OFFICE OF THE
STATE AUDITOR

This document is for educational purposes only and needs to be customized further. Reach out to the State Privacy Officer at wphillips@utah.gov before implementation.

Governmental Entity Privacy Program Template

(this document is related to the Privacy Program requirement under The Utah Government Data Privacy Act)

Mission Statement

The Privacy Program is dedicated to ensuring the protection and proper management of personal data within the entity. By adhering to privacy laws and implementing best practices, the program aims to foster a culture of privacy awareness, accountability, and continuous improvement. Our goal is to protect individual privacy rights while enabling the entity to carry out its mission effectively and to follow the state privacy vision and requirements stipulated in the Utah Government Data Privacy Act.

1. Introduction

- **Purpose**: Ensure compliance with privacy laws and protect personal data.
- **Scope**: Applies to all employees, contractors, and third parties handling personal data.

2. Activities

- **Data Inventory**: Conduct a comprehensive data inventory to identify all personal data collected, stored, and processed.
- **Risk Assessment**: Perform privacy risk assessments to identify potential vulnerabilities.
- **Policy Review**: Review and update privacy policies (Data Retention, Data Access, etc.) regularly.
- **Training and Awareness**: Conduct mandatory privacy training for all employees annually and provide training for new hires within 30 days of their start date.
- **Third-Party Audits**: Assess third-party data handling practices and update agreements as needed.
- **Privacy Impact Assessments (PIA)**: Perform PIAs for new projects or significant changes in data processing or high-risk processing.
- **Security Enhancements**: Implement technical security measures in collaboration with the IT department and the Utah Cyber Security Center and their standards.

- **Data Subject Rights**: Ensure mechanisms are in place for individuals to access, correct, and delete their data.
- **Breach Simulation**: Conduct data breach simulation exercises to test incident response plans.
- **Annual Reporting**:
    - Prepare and submit an annual report on data sharing to the State Privacy Officer by the end of August.
    - Prepare and submit an annual report of breaches to the Cyber Center by the end of August.
- **Audit and Compliance Check**: Conduct internal audits to ensure compliance with privacy policies.
- **Review Incident Reports**: Analyze and document any data breaches or incidents and implement corrective actions.
- **Annual Privacy Report**: Prepare an annual privacy report summarizing activities, assessments, and improvements made throughout the year.

3. Key Roles and Responsibilities

- **Privacy Officer**: Oversee the privacy program and manage data protection efforts.
- **IT Department**: Implement and maintain technical security measures.
- **Records Management Officer**: Oversee implementation of retention schedules and management of records access requests.
- **Employees**: Adhere to privacy policies and report any privacy incidents.
- **Leadership**: Provide necessary resources and support for the privacy program.
- **Legal counsel**: provide legal advice including classification of incidents and breaches.

4. Continuous Improvement

- Regularly review and update the privacy program based on changes in laws, regulations, and best practices.
- Foster a culture of privacy awareness and responsibility within the entity.
- Use a privacy maturity model to assess and improve the program's maturity, considering factors such as policy implementation, risk management, and incident response capabilities.
- **Responsibility**: The Privacy Officer, in collaboration with Leadership and the Records Management Officer, is responsible for driving continuous improvement.

5. Partnerships

- **Attorney General's Office**: Collaborate for legal guidance and compliance.
- **State Privacy Officer**: Work together to align with state privacy initiatives and reporting requirements.
- **Cyber Center**: Partner for cybersecurity measures and incident management.

6. Monitoring Metrics and Maturity Measurement

- **Metrics**: Track the number of data breaches, training completion rates, and compliance audit results, including additional metrics per your privacy policy.
- **Maturity Measurement**: Evaluate the program's maturity using a privacy maturity model, assessing factors such as policy implementation, risk management, and incident response capabilities.

7. Recommended Policies and Standards and Templates

- **Data Retention Policy**: Guidelines for how long different types of data should be retained.
- **Data Access Policy**: Rules for who can access specific types of data and under what conditions.
- **Data Classification Policy**: Framework for categorizing data based on sensitivity and criticality.
- **Breach Notification Policy**: Procedures for reporting data breaches to authorities and affected individuals.
- **Incident Response Plan**: Steps for responding to data breaches or other security incidents.
- **Employee Privacy Training Policy**: Requirements for regular privacy training and awareness programs.
- **Third-Party Data Handling Policy**: Standards for how third parties must manage and protect personal data.
- **Data Minimization Policy**: Practices for collecting only the data necessary for a specific purpose.
- **Encryption Policy**: Guidelines for encrypting sensitive data both at rest and in transit.
- **Privacy by Design and Default Policy**: Ensuring privacy considerations are integrated into all projects and systems from the outset.
- **Individual's Privacy Rights Policy**: Procedures for enabling individuals to exercise their rights over their personal data.
- **Privacy policy statement -** Document describing data processing practices related to organization's website.
- **Privacy data request notice:** Document used at data collection for transparency.

- **Consent with Data Processing:** Document used for processing of personal data where expressed consent is required.

8. Contact Information

- Privacy Officer: [Name, Email, Phone Number]