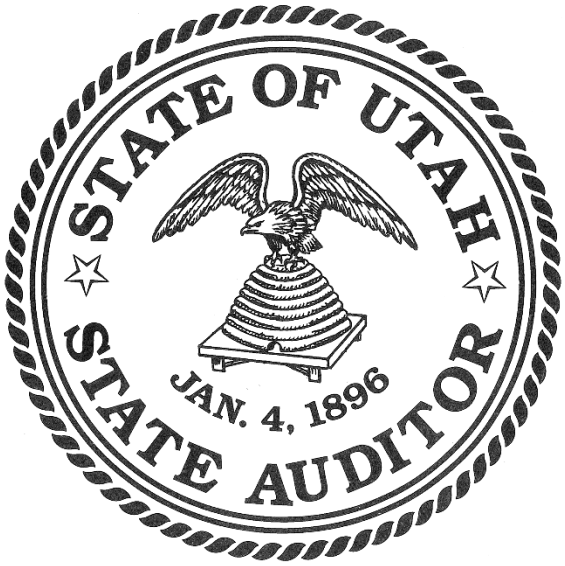


OFFICE OF THE STATE AUDITOR

State Privacy Officer Annual Report FY2022

October 1, 2022

State Privacy Officer Annual Report FY2022

Purpose and Scope

Utah Code § 67-3-13 requires the State Privacy Officer to submit an annual report to the Judiciary Interim Committee on or before October 1. This initial annual report highlights Utah legislature's recognition that the government has an obligation to handle personal information about Utah residents responsibly and in a fair and transparent way. In 2021, the legislature passed the Privacy Protection Amendments to oversee privacy practices in state government (See Appendix A: Authorities of the Utah Privacy Program). This legislation created the State Privacy Officer position within the Office of the State Auditor. The State Privacy Officer supports over 1,000 local government and state entities including:

- 391 Local and Special Service Districts
- 152 School Districts or Charter Schools
- 146 Cities
- 108 Towns
- 89 Redevelopment Agencies/Project Areas
- 62 Interlocal entities
- 38 Conservation Districts
- 29 Counties
- 19 Housing entities
- 18 Institutions of Higher Education

Goals to Increase Privacy Maturity

In order to increase privacy maturity, the State Privacy Officer has set three State of Utah Privacy Program goals. These goals were set for FY2022 and will continue into FY2023. The status of the goals is based on evidence as of June 30, 2022. The goals are:

1. Prioritize scope,
2. Determine baseline metrics, and
3. Increase privacy capacity of local/state government entities.

Goal 1: Prioritize Scope. The State Privacy Officer has determined both targeted and broad focuses for the initial implementation of Utah's privacy program (See Table 1.).

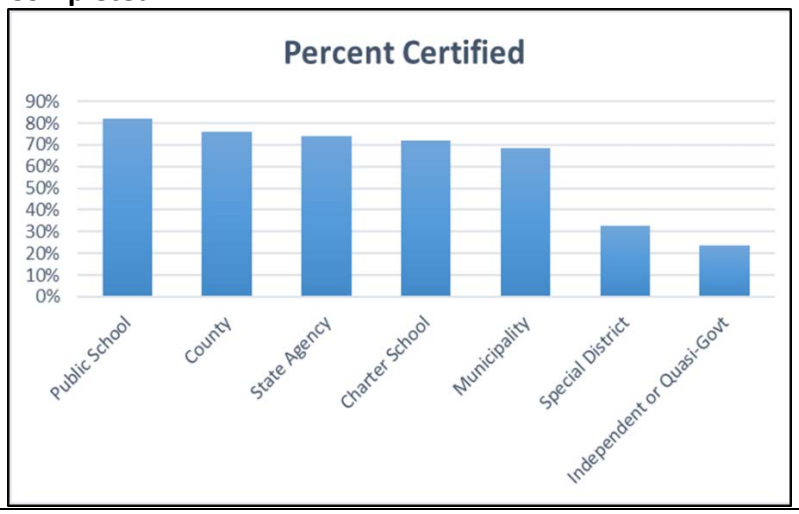
Table 1. Goal 1: Prioritize Scope

FY 2022-2023	Status
Utah's Institutions of Higher Education is a targeted priority due to the amount of data they hold.	The State Privacy Officer: • Coordinated with legislators on drafting "Higher Education Student Data Protection" 53B-28-503 • Determined a privacy point of contact for 15 of the 18 Institutions of Higher Education • Invited privacy points of contacts to participate in Certified Information Privacy Manager training
Data minimization is a broad priority across all local government entities. FY2023 Modernize the General Record Retention Schedule	State Privacy Officer is coordinating with the Utah State Archives to: 1. Modernize the general record retention schedules 2. Modernize record management certification course 3. Create sector specific records management certification courses 4. Increase the percentage of certified record officers (63G-2-108)

Goal 2: Determine Baseline Metrics. The State Privacy Officer has determined both targeted and broad metrics for baseline and future program evaluation (See Table 2.).

Table 2. Determine Baseline Metrics.

FY 2022-2023	Status
FY 2022 Targeted baseline metric includes Institutions of Higher Education's compliance of 53B-28-503 and Utah Board of Higher Education's compliance of 53B-28-502. FY2023 Complete baseline measure of compliance of 53B-28-503 and 53B-28-502.	**Completed:** 16/18 Institutions of Higher Education have determined a privacy point of contact **To be completed:** • The Utah Board of Higher Education designation of a Higher Education Privacy Officer • Adoption policies to protect student data • Development of privacy standards, model documents, or training materials • Percent of Intuitions of Higher Education that have created and maintained a data governance plan • Creation of the Higher Education Privacy Advisory Group

FY2022 Broad baseline metric includes the percentage of active certified records officers (63G-2-108). FY2023 Increase the percent of certified records officers.	**Completed:** 
FY2022 Conduct an initial assessment of privacy maturity of a sub-set of local government entities.	**Completed:** An optional survey based on Generally Accepted Privacy Principles (See Appendix B. Privacy Maturity Survey Questions) was sent to: ● All 153 Local Education Agencies ● All 29 Counties ● All 168 other designated government entities with 50 or more employees. **Results:** The survey revealed very low privacy maturity. The top 10 scores belonged to 8 Local Education Agencies and 2 Behavioral Health Facilities. The bottom 10 scores belonged to 4 counties and 6 cities. 

FY2022 Review and document existing local education agency (LEA; i.e., K-12 public education) evidence of compliance.	Utah State Board of Education's rule R277-487 requires that all local education agencies provide evidence of compliance each year on October 1st. • Appendix C. Local Education Agency Privacy Compliance describes the mature privacy metrics that have been measured for the last 4 years. • For FY22 evidence of privacy compliance was an average of 90% across all LEAs.

Goal 3. Increase privacy capacity of local/state government entities. The State Privacy Officer has provided professional and basic awareness training opportunities for local and state government entities to increase privacy capacity (See Table 3.).

Table 3. Goal 3. Increase privacy capacity of local and state government entities

FY 2022-2023	Status
FY2022 Coordinate with the Personal Privacy Oversight Commission to identify "standards and best practices with respect to government privacy practices" as required by 63C-24-202. (See Appendix D. Personal Privacy Oversight Commission) FY2023 Develop educational and training materials based on Utah's Fundamental Privacy Principles required in 63C-24-202.	**Completed:** The Personal Privacy Oversight Commission adopted Utah's Fundamental Privacy Principles (See Appendix E)
FY2022 Provide targeted professional privacy training to Institutions of Higher Education and other interested local government entities. FY2023 100% of Institutions of Higher Education will have an employee that is a Certified Information Privacy Managers FY2023 Twenty or more local government employees will be a Certified Information Privacy Manager	**Completed:** All privacy points of contact for Institutions of Higher Education have been invited to participate in a two-day training provided by the International Association of Privacy Professionals. Participants will have an opportunity to become Certified Information Privacy Managers. This certification includes: • How to create a company vision • How to structure the privacy team • How to develop and implement a privacy program framework • How to communicate to stakeholders • How to measure performance • The privacy program operational life cycle

FY2022 Provide broad privacy awareness training to a sub-set of local government entities. FY2023 Develop at least 5 privacy training modules for Utah Association of Counties and Utah League of Cities and Towns.	State Privacy Officer provided broad privacy awareness training to: • Utah Association of Counties (UAC) • Utah League of Cities and Towns (ULCT) • Technical Coordinators Council (TCC)

Appendix A. Authorities of the Utah Privacy Program

- Division of Archives and Records Services
  Utah Code § 63A-12-100 et seq. (Fka. Public Records Management Act (PRMA))
- Government Records Access and Management Act
  Utah Code § 63G-2-101 et seq.
- Governmental Internet Information Privacy Act
  Utah Code § 63D-2-101 et seq.
- Government Operations Privacy Officer
  Utah Code § 67-1-17
- Personal Privacy Oversight Commission
  Utah Code § 63C-24-101 et seq.
- State Privacy Officer (Auditor)
  Utah Code § 67-3-13
- Unauthorized Access to Information Technology
  Utah Code § 63D-3-101 et seq. (Part 1 - Computer Abuse Data Recovery Act)
- Utah Technology Governance Act. Chief Information Officer.
  Utah Code § 63A-16-210 Chief Information Security Officer
- Utah Technology Governance Act. Data Security Management Council
  Utah Code § 63A-16-701--702
- Single Sign-on Portal
  Utah Code § 63A-16-801 et seq.
- Utah Open Records Portal Website
  Utah Code § 63A-12-114
- Utah Open Data Portal Website
  Utah Code § 63A-16-107
- Utah Transparency Advisory Board
  Utah Code 63A-18-101 et seq.
- Cybersecurity Affirmative Defense Act
  Utah Code § 78B-4-701 et seq.
- Utah Geographic Information Systems Advisory Council
  UT-ADC R895-9 et seq.
- Uniform Electronic Transactions Act
  Utah Code 46-4-101 et seq.

- Electronic Records in Government Agencies
  Utah Code § 46-4-501--503
- Public School Data Confidentiality and Disclosure
  R277-487

Appendix B. Privacy Maturity Survey Questions

	Privacy Program Criteria								
Maturity Level	Contracts with Clients & Partners	Infrastructure & Systems Management	Policy Documentation	Privacy Awareness & Training	Privacy Budget	Privacy Function	Privacy Incident Management	Privacy Personnel	Risk Assessment
0	Contracts do not address privacy	Procurement of IT-related products & services do not address privacy	There are no documented privacy policies	Contents of privacy policies are never communicated with personnel	There is no budget specifically allocated to privacy purposes	There is no assigned privacy office or function	There is no way to respond to suspected incidents	No one person with a job description of a privacy officer	Project plans & acquisition of IT-related products do not address privacy
1	Confidentiality clauses are included incontracts, but compliance cannot be monitored	Project and IT managers occasionally address privacy in plans & system-development	Multiple, inconsistent policies, or policies that do not address all privacy principles	Some contents of privacy policies are communicated to some personnel	No specific budget, but privacy dollars are spent ad hoc as add-ons to other projects	One person assigned privacy responsibilites serves as the privacy function	Some personnel have knowledge and skills to respond to suspected incidents	At least one person is assigned privacy responsibility, but time commitment exceeds the person's availability	Project & IT managers occasionally address privacy in project plans & system development
2	Personnel review contracts for consistency with privacy policies	Policies require that IT products, services, and system development address privacy	Policies address all privacy principles, and are displayed on relevant websites.	Privacy policies are communicated annually to personnel who encounter PII	Specific budget sufficient to cover basic travel & subscriptions, and modest amount for special projects	Privacy function is identified in org charts, reflecting sustained commitment	Privacy incidents have been effectively resolved, but at most only high-level policy or procedures are documented	At least one person devoted exclusively to privacy, with sufficient staff assistance	Policies require acquisition of IT-related products & services address privacy
3	Standard contractual clauses are in place, and compliance can be monitored	Detailed checklists & procedrues are used to insure compliance with policies	Policies address all privacy principles, are publicly displayed, and details for implementation are included	Privacy policies are communicated annually to personnel who encounter PII and are provided role-based training	Specific budget that includes enough money to accomplish most privacy objectives	An executive committee member is formally assigned to be privacy champion, and an annual report is presented to board	Personnel have detailed roles and responsibilities, and detailed policies & procedures are maintained	Privacy staff have clearly defined job descriptions that require certification as CIPP, including at least one with a leadership title, and enough staff to meet most privacy objectives	Detailed checklists, procedures and assigned personnel to ensure all IT-related projectsare compliant with privacy policies
4	Standard privacy & secuity clauses and internal compliance are measured annually	Compliance with privacy policies of IT products and services are measured and routinely tested	Business operations, processes, etc. are reviewed annually, and are updated as needed	Personnel comprehension of, and compliance with privacy policies is measured annually	A "Balanced Privacy Scorecard" or other approach used to determine a budget sufficient to cover all objectives	The privacy function is placed in a particular dept to support its strategy, and has direct access to Executive Committee	Suspected incidents are routinely measured & tested for privacy compliance, improvements are made based on this	Privacy staff have clearly defined job descriptions that require certification as CIPP, a Chief Privacy Officer, and enough staff to meet all privacy objectives	Information-related products and services are routinely measured and tested for complance with privacy policies
5	Controls in place to prevent adoption of privacy & security commitments that cannot be kept	Controls in place to ensure IT products and services are compliant with policy and procedure	Policies & standards are compared annually to others, and have achieved "best practices" status	Policy compliance is compared annually to others, and have achieved "best practices" status	Privacy function funds are exceeded by privacy dollars spent elsewhere in the organization	The head of the privacy function has direct access to leadership and is a part of business strategy decision-making	All incidents are resolved within 30 days	Privacy objectives are in the job descriptions of all personnel who access PII	Controls in place to prevent new IT-related products and services from being deployed without being compliant with privacy policies

Appendix C. Local Education Agency Privacy Compliance

One time	
Develop the following policies	
☐ Create a data governance plan	53E-9-301(7)
☐ Work with parents to create a PPRA policy	20 USC 1232h(c)
Beginning of year	
Provide the following notices to parents	
☐ Annual FERPA Notice	34 CFR 99.7
☐ Directory Information	34 CFR 99.37
☐ Military Recruiter/Institution of Higher Education notice (often included in Annual FERPA Notice)	20 USC 7908
☐ Notice of record exchange after school transfer (often included in Annual FERPA Notice)	34 CFR 99.34
☐ Collection Notice	53E-9-305(2)
☐ PPRA notice (must be given by hand, mail, or email)	20 USC 1232h(c)(2) 53E-9-203(4) – (5)
Throughout the year	
☐ Provide annual training to all staff that have access to student education records on federal and state privacy laws	53E-9-203
☐ Ensure that data are collected in accordance with your collection and survey notices	53E-9-305 53E-9-203 20 USC 1232h
☐ Ensure that parent and eligible student rights to access, seek to amend, and consent to disclose are followed	34 CFR 99, Subparts B, C, and D
☐ Ensure that all disclosures of student data follow FERPA, the contract requirements of the SDPA, and your data governance plan	34 CFR 99, Subpart D 53E-9-308 53E-9-309
☐ Update your metadata dictionary	53E-9-303

Information Security Officer To Do List

Throughout the year	
☐ Implement the CIS controls or a comparable IT security framework	R277-487-2(6) R277-487-3(14)
☐ Investigate any incidents to determine if they are significant data breaches	R277-487-2(17)
☐ Ensure that parents, eligible students, and USBE are notified of any significant data breaches	53E-9-304(2)(a) R277-487-3(12)

Records Officer To Do List

Throughout the year	
☐ Complete annual certification	63G-2-108
☐ Follow retention schedules	53E-9-306(3) R277-487-4
☐ Expunge records (as requested)	53E-9-306(1)(d) R277-487-4

Appendix D. Personal Privacy Oversight Commission

The Personal Privacy Oversight Commission is a 12 member commission with members appointed by the Governor, Attorney General and State Auditor. This commission is authorized to create and propose privacy standards for government entities, review privacy practice assessments reported by the GOPO/CPO, and report annually to the Judiciary Interim Committee to propose privacy standards and recommendations for legislation based on proposed standards. Commission members will work closely with the Government Operations Privacy Officer and the State Privacy Officer, reviewing specific government privacy practices recommended by these privacy officers. The current appointment commission members are:

Governor Appointments (63C-24-2-1(2)(b)):

- **Quinn Fowers:** Director of information technologies & digital services, Weber County -- member who, at the time of appointment provides internet technology services for a county or a municipality;
- **Aliahu "Alli" Bey:** President, Haight Bey & Associates, CEO, Totem Tech -- member with experience in cybersecurity;
- **Nayana Penmetsa:** Engineering manager, Plaid -- member representing private industry in technology;
- **Keith Squires:** Interim chief safety officer, University of Utah -- member representing law enforcement; and
- **Chris Koopman:** Executive director, The Center for Growth and Opportunity, Utah State University -- member with experience in data privacy law

Attorney General Appointments (63C-24-2-1(2)(d))

- **David Sonnenreich (formerly Jeff Gray)**: Utah Office of the Attorney General — a member with experience as a prosecutor or appellate attorney and with experience in civil liberties law; and
- **Mike Smith**: Utah County Sheriff — member representing law enforcement.

State Auditor Appointments (63C-24-2-1(2)(c))

- **Matthew Weller:** President, All West Communications; Board Member, Executive Education Advisory Board, University of Utah – David Eccles School of Business; Board Member, National Cable Television Cooperative -- member with experience in internet technology services;
- **Amy Knapp:** Former VP-Information Security and Compliance, O.C. Tanner -- member with experience in cybersecurity;

- **Brandon Greenwood:** CISO, VP Security & IT, Overstock; Board Member, SL|CISO -- member representing private industry in technology;
- **Phillip J. Windley, Ph.D.:** Formerly Principal Engineer, Office of IT, Brigham Young University; Founder and Organizer of Internet Identity Workshop and author of Digital Identity -- member with experience in data privacy law
- **Marina Lowe:** Legislative Counsel, ACLU of Utah -- member with experience in civil liberties law or policy and with specific experience in identifying the disparate impacts of the use of a technology or a policy on different populations.

Appendix E. Utah Fundamental Privacy Principles

1. **Individual Participation**
   Give people control of their information when possible.
2. **Lawful, Fair, and Responsible use**
   Collection, use and disclosure is:
   - Based on legal authority;
   - Not deceptive
   - Not discriminatory or harmful; and
   - Relevant and readably necessary for legitimate purposes.
3. **Data Minimization**
   The minimum amount of information is collected, used, or disclosed to accomplish the stated purpose for collecting the information.
4. **Transparency and Accountability**
   Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances. Accountability means being responsible and answerable for following data privacy laws and principles.
5. **Security**
   Appropriate administrative, technical and physical security practices to protect the confidentiality, integrity, availability and control of personal information.
6. **Due Diligence**
   Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.