/projects/risk-management/about-rmf

Activities by the SPO supporting and enhancing risk management included:

- Review of PIA submissions. The PIA provides project managers with a risk assessment tool for reviewing privacy implications involved with the purchase of information technologies or system redesign processes that collect or store PII. The PIA includes: a privacy threshold analysis; a review of data classification and collection, use and storage factors; disclosure practices; and administrative, physical and technical controls.

  Submissions of PIAs have increased significantly over the last several years. PIA submissions counts from 2019 are:

  - 2019 – 25
  - 2020 – 48
  - 2021 – 52
  - 2022 – 67

- Regular collaboration between the CPO and the CISO regarding risk management, incident response, strategic planning, and workforce development.

- Training and education of the workforce continued to be a high priority for the SPO. The SPO collaborated with the CISO to roll out a new privacy and security online training for all members of the State's Executive branch agencies. By the end of 2022, 79% of all employees had completed it.

  According to the Ponemon Institute's 2022 Cost of Data Breach Study, training was one of the most effective factors for reducing the cost of a data breach. Twenty-eight factors were reviewed in the study. Having an incident response team and use of incident response testing were other top factors. [2]

  Beyond the training completed for privacy officers or the regular PMT meetings, the following training was provided in 2022:

  - January 2022: Data Privacy Day, a virtual presentation of methods for incident investigation and break out room exercises by an expert in the field.
  - April 2022, Chief Privacy Officer provided a CLE seminar presentation entitled, "Privacy Matters", for the Division of Purchasing's 2022 day of CLE training.
  - May 2022, SPO staff did a live virtual presentation for the West Virginia Division of Purchasing's In House Training, "Purchasing as a Privacy Powerhouse."
  - July 2022, Chief Privacy Officer presented a privacy webinar entitled "The Balancing Act Between Data and Privacy," as part of a panel discussion for the WV Digital Government Summit.

---

[2] Ponemon Institute. "Cost of Data Breach Study: 2022." IBM Security. https://www.ibm.com/downloads/cas/3R8N1DZJ

- October 17-19, 2022, SPO staff provided a Privacy Retreat for departmental and agency privacy officers at Canaan Valley Resort State Park, entitled "What Every Privacy Officer Should Know About Cybersecurity".
- On November 1, 2022, the Chief Privacy Officer did an overview of the State Privacy Office at the West Virginia Auditor's Office for their annual required training for Chapter 30 State Licensing Boards.

- The SPO has been working with the other divisions within BRIM and within the Department of Administration to update their agency's records retention and disposal schedule. Using the Retention schedule, many old files are being cleared out of their office and Iron Mountain (the state's archive service) to be destroyed. Current files and documents are being scanned and retained electronically. These electronic documents are now considered the official documents of record. The electronic files will be purged as their disposal dates are reached. This is a risk management project that reflects the Minimum Necessary and Limited Use privacy policy by adhering to best practices for the data lifecycle of PII, which includes data destruction.

## COMPLIANCE

The commitment to comply with internal policies, industry standards, and external regulations was demonstrated by the SPO with the following activities and projects:

- Management of the executive branch privacy incident response program to assure notification compliance with privacy laws. The SPO provides oversight and serves as a resource, throughout the duration of managing a privacy incident, from filing the initial report, through the investigation, to resolution.

- Oversight, tracking and reporting of required online privacy training courses for the state's workforce, completed through the Learning Management System (LMS). These include the West Virginia Executive Branch Confidentiality Agreement, Privacy Awareness , and HIPAA/HITECH Awareness Training. The State Privacy Office contracted with a privacy training provider to provide an updated general privacy training which is available on a new LMS software. The new privacy, as well as security, training was introduced to all members of the Executive Branch's workforce in June.

- Provided advice and consultation, as needed, to the state's workforce on privacy issues related to:

    - Executive branch contracts with vendors;
    - Privacy policies, procedures, laws, and regulations;
    - Incident investigation; and
    - Best practices in project design and implementation.

- Revised the annual Privacy Requirements Report. This is a review of new federal and state privacy laws that affect the executive branch. Each law is identified by common name, legal citation and description, implications, electronic source, and mapped to applicable privacy principles.

- Updated the annual HIPAA Preemption Analysis, which is an overview of the preemption issues that arise between state and federal law. The Privacy, Security, Breach Notification, and Enforcement Rules of HIPAA and the HITECH Act, and the requirements of West Virginia laws are compared to determine which laws are more stringent, and thereby supersede or preempt the other, to become the primary law for a particular aspect of health care privacy.

## Conclusion

The SPO continues to work diligently to advance methods of operating a vibrant statewide privacy program with a very small staff. Involvement of the State Privacy Office in the management of the State's incident response, employee privacy training and the organization of the Privacy Management Team are imperative to the State's continued cyber insurance coverage. Our commitment to protecting the privacy of the state's citizens and workforce remains high. We have had unexpected global challenges to address, but these are being overcome with necessary flexibility, ingenuity and dedication. We look forward to sharing in future reports the SPO's progress to grow and mature West Virginia's Privacy Program.

## References

Dept. of Commerce. NIST. "Risk Management." Updated December 13, 2017. Accessed December 29, 2017. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview.

Ponemon Institute. "Cost of Data Breach Study: 2022." IBM Security. https://www.ibm.com/downloads/cas/3R8N1DZJ