Effective 7/1/2021

Part 1
General Provisions

63A-16-101 Title.

This chapter is known as the "Utah Technology Governance Act."

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-102 Definitions.

As used in this chapter:

(1) "Chief information officer" means the chief information officer appointed under Section 63A-16-201.

(2) "Data center" means a centralized repository for the storage, management, and dissemination of data.

(3) "Division" means the Division of Technology Services.

(4) "Enterprise architecture" means:

(a) information technology assets and functions that can be applied across state government, including:

(i) mainframes, servers, desktop devices, peripherals, and other computing devices;

(ii) networks;

(iii) enterprise-wide applications;

(iv) maintenance and help desk functions for common hardware and applications;

(v) standards for other computing devices, operating systems, common applications, and software; and

(vi) master contracts that are available for use by agencies for various systems, including operating systems, databases, enterprise resource planning and customer relationship management software, application development services, and enterprise integration; and

(b) support for information technology that can be applied across state government, including:

(i) technical support;

(ii) master software licenses; and

(iii) hardware and software standards.

(5)

(a) "Executive branch agency" means an agency or administrative subunit of state government.

(b) "Executive branch agency" does not include:

(i) the legislative branch;

(ii) the judicial branch;

(iii) the State Board of Education;

(iv) the Utah Board of Higher Education;

(v) institutions of higher education;

(vi) independent entities as defined in Section 63E-1-102; or

(vii) the following elective constitutional offices of the executive department:

(A) the state auditor;

(B) the state treasurer; and

(C) the attorney general.

(6) "Executive branch strategic plan" means the executive branch strategic plan created under Section 63A-16-202.

(7) "Individual with a disability" means an individual with a condition that meets the definition of "disability" in 42 U.S.C. Sec. 12102.
(8) "Information technology" means all computerized and auxiliary automated information handling, including:
  (a) systems design and analysis;
  (b) acquisition, storage, and conversion of data;
  (c) computer programming;
  (d) information storage and retrieval;
  (e) voice, video, and data communications;
  (f) requisite systems controls;
  (g) simulation; and
  (h) all related interactions between people and machines.
(9) "State information architecture" means a logically consistent set of principles, policies, and standards that guide the engineering of state government's information technology and infrastructure in a way that ensures alignment with state government's business and service needs.

Amended by Chapter 169, 2022 General Session

63A-16-103 Division of Technology Services.
(1) There is created within the department the Division of Technology Services.
(2) The division has authority to operate as an internal service fund agency as provided in Section 63J-1-410.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-104 Duties of division.
The division shall:
(1) lead state executive branch agency efforts to establish and reengineer the state's information technology architecture with the goal of coordinating central and individual agency information technology in a manner that:
  (a) ensures compliance with the executive branch agency strategic plan; and
  (b) ensures that cost-effective, efficient information and communication systems and resources are being used by agencies to:
    (i) reduce data, hardware, and software redundancy;
    (ii) improve system interoperability and data accessibility between agencies; and
    (iii) meet the agency's and user's business and service needs;
(2) coordinate an executive branch strategic plan for all agencies;
(3) develop and implement processes to replicate information technology best practices and standards throughout the executive branch;
(4) once every three years:
  (a) conduct an information technology security assessment via an independent third party:
    (i) to evaluate the adequacy of the division's and the executive branch agencies' data and information technology system security standards; and
    (ii) that will be completed over a period that does not exceed two years; and
  (b) communicate the results of the assessment described in Subsection (4)(a) to the appropriate executive branch agencies and to the president of the Senate and the speaker of the House of Representatives;

(5) subject to Subsection 63G-6a-109.5(9):
(a) advise executive branch agencies on project and contract management principles as they relate to information technology projects within the executive branch; and
(b) approve the acquisition of technology services and products by executive branch agencies as required under Section 63G-6a-109.5;
(6) work toward building stronger partnering relationships with providers;
(7) develop service level agreements with executive branch departments and agencies to ensure quality products and services are delivered on schedule and within budget;
(8) develop standards for application development including a standard methodology and cost-benefit analysis that all agencies shall utilize for application development activities;
(9) determine and implement statewide efforts to standardize data elements;
(10) coordinate with executive branch agencies to provide basic website standards for agencies that address common design standards and navigation standards, including:
(a) accessibility for individuals with disabilities in accordance with:
(i) the standards of 29 U.S.C. Sec. 794d; and
(ii) Section 63A-16-209;
(b) consistency with standardized government security standards;
(c) designing around user needs with data-driven analysis influencing management and development decisions, using qualitative and quantitative data to determine user goals, needs, and behaviors, and continual testing of the website, web-based form, web-based application, or digital service to ensure that user needs are addressed;
(d) providing users of the website, web-based form, web-based application, or digital service with the option for a more customized digital experience that allows users to complete digital transactions in an efficient and accurate manner; and
(e) full functionality and usability on common mobile devices;
(11) consider, when making a purchase for an information system, cloud computing options, including any security benefits, privacy, data retention risks, and cost savings associated with cloud computing options;
(12) develop systems and methodologies to review, evaluate, and prioritize existing information technology projects within the executive branch and report to the governor and the Government Operations Interim Committee in accordance with Section 63A-16-201 on a semiannual basis regarding the status of information technology projects;
(13) assist the Governor's Office of Planning and Budget with the development of information technology budgets for agencies;
(14) ensure that any training or certification required of a public official or public employee, as those terms are defined in Section 63G-22-102, complies with Title 63G, Chapter 22, State Training and Certification Requirements, if the training or certification is required:
(a) under this chapter;
(b) by the department; or
(c) by the division;
(15) provide support to executive branch agencies for the information technology assets and functions that are unique to the agency and are mission critical functions of the agency;
(16) provide in-house information technology staff support to executive branch agencies;
(17) establish a committee composed of agency user groups to coordinate division services with agency needs;
(18) assist executive branch agencies in complying with the requirements of any rule made by the chief information officer;

(19) develop and implement an effective enterprise architecture governance model for the executive branch;
(20) provide oversight of information technology projects that impact statewide information technology services, assets, or functions of state government to:
(a) control costs;
(b) ensure business value to a project;
(c) maximize resources;
(d) ensure the uniform application of best practices; and
(e) avoid duplication of resources;
(21) develop a method of accountability to agencies for services provided by the department through service agreements with the agencies;
(22) serve as a project manager for enterprise architecture, including management of applications, standards, and procurement of enterprise architecture;
(23) coordinate the development and implementation of advanced state telecommunication systems;
(24) provide services, including technical assistance:
(a) to executive branch agencies and subscribers to the services; and
(b) related to information technology or telecommunications;
(25) establish telecommunication system specifications and standards for use by:
(a) one or more executive branch agencies; or
(b) one or more entities that subscribe to the telecommunication systems in accordance with Section 63A-16-302;
(26) coordinate state telecommunication planning, in cooperation with:
(a) state telecommunication users;
(b) executive branch agencies; and
(c) other subscribers to the state's telecommunication systems;
(27) cooperate with the federal government, other state entities, counties, and municipalities in the development, implementation, and maintenance of:
(a)
(i) governmental information technology; or
(ii) governmental telecommunication systems; and
(b)
(i) as part of a cooperative organization; or
(ii) through means other than a cooperative organization;
(28) establish, operate, manage, and maintain:
(a) one or more state data centers; and
(b) one or more regional computer centers;
(29) design, implement, and manage all state-owned, leased, or rented land, mobile, or radio telecommunication systems that are used in the delivery of services for state government or the state's political subdivisions;
(30) in accordance with the executive branch strategic plan, implement minimum standards to be used by the division for purposes of compatibility of procedures, programming languages, codes, and media that facilitate the exchange of information within and among telecommunication systems;
(31) establish standards for the information technology needs of a collection of executive branch agencies or programs that share common characteristics relative to the types of stakeholders the agencies or programs serve, including:
(a) project management;

(b) application development; and
(c) subject to Subsections (5) and 63G-6a-109.5(9), procurement;
(32) provide oversight of information technology standards that impact multiple executive branch agency information technology services, assets, or functions to:
(a) control costs;
(b) ensure business value to a project;
(c) maximize resources;
(d) ensure the uniform application of best practices; and
(e) avoid duplication of resources;
(33) establish a system of accountability to user agencies through the use of service agreements; and
(34) provide the services described in Section 63A-16-109 for a state elected official or state employee who has been threatened.

Amended by Chapter 508, 2024 General Session

63A-16-105 Director -- Authority.
(1) The executive director shall, with the approval of the governor, appoint the director.
(2) The director:
(a) shall exercise all powers given to, and perform all duties imposed on, the division;
(b) has administrative jurisdiction over the division and each office within the division;
(c) may make changes in division personnel and service functions under the director's administrative jurisdiction; and
(d) may authorize a designee to perform appropriate responsibilities.
(3) The director may, to facilitate division management, establish offices and bureaus to perform division functions.
(4)
(a) The director may hire employees in the division and offices of the division as permitted by division resources.
(b) Except as provided in Subsection (5), each employee of the division is exempt from career service or classified service status as provided in Section 63A-17-301.
(5)
(a) Unless the employee voluntarily converted to an exempt position described in Section 63A-17-301, an employee of an executive branch agency who was a career service employee as of July 1, 2005, who was transferred to the division at the time it was newly created as the Department of Technology Services continues in the employee's career service status during the employee's service to the division if the duties of the position in the division are substantially similar to those in the employee's previous position.
(b) A career service employee transferred under the provisions of Subsection (5)(a), whose duties or responsibilities subsequently change, may not be converted to exempt status without the review process required by Subsection 63A-17-301(3).

Amended by Chapter 169, 2022 General Session

63A-16-107 Utah Open Data Portal Website.
(1) As used in this section:
(a) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
(b) "Public information" means:

(i) a record of a state governmental entity, a local governmental entity, or an independent entity that is classified as public under Title 63G, Chapter 2, Government Records Access and Management Act; or

(ii) subject to any specific limitations and requirements regarding the provision of financial information from the entity under Section 67-3-12, for an entity that is exempt from Title 63G, Chapter 2, Government Records Access and Management Act, records that would normally be classified as public if the entity were not exempt from Title 63G, Chapter 2, Government Records Access and Management Act.

(c) "Private, controlled, or protected information" means information classified as private, controlled, or protected under Title 63G, Chapter 2, Government Records Access and Management Act.

(d) "Website" means the Utah Open Data Portal Website created in this section.

(2) There is created the Utah Open Data Portal Website to be administered by the division.

(3) The website shall serve as a point of access for public information.

(4) The division shall:

(a) establish and maintain the website;

(b) provide equipment, resources, and personnel as needed to establish and maintain the website;

(c) provide a mechanism for a governmental entity to gain access to the website for the purpose of posting and modifying public information; and

(d) maintain an archive of all public information posted to the website.

(5) The timing for posting and the content of the public information posted to the website is the responsibility of the governmental entity posting the public information.

(6) A governmental entity may not post private, controlled, or protected information to the website.

(7) A person who negligently discloses private, controlled, or protected information is not criminally or civilly liable for improper disclosure of the information if the information is disclosed solely as a result of the preparation or publication of the website.

Amended by Chapter 249, 2023 General Session

63A-16-108 Digital verifiable credential and records.

(1) As used in this section:

(a) "Blockchain" means a distributed ledger of ordered electronic records that:

(i) is distributed across a network of computers;

(ii) utilizes technology to prevent the unauthorized alteration of electronic records; and

(iii) is mathematically verified.

(b) "Digital record schema" means a description of the data fields and tamper-evident technologies required to create a digital verifiable credential or digital verifiable record that can be registered on a distributed ledger technology.

(c) "Digital signature" means a tamper-evident, immutable, electronic seal that is equivalent in function and status to a notary seal issued by a government entity.

(d) "Digital verifiable credential" means a digital document that:

(i) attests to a fact;

(ii) is issued by a government entity;

(iii) can be mathematically verified; and

(iv) conveys rights, privileges, and legal enforceability equivalent to the possession of a physical credential of the same type.

(e) "Digital verifiable record" means a digital record that:

(i) is issued by a government entity or has been digitally signed by a government entity;
(ii) has a digital signature;
(iii) can be mathematically verified; and
(iv) conveys rights, privileges, and legal enforceability equivalent to the possession of a physical record of the same type.
(f) "Distributed ledger" means a decentralized database that is maintained by the consensus of replicated, shared, and synchronized digital data.
(g) "Government entity" means:
(i) the state;
(ii) a state agency; or
(iii) a political subdivision of the state.
(h) "Government operations privacy officer" means the government operations privacy officer described in Section 67-1-17.
(i) "State archivist" means the state archivist appointed under Section 63A-12-102.
(j) "State privacy officer" means the state privacy officer described in Section 67-3-13.
(k) "State registrar" means the state registrar of vital records appointed under Section 26B-8-102.
(2) The Division of Technology Services shall:
(a) provide recommendations to government entities regarding:
(i) appropriate digital record schemas that allow a government to issue a digital verifiable credential or record;
(ii) policies and procedures to protect the privacy of personal identifying information maintained within distributed ledger programs;
(iii) the manner and format in which an issuer may certify a document through blockchain; and
(iv) processes and procedures for the preservation, auditability, integrity, security, and confidentiality of digital verifiable credentials and records;
(b) create a pilot program for the implementation of digital verifiable credentials by governmental entities; and
(c) report to Public Utilities, Energy, and Technology Interim Committee by October 31, 2023, on the duties described in Subsections (2)(a) and (b).
(3) In performing the duties described in Subsections (2)(a) and (b), the Division of Technology Services shall consult with:
(a) the state archivist;
(b) the state privacy officer;
(c) the government operations privacy officer;
(d) the state registrar;
(e) private industry professionals with relevant expertise;
(f) the Utah League of Cities and Towns; and
(g) an association of counties in the state.

Enacted by Chapter 201, 2023 General Session

63A-16-109 Removal of state elected official or employee personal identifying information.
(1) As used in this section:
(a) "Open web" means the Internet used for everyday activities like browsing, searching, reading media, online shopping, or other website or online applications.
(b) "Personal identifying information" means the following:
(i) physical home address and personal email address;
(ii) home telephone number and personal mobile telephone number;

(iii) driver license or other government-issued identification; or
(iv) social security number.
(c)
(i) "State elected official" means a person who holds an office in state government that is required by law to be filled by an election, including the offices of governor, lieutenant governor, attorney general, state auditor, state treasurer, and legislator.
(ii) "State elected official" does not include a judge.
(d) "State employee who has been threatened" means an individual:
(i)
(A) who is a cabinet level official or senior staff of the governor; or
(B) who is an employee of the state executive branch and meets selective criteria implemented by the division that are established by rule made under Subsection (4); and
(ii) whose life or safety has been threatened in the course of performing the individual's state duties through a text, phone call, email, postal delivery, face-to-face encounter, or website or online application.
(2) At the written request of a state elected official or a state employee who has been threatened, the division shall within 30 days of receipt of the request:
(a) search the open web for personal identifying information that is about the state elected official or state employee who has been threatened;
(b) when possible, remove the personal identifying information found under Subsection (2)(a) from the open web; and
(c) conduct continuous monthly removal when possible of personal identifying information from the open web.
(3) The chief information officer may contract, in accordance with Title 63G, Chapter 6a, Utah Procurement Code, with a third party to provide the services described in Subsection (2).
(4) The chief information officer may by rule made in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, establish requirements related to:
(a) what information the state elected official or state employee who has been threatened shall provide the division as part of the request described in Subsection (2);
(b) procedures for submitting the written request to the division; and
(c) establishing the selective criteria used to determine whether a state employee may receive the services described in Subsection (2).
(5) The division may not charge a rate for the services provided under this section.
(6)
(a) In addition to the governmental immunity granted in Title 63G, Chapter 7, Governmental Immunity Act of Utah, the division is not liable for actions performed under this section except as a result of intentional misconduct or gross negligence including reckless, willful, or wanton misconduct.
(b) This section does not create a special duty of care.
(7) A federal, state, or local government record is not subject to this section, even if the government record contains personal identifying information.

Enacted by Chapter 508, 2024 General Session

63A-16-110 Use of authorized domain extensions for government websites.
(1) As used in this section:
(a) "Authorized top-level domain" means any of the following suffixes that follow the domain name in a website address:

(i) gov;
(ii) edu; and
(iii) mil.
(b) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
(c) "Government website" means the same as that term is defined in Section 63A-19-101.
(d) "Person" means the same as that term is defined in Section 63G-2-103.
(e) "School" means a public elementary or secondary school.
(2) Beginning July 1, 2025, a governmental entity shall use an authorized top-level domain for:
(a) the website address for the governmental entity's government website; and
(b) the email addresses used by the governmental entity and the governmental entity's employees.
(3) Notwithstanding Subsection (2), a governmental entity may operate a website that uses a top-level domain that is not an authorized top-level domain if:
(a)
(i) a reasonable person would not mistake the website as the governmental entity's primary government website; and
(ii) the government website is:
(A) solely for internal use and not intended for use by members of the public;
(B) temporary and in use by the governmental entity for a period of less than one year; or
(C) related to an event, program, or informational campaign operated by the governmental entity in partnership with another person that is not a governmental entity; or
(b) the governmental entity is a school district or a school that is not an institution of higher education and the use of an authorized top-level domain is otherwise prohibited, provided that once the use of an authorized top-level domain is not otherwise prohibited, the school district or school shall transition to an authorized top-level domain within 15 months.
(4) The chief information officer appointed under Section 63A-16-201 may authorize a waiver of the requirement in Subsection (2) if:
(a) there are extraordinary circumstances under which use of an authorized domain extension would cause demonstrable harm to citizens or businesses; and
(b) the executive director or chief executive of the governmental entity submits a written request to the chief information officer that includes a justification for the waiver.

Renumbered and Amended by Chapter 475, 2025 General Session