State of Indiana Standard: *Agency Privacy Officer Job Description*

Version: 1.0 (7/2023)

Job Title: Agency Privacy Officer

Job Summary:

The Agency Privacy Officer (APO) is responsible for developing, implementing, and maintaining the privacy program for the agency, in compliance with the *State of Indiana Policy: Information Privacy* and in consultation with the State Chief Privacy Officer (State CPO). The APO is responsible for ensuring the agency complies with applicable privacy laws and regulations and that agency privacy risks are effectively managed.

Responsibilities:

In consultation with the State CPO:

1. Develop and maintain agency privacy policies, standards, procedures, and guidance to ensure the agency complies with applicable privacy laws, regulations, and expectations.
2. Advise the agency regarding the exchange of agency information, as well as the maintenance and management of agency information by third-party vendors.
3. Oversee the completion of privacy training programs for agency employees, contractors, and partners.
4. Manage completion by the agency of the State of Indiana Privacy Impact Assessment program to identify and mitigate privacy risks in processes and systems.
5. Conduct agency privacy audits and assessments to ensure that privacy risks are effectively managed; report privacy risks to the State CPO for inclusion in the State of Indiana Privacy Risk Register.
6. Respond to agency privacy incidents and coordinate with internal and external stakeholders to ensure that privacy incidents are handled in a timely and effective manner.
7. Stay informed of changes in privacy laws and regulations and ensure that the agency privacy program is updated accordingly.
8. Provide advice and guidance to the agency on privacy-related issues.
9. Collaborate with the agency Security Team to ensure that privacy risks are integrated into the cybersecurity risk management program.
10. Represent the agency in privacy-related matters, including discussions with regulators and stakeholders, and constituents.

Requirements & Preferences:

1. Bachelor's degree in law, public policy, information technology, or a related field is required. Juris doctorate or masters in public policy or information technology is preferred.
2. Certification by the International Association of Privacy Professionals is preferred.
3. Previous exposure to privacy and data protection as a practice area.
4. Strong understanding of privacy laws and regulations applicable to the agency, including the Indiana Fair Information Practices Act.

5. Willingness to partner with the State CPO in the development and implementation of privacy program components.
6. Excellent communication and interpersonal skills.
7. Ability to work independently and as part of a team.
8. Strong project management and organizational skills.
9. Familiarity with privacy technologies and tools.

Professional Competencies of an APO:

1. Privacy Laws and Regulations: Thorough knowledge and understanding of privacy laws and regulations relevant to the agency, including the Indiana Fair Information Practices Act.
2. Risk Management: Ability to identify, assess, and manage privacy risks effectively, leveraging standards and frameworks such as the NIST Privacy Framework, NIST SP 800-53, and NIST AI Risk Management Framework.
3. Policy and Procedure Development: Experience in developing and maintaining privacy policies, standards, procedures, and guidance documentation.
4. Privacy Impact Assessments: Knowledge of privacy impact assessments and the ability to conduct them effectively, using the *State of Indiana Standard: Privacy Impact Assessment Methodology: A NIST-Based Framework to Support Enhanced Privacy Protections within Government*.
5. Privacy Training: Ability to manage privacy training programs for agency employees, contractors, and partners.
6. Incident Response: Experience in responding to privacy incidents and managing incident response processes.
7. Communication Skills: Strong verbal and written communication skills, including the ability to explain complex privacy concepts to a non-technical audience.
8. Interpersonal Skills: Ability to work effectively with internal and external stakeholders, including regulators and constituents.
9. Project Management: Strong project management skills, including the ability to manage multiple projects simultaneously.
10. Technical Knowledge: Familiarity with privacy technologies and tools, including data protection and encryption technologies.
11. Adaptability: Ability to adapt to changes in privacy laws and regulations and to enhance the privacy program accordingly.