Effective 7/1/2021

Chapter 16
Utah Technology Governance Act

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

Part 2
Chief Information Officer

63A-16-201 Chief information officer -- Appointment -- Powers -- Reporting.

(1) The director of the division shall serve as the state's chief information officer.

(2) The chief information officer shall:

(a) advise the governor on information technology policy; and

(b) perform those duties given the chief information officer by statute.

(3)

(a) The chief information officer shall report annually to:

(i) the governor; and

(ii) the Government Operations Interim Committee.

(b) The report required under Subsection (3)(a) shall:

(i) summarize the state's current and projected use of information technology;

(ii) summarize the executive branch strategic plan including a description of major changes in the executive branch strategic plan;

(iii) provide a brief description of each state agency's information technology plan;

(iv) include the status of information technology projects described in Subsection 63A-16-104(10);

(v) include the performance report described in Section 63A-16-211; and

(vi) include the expenditure of the funds provided for electronic technology, equipment, and hardware.

Amended by Chapter 43, 2023 General Session

63A-16-202 Executive branch information technology strategic plan.

(1) In accordance with this section, the chief information officer shall prepare an executive branch information technology strategic plan:

(a) that complies with this chapter; and

(b) that includes:

(i) a strategic plan for the:

(A) interchange of information related to information technology between executive branch agencies;

(B) coordination between executive branch agencies in the development and maintenance of information technology and information systems, including the coordination of agency information technology plans described in Section 63A-16-203; and

(C) protection of the privacy of individuals who use state information technology or information systems, including the implementation of industry best practices for data and system security;

(ii) priorities for the development and implementation of information technology or information systems including priorities determined on the basis of:

(A) the importance of the information technology or information system; and

(B) the time sequencing of the information technology or information system; and

(iii) maximizing the use of existing state information technology resources.

(2) In the development of the executive branch strategic plan, the chief information officer shall consult with all cabinet level officials.

(3)

(a) Unless withdrawn by the chief information officer or the governor in accordance with Subsection (3)(b), the executive branch strategic plan takes effect 30 days after the day on which the executive branch strategic plan is submitted to:

(i) the governor; and

(ii) the Government Operations Interim Committee.

(b) The chief information officer or the governor may withdraw the executive branch strategic plan submitted under Subsection (3)(a) if the governor or chief information officer determines that the executive branch strategic plan:

(i) should be modified; or
(ii) for any other reason should not take effect.
(c) The Government Operations Interim Committee may make recommendations to the governor and to the chief information officer if the commission determines that the executive branch strategic plan should be modified or for any other reason should not take effect.
(d) Modifications adopted by the chief information officer shall be resubmitted to the governor and the Government Operations Interim Committee for their review or approval as provided in Subsections (3)(a) and (b).
(4)
(a) The chief information officer shall annually, on or before January 1, modify the executive branch information technology strategic plan to incorporate security standards that:
(i) are identified as industry best practices in accordance with Subsections 63A-16-104(3) and (4); and
(ii) can be implemented within the budget of the department or the executive branch agencies.
(b) The chief information officer shall inform the speaker of the House of Representatives and the president of the Senate on or before January 1 of each year if best practices identified in Subsection (4)(a)(i) are not adopted due to budget issues considered under Subsection (4)(a)(ii).
(5) Each executive branch agency shall implement the executive branch strategic plan by adopting an agency information technology plan in accordance with Section 63A-16-203.

Amended by Chapter 169, 2022 General Session

63A-16-203 Agency information technology plans.
(1)
(a) On or before July 1 each year, each executive branch agency shall submit an agency information technology plan to the chief information officer at the department level, unless the governor or the chief information officer request an information technology plan be submitted by a subunit of a department, or by an executive branch agency other than a department.
(b) The information technology plans required by this section shall be in the form and level of detail required by the chief information officer, by administrative rule under Section 63A-16-205, and shall include, at least:
(i) the information technology objectives of the agency;
(ii) any performance measures used by the agency for implementing the agency's information technology objectives;
(iii) any planned expenditures related to information technology;
(iv) the agency's need for appropriations for information technology;
(v) how the agency's development of information technology coordinates with other state and local governmental entities;
(vi) any efforts the agency has taken to develop public and private partnerships to accomplish the information technology objectives of the agency;
(vii) the efforts the executive branch agency has taken to conduct transactions electronically in compliance with Section 46-4-503; and
(viii) the executive branch agency's plan for the timing and method of verifying the department's security standards, if an agency intends to verify the department's security standards for the data that the agency maintains or transmits through the department's servers.
(2)

(a) Except as provided in Subsection (2)(b), an agency information technology plan described in Subsection (1) shall comply with the executive branch strategic plan established in accordance with Section 63A-16-202.
(b) If the executive branch agency submitting the agency information technology plan justifies the need to depart from the executive branch strategic plan, an agency information technology plan may depart from the executive branch strategic plan to the extent approved by the chief information officer.
(3) The chief information officer shall review each agency plan to determine:
(a)
(i) whether the agency plan complies with the executive branch strategic plan and state information architecture; or
(ii) to the extent that the agency plan does not comply with the executive branch strategic plan or state information architecture, whether the executive branch entity is justified in departing from the executive branch strategic plan, or state information architecture; and
(b) whether the agency plan meets the information technology and other needs of:
(i) the executive branch agency submitting the plan; and
(ii) the state.
(4) After the chief information officer conducts the review described in Subsection (3) of an agency information technology plan, the chief information officer may:
(a) approve the agency information technology plan;
(b) disapprove the agency information technology plan; or
(c) recommend modifications to the agency information technology plan.
(5) An executive branch agency or the department may not submit a request for appropriation related to information technology or an information technology system to the governor in accordance with Section 63J-1-201 until after the executive branch agency's information technology plan is approved by the chief information officer.

Amended by Chapter 169, 2022 General Session

63A-16-205 Rulemaking -- Policies.
(1)
(a) Except as provided in Subsection (2), the chief information officer shall, by rule made in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act:
(i) establish standards that impose requirements on executive branch agencies related to the security of the statewide area network;
(ii) establish standards for when an agency must obtain approval before obtaining items described in Subsection 63G-6a-109.5(2);
(iii) specify the detail and format required in an agency information technology plan submitted in accordance with Section 63A-16-203;
(iv) establish standards related to the privacy policies of websites operated by or on behalf of an executive branch agency;
(v) subject to Subsection 63G-6a-109.5(9), establish standards for the acquisition, licensing, and sale of computer software;
(vi) specify the requirements for the project plan and business case analysis required under Section 63G-6a-109.5;
(vii) provide for project oversight of agency technology projects when required under Section 63G-6a-109.5;

(viii) establish, in accordance with Subsection 63G-6a-109.5(3), the implementation of the needs assessment for information technology purchases;
(ix) establish telecommunications standards and specifications in accordance with Subsection 63G-6a-109.5(25); and
(x) establish standards for accessibility of information technology by individuals with disabilities in accordance with Section 63A-16-209.
(b) The rulemaking authority granted by Subsection (1)(a) is in addition to any other rulemaking authority granted under this chapter.
(2)
(a) Notwithstanding Title 63G, Chapter 3, Utah Administrative Rulemaking Act, and subject to Subsection (2)(b), the chief information officer may adopt a policy that outlines procedures to be followed by the chief information officer in facilitating the implementation of this title by executive branch agencies if the policy:
(i) is consistent with the executive branch strategic plan; and
(ii) is not required to be made by rule under Subsection (1) or Section 63G-3-201.
(b)
(i) A policy adopted by the chief information officer under Subsection (2)(a) may not take effect until 30 days after the day on which the chief information officer submits the policy to:
(A) the governor; and
(B) all cabinet level officials.
(ii) During the 30-day period described in Subsection (2)(b)(i), cabinet level officials may review and comment on a policy submitted under Subsection (2)(b)(i).
(3)
(a) Notwithstanding Subsection (1) or (2) or Title 63G, Chapter 3, Utah Administrative Rulemaking Act, without following the procedures of Subsection (1) or (2), the chief information officer may adopt a security procedure to be followed by executive branch agencies to protect the statewide area network if:
(i) broad communication of the security procedure would create a significant potential for increasing the vulnerability of the statewide area network to breach or attack; and
(ii) after consultation with the chief information officer, the governor agrees that broad communication of the security procedure would create a significant potential increase in the vulnerability of the statewide area network to breach or attack.
(b) A security procedure described in Subsection (3)(a) is classified as a protected record under Title 63G, Chapter 2, Government Records Access and Management Act.
(c) The chief information officer shall provide a copy of the security procedure as a protected record to:
(i) the chief justice of the Utah Supreme Court for the judicial branch;
(ii) the speaker of the House of Representatives and the president of the Senate for the legislative branch;
(iii) the chair of the Utah Board of Higher Education; and
(iv) the chair of the State Board of Education.

Amended by Chapter 43, 2023 General Session

63A-16-206 Coordination within the executive branch -- Cooperation with other branches.
(1) In accordance with the executive branch strategic plan and the requirements of this title, the chief information officer shall coordinate the development of information technology systems between two or more executive branch agencies subject to:

(a) the budget approved by the Legislature; and
(b) Title 63J, Chapter 1, Budgetary Procedures Act.
(2) In addition to the coordination described in Subsection (1), the chief information officer shall promote cooperation regarding information technology between branches of state government.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-207 Delegation of division functions.
(1)
(a) If the conditions of Subsections (1)(b) and (2) are met and subject to the other provisions of this section, the chief information officer may delegate a function of the division to another executive branch agency or an institution of higher education by contract or other means authorized by law.
(b) The chief information officer may delegate a function of the division as provided in Subsection (1)(a) if in the judgment of the director of the executive branch agency and the chief information officer:
(i) the executive branch agency or institution of higher education has requested that the function be delegated;
(ii) the executive branch agency or institution of higher education has the necessary resources and skills to perform or control the function to be delegated; and
(iii) the function to be delegated is a unique or mission-critical function of the agency or institution of higher education.
(2) The chief information officer may delegate a function of the division only when the delegation results in net cost savings or improved service delivery to the state as a whole or to the unique mission critical function of the executive branch agency.
(3) The delegation of a function under this section shall:
(a) be in writing;
(b) contain all of the following:
(i) a precise definition of each function to be delegated;
(ii) a clear description of the standards to be met in performing each function delegated;
(iii) a provision for periodic administrative audits by the division;
(iv) a date on which the agreement shall terminate if the agreement has not been previously terminated or renewed; and
(v) any delegation of division staff to the agency to support the function in-house with the agency and rates to be charged for the delegated staff; and
(c) include a cost-benefit analysis justifying the delegation.
(4) An agreement to delegate functions to an executive branch agency or an institution of higher education may be terminated by the division if the results of an administrative audit conducted by the division reveals a lack of compliance with the terms of the agreement by the executive branch agency or institution of higher education.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-208 Delegation of division staff to executive branch agencies -- Prohibition against executive branch agency information technology staff.
(1)

(a) The chief information officer shall assign division staff to serve an agency in-house if the chief information officer and the executive branch agency director jointly determine it is appropriate to provide information technology services to:
(i) the agency's unique mission-critical functions and applications;
(ii) the agency's participation in and use of statewide enterprise architecture; and
(iii) the agency's use of coordinated technology services with other agencies that share similar characteristics with the agency.
(b)
(i) An agency may request the chief information officer to assign in-house staff support from the division.
(ii) The chief information officer shall respond to the agency's request for in-house staff support in accordance with Subsection (1)(a).
(c) The division shall enter into service agreements with an agency when division staff is assigned in-house to the agency under the provisions of this section.
(d) An agency that receives in-house staff support assigned from the division under the provision of this section is responsible for paying the rates charged by the division for that staff as established under Section 63A-16-301.
(2)
(a) An executive branch agency may not create a full-time equivalent position or part-time position, or request an appropriation to fund a full-time equivalent position or part-time position under the provisions of Section 63J-1-201 for the purpose of providing information technology services to the agency unless:
(i) the chief information officer has approved a delegation under Section 63A-16-207; and
(ii) the division conducts an audit in relation to Section 63A-16-102 and finds that the delegation of information technology services to the agency meets the requirements of Section 63A-16-207.
(b) The prohibition against a request for appropriation under Subsection (2)(a) does not apply to a request for appropriation needed to pay rates imposed under Subsection (1)(d).

Amended by Chapter 169, 2022 General Session

63A-16-209 Accessibility standards for executive branch agency information technology.
(1) The chief information officer shall establish, by rule made in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act:
(a) minimum standards for accessibility of executive branch agency information technology by an individual with a disability that:
(i) include accessibility criteria for:
(A) agency websites;
(B) hardware and software procured by an executive branch agency; and
(C) information systems used by executive branch agency employees;
(ii) include a protocol to evaluate the standards via testing by individuals with a variety of access limitations; and
(iii) are, at minimum, consistent with the most recent Web Content Accessibility guidelines published by the World Wide Web Consortium; and
(b) grievance procedures for an individual with a disability who is unable to access executive branch agency information technology, including:
(i) a process for an individual with a disability to report the access issue to the chief information officer; and

(ii) a mechanism through which the chief information officer can respond to the report.
(2) The chief information officer shall update the standards described in Subsection (1)(a) at least every three years to reflect advances in technology.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-210 Chief information security officer.
(1) The chief information officer shall appoint a chief information security officer.
(2) The chief information security officer described in Subsection (1) shall:
(a) assess cybersecurity risks;
(b) coordinate with executive branch agencies to assess the sensitivity of information; and
(c) manage cybersecurity support for the department and executive branch agencies.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-211 Report to the Legislature.
The division shall, in accordance with Section 63A-16-201, before November 1 each year, report to the Government Operations Interim Committee on:
(1) performance measures that the division uses to assess the division's effectiveness in performing the division's duties under this part; and
(2) the division's performance, evaluated in accordance with the performance measures described in Subsection (1).

Amended by Chapter 169, 2022 General Session

63A-16-214 Zero trust architectures -- Implementation -- Requirements -- Reporting.
(1) As used in this section:
(a) "Endpoint detection and response" means a cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.
(b) "Governmental entity" means:
(i) the state;
(ii) a political subdivision of the state; and
(iii) an entity created by the state or a political subdivision of the state, including an agency, board, bureau, commission, committee, department, division, institution, instrumentality, or office.
(c) "Multi-factor authentication" means using two or more different types of identification factors to authenticate a user's identity for the purpose of accessing systems and data, which may include:
(i) knowledge-based factors, which require the user to provide information that only the user knows, such as a password or personal identification number;
(ii) possession-based factors, which require the user to have a physical item that only the user possesses, such as a security token, key fob, subscriber identity module card, or smart phone application; or
(iii) inherence-based credentials, which require the user to demonstrate specific known biological traits attributable only to the user, such as fingerprints or facial recognition.
(d) "Zero trust architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy that employs continuous monitoring, risk-based access controls, secure identity and access management practices,

and system security automation techniques to address the cybersecurity risk from threats inside and outside traditional network boundaries.

(2) This section applies to:

(a) all systems and data owned, managed, maintained, or utilized by or on behalf of an executive branch agency to access state systems or data; and

(b) all hardware, software, internal systems, and essential third-party software, including for on-premises, cloud, and hybrid environments.

(3)

(a) On or before November 1, 2023, the chief information officer shall develop uniform technology policies, standards, and procedures for use by executive branch agencies in implementing zero trust architecture and multi-factor authentication on all systems in accordance with this section.

(b) On or before July 1, 2024, the division shall consider adopting the enterprise security practices described in this section and consider implementing zero trust architecture and robust identity management practices, including:

(i) multi-factor authentication;

(ii) cloud-based enterprise endpoint detection and response solutions to promote real-time detection, and rapid investigation and remediation capabilities; and

(iii) robust logging practices to provide adequate data to support security investigations and proactive threat hunting.

(4)

(a) If implementing a zero trust architecture and multi-factor authentication, the division shall consider prioritizing the use of third-party cloud computing solutions that meet or exceed industry standards.

(b) The division shall consider giving preference to zero trust architecture solutions that comply with, are authorized by, or align to applicable federal guidelines, programs, and frameworks, including:

(i) the Federal Risk and Authorization Management Program;

(ii) the Continuous Diagnostics and Mitigation Program; and

(iii) guidance and frameworks from the National Institute of Standards and Technology.

(5)

(a) In procuring third-party cloud computing solutions, the division may utilize established purchasing vehicles, including cooperative purchasing contracts and federal supply contracts, to facilitate efficient purchasing.

(b) The chief information officer shall establish a list of approved vendors that are authorized to provide zero trust architecture to governmental entities in the state.

(c) If an executive branch agency determines that procurement of a third-party cloud computing solution is not feasible, the executive branch agency shall provide a written explanation to the division of the reasons that a cloud computing solution is not feasible, including:

(i) the reasons why the executive branch agency determined that a third-party cloud computing solution is not feasible;

(ii) specific challenges or difficulties of migrating existing solutions to a cloud environment; and

(iii) the total expected cost of ownership of existing or alternative solutions compared to a cloud computing solution.

(6)

(a) On or before November 30 of each year, the chief information officer shall report on the progress of implementing zero trust architecture and multi-factor authentication to:

(i) the Public Utilities, Energy, and Technology Interim Committee; and

(ii) the Cybersecurity Commission created in Section 63C-25-201.

(b) The report described in Subsection (6)(a) may include information on:

(i) applicable guidance issued by the United States Cybersecurity and Infrastructure Security Agency; and

(ii) the progress of the division, executive branch agencies, and governmental entities with respect to:

(A) shifting away from a paradigm of trusted networks toward implementation of security controls based on a presumption of compromise;

(B) implementing principles of least privilege in administering information security programs;

(C) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(D) identifying incidents quickly; and

(E) isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for cyber threat intelligence or law enforcement purposes.

Enacted by Chapter 484, 2023 General Session

Part 3
Information Technology Services and Rates

63A-16-301 Cost based services -- Rates -- Submission to rate committee.

(1) The chief information officer shall:

(a) at the lowest practical cost, manage the delivery of efficient and cost-effective information technology and telecommunication services for:

(i) all executive branch agencies; and

(ii) entities that subscribe to the services in accordance with Section 63A-16-302; and

(b) provide priority service to public safety agencies.

(2)

(a) In accordance with this Subsection (2), the chief information officer shall prescribe a schedule of rates for all services rendered by the division to:

(i) an executive branch entity; or

(ii) an entity that subscribes to services rendered by the division in accordance with Section 63A-16-302.

(b) Each rate included in the schedule of rates required by Subsection (2)(a):

(i) shall be equitable;

(ii) should be based upon a zero based, full cost accounting of activities necessary to provide each service for which a rate is established; and

(iii) for each service multiplied by the projected consumption of the service recovers no more or less than the full cost of each service.

(c) Before charging a rate for its services to an executive branch agency or to a subscriber of services other than an executive branch agency, the chief information officer shall:

(i) submit the proposed rates and cost analysis to the Rate Committee established in Section 63A-1-114; and

(ii) obtain the approval of the Legislature as required by Section 63J-1-410.

(d) The chief information officer shall periodically conduct a market analysis of proposed rates, which analysis shall include a comparison of the division's rates with the rates of other public or private sector providers where comparable services and rates are reasonably available.

Amended by Chapter 169, 2022 General Session

63A-16-302 Executive branch agencies -- Subscription by institutions.

(1) An executive branch agency in accordance with its agency information technology plan approved by the chief information officer shall:
  (a) subscribe to the information technology services provided by the division; or
  (b) contract with one or more alternate private providers of information technology services if the chief information officer determines that the purchase of the services from a private provider will:
    (i) result in:
      (A) cost savings;
      (B) increased efficiency; or
      (C) improved quality of services; and
    (ii) not impair the interoperability of the state's information technology services.
(2) An institution of higher education may subscribe to the services provided by the division if:
  (a) the president of the institution recommends that the institution subscribe to the services of the division; and
  (b) the Utah Board of Higher Education determines that subscription to the services of the division will result in cost savings or increased efficiency to the institution.
(3) The following may subscribe to information technology services by requesting that the services be provided from the division:
  (a) the legislative branch;
  (b) the judicial branch;
  (c) the State Board of Education;
  (d) a political subdivision of the state;
  (e) an agency of the federal government;
  (f) an independent entity as defined in Section 63E-1-102; and
  (g) an elective constitutional officer of the executive department as defined in Subsection 63A-16-102(5)(b)(vii).

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-302.1 Reporting on consolidation of certain information technology services.

(1) The division shall, in collaboration with the Cybersecurity Commission created in Section 63C-27-201, identify opportunities, limitations, and barriers to enhancing the overall cybersecurity resilience of the state by consolidating:
  (a) certain information technology services utilized by governmental entities; and
  (b) to the extent feasible, the information technology networks that are operated or utilized by governmental entities.
(2) On or before November 15, 2023, the division shall report the information described in Subsection (1) to:
  (a) the Government Operations Interim Committee;
  (b) the General Government Appropriations Subcommittee; and
  (c) the Cybersecurity Commission created in Section 63C-27-201.

Amended by Chapter 271, 2025 General Session

Part 5
Integrated Technology

63A-16-501 Definitions.

As used in this part:

(1) "Center" means the Utah Geospatial Resource Center created in Section 63A-16-505.
(2) "Database" means the State Geographic Information Database created in Section 63A-16-506.
(3) "Geographic Information System" or "GIS" means a computer driven data integration and map production system that interrelates disparate layers of data to specific geographic locations.
(4) "State Geographic Information Database" means the database created in Section 63A-16-506.
(5) "Statewide Global Positioning Reference Network" or "network" means the network created in Section 63A-16-508.

Amended by Chapter 169, 2022 General Session

63A-16-504 Information technology plan.

(1) In accordance with this section, the division shall submit an information technology plan to the chief information officer.
(2) The information technology plan submitted by the division under this section shall include:
  (a) the information required by Section 63A-16-202;
  (b) a list of the services the division offers or plans to offer; and
  (c) a description of the performance measures used by the division to measure the quality of the services described in Subsection (2)(b).
(3)
  (a) In submitting the information technology plan under this section, the division shall comply with Section 63A-16-203.
  (b) The information technology plan submitted by the division under this section is subject to the approval of the chief information officer as provided in Section 63A-16-203.

Amended by Chapter 169, 2022 General Session

63A-16-505 Utah Geospatial Resource Center.

(1) There is created the Utah Geospatial Resource Center as part of the division.
(2) The center shall:
  (a) provide geographic information system services to state agencies under rules made under Section 63A-16-104 and policies established by the office;
  (b) provide geographic information system services to federal government, local political subdivisions, and private persons under rules and policies established by the office;
  (c) manage the State Geographic Information Database; and
  (d) establish standard format, lineage, and other requirements for the database.
(3)
  (a) There is created a position of surveyor within the center.
  (b) The surveyor under this Subsection (3) shall:

(i) be licensed as a professional land surveyor under Title 58, Chapter 22, Professional Engineers and Professional Land Surveyors Licensing Act;
(ii) provide technical support to the office of lieutenant governor in the lieutenant governor's evaluation under Section 67-1a-6.5 of a proposed boundary action, as defined in Section 17-73-101;
(iii) as requested by a county surveyor, provide technical assistance to the county surveyor with respect to the county surveyor's responsibilities under Section 17-73-507;
(iv) fulfill the duties described in Section 17-61-102, if engaged to do so as provided in that section;
(v) assist the State Tax Commission in processing and quality assurance of boundary descriptions or maps into digital format for inclusion in the State Geographic Information Database;
(vi) coordinate with county recorders and surveyors to create a statewide parcel layer in the State Geographic Information Database containing parcel boundary, parcel identifier, parcel address, owner type, and county recorder contact information; and
(vii) facilitate and integrate the collection efforts of local government and federal agencies for data collection to densify and enhance the statewide Public Land Survey System reference network in the State Geographic Information Database.

(4) The office may:
(a) make rules and establish policies to govern the center and the center's operations; and
(b) set fees for the services provided by the center.

(5) The state may not sell information obtained from counties under Subsection (3)(b)(v).

Amended by Chapter 17, 2025 Special Session 1

63A-16-506 State Geographic Information Database.

(1) There is created a State Geographic Information Database to be managed by the center.

(2) The database shall:
(a) serve as the central reference for all information contained in any GIS database by any state agency;
(b) serve as a clearing house and repository for all data layers required by multiple users;
(c) serve as a standard format for geographic information acquired, purchased, or produced by any state agency;
(d) include an accurate representation of all civil subdivision boundaries of the state; and
(e) for each public highway, as defined in Section 72-1-102, in the state, include an accurate representation of the highway's centerline, physical characteristics, and associated street address ranges.

(3) The center shall, in coordination with municipalities, counties, emergency communications centers, and the Department of Transportation:
(a) develop the information described in Subsection (2)(e); and
(b) update the information described in Subsection (2)(e) in a timely manner after a county recorder records a final plat.

(4) The center, in coordination with county assessors and metropolitan planning organizations:
(a) shall inventory existing housing units and their general characteristics within each county of the first or second class to support infrastructure planning and economic development in each of those counties; and

(b) may inventory existing housing units and their general characteristics within one or more counties of the third, fourth, fifth, or sixth class to support infrastructure planning and economic development in one or more of those counties.

(5)
(a) The center shall, in coordination with the Governor's Office of Planning and Budget and county assessors, annually compile a statewide GIS database of all government-owned property parcels in internet-accessible, searchable, and map format.
(b) The database described in Subsection (5)(a) shall include a parcel's:
(i) number, if available;
(ii) owner;
(iii) location; and
(iv) size.

(6) Each state agency that acquires, purchases, or produces digital geographic information data shall:
(a) inform the center of the existence of the data layers and their geographic extent;
(b) allow the center access to all data classified public; and
(c) comply with any database requirements established by the center.

(7) At least annually, the State Tax Commission shall deliver to the center information the State Tax Commission receives under Section 67-1a-6.5 relating to the creation or modification of the boundaries of political subdivisions.

(8) The boundary of a political subdivision within the State Geographic Information Database is the official boundary of the political subdivision for purposes of meeting the needs of the United States Bureau of the Census in identifying the boundary of the political subdivision.

Amended by Chapter 197, 2023 General Session

63A-16-508 Statewide Global Positioning Reference Network created -- Rulemaking authority.

(1)
(a) There is created the Statewide Global Positioning Reference Network to improve the quality of geographic information system data and the productivity, efficiency, and cost-effectiveness of government services.
(b) The network shall provide a system of permanently mounted, fully networked, global positioning system base stations that will provide real time radio navigation and establish a standard statewide coordinate reference system.
(c) The center shall administer the network.

(2)
(a) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the chief information officer shall make rules providing for operating policies and procedures for the network.
(b) When making rules under this section, the chief information officer shall consider:
(i) network development that serves a public purpose;
(ii) increased productivity and efficiency for state agencies; and
(iii) costs and longevity of the network.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-509 Monument Replacement and Restoration Committee.

(1) As used in this section:
(a) "Committee" means the Monument Replacement and Restoration Committee created in this section.
(b) "Corner" means the same as that term is defined in Section 17-73-101.
(c) "Monument" means the same as that term is defined in Section 17-73-101.
(2)
(a) There is created the Monument Replacement and Restoration Committee composed of the following seven members:
(i) five members appointed by an organization or association that represents Utah counties:
(A) that have knowledge and understanding of the Public Land Survey System; and
(B) who each represents a different county; and
(ii) two members, appointed by the center, who have a knowledge and understanding of the Public Land Survey System.
(b)
(i) Except as provided in Subsection (2)(b)(ii), a member appointed to the committee is appointed for a four-year term.
(ii) The director of the center shall, at the time an entity appoints or reappoints an individual to serve on the committee, adjust the length of the appointed individual's term, as necessary, to ensure that the terms of committee members are staggered so that approximately half of the committee members are appointed every two years.
(iii) When a vacancy occurs on the committee for any reason, the replacement appointee shall serve on the committee for the unexpired term.
(c) The committee shall elect one committee member to serve as chair of the committee for a term of two years.
(d) A majority of the committee constitutes a quorum, and the action of a majority of a quorum constitutes the action of the committee.
(e)
(i) The center shall provide staff support to the committee.
(ii) An individual who is a member of the committee may not serve as staff to the committee.
(f) A member of the committee may not receive compensation for the member's service on the committee.
(g) The committee may adopt bylaws to govern the committee's operation.
(3)
(a) The committee shall administer a grant program to assist counties in maintaining and protecting corners or monuments.
(b) A county wishing to receive a grant under the program described in Subsection (3)(a) shall submit to the committee an application that:
(i) identifies one or more monuments in the county that are in need of protection or rehabilitation;
(ii) establishes a plan that is consistent with federal law or rule to protect or rehabilitate each monument identified under Subsection (3)(b)(i); and
(iii) requests a specific amount of funding to complete the plan established under Subsection (3)(b)(ii).
(c) The committee shall:
(i) adopt criteria to:
(A) evaluate whether a monument identified by a county under Subsection (3)(b)(i) needs protection or rehabilitation; and

(B) identify which monuments identified by a county under Subsection (3)(b)(i) have the greatest need of protection or rehabilitation;
(ii) evaluate each application submitted by a county under Subsection (3)(b) using the criteria adopted by the committee under Subsection (3)(c)(i);
(iii) subject to sufficient funding and Subsection (3)(d), award grants to counties whose applications are most favorably evaluated under Subsection (3)(c)(ii); and
(iv) establish a date by which a county awarded a grant under Subsection (3)(c)(iii) shall report back to the committee.
(d) The committee may not award a grant to a county under this section in an amount greater than $100,000.
(4) A county that is awarded a grant under this section shall:
(a) document the work performed by the county, pursuant to the plan established by the county under Subsection (3)(b)(ii), to protect or rehabilitate a monument; and
(b) before the date established under Subsection (3)(c)(iv), report to the committee on the work performed by the county.
(5)
(a) If the committee has not expended all of the funds appropriated to the committee by the Legislature for the fulfillment of the committee's duties under this section before December 31, 2017, the committee shall disburse any remaining funds equally among all counties that have established a preservation fund by ordinance as provided in Section 17-63-710.
(b) A county to which the center has disbursed funds under Subsection (5)(a) shall:
(i) deposit the funds into the county's preservation fund; and
(ii) expend the funds, in consultation with the committee, for the maintenance and preservation of monuments in the county.

Amended by Chapter 17, 2025 Special Session 1

Part 6
Utah Public Notice Website

63A-16-601 Utah Public Notice Website -- Establishment and administration.
(1) As used in this part:
(a) "Executive board" means the same as that term is defined in Section 67-1-2.5.
(b) "Public body" means the same as that term is defined in Section 52-4-103.
(c) "Public information" means a public body's public notices, minutes, audio recordings, and other materials that are required to be posted to the website under Title 52, Chapter 4, Open and Public Meetings Act, or other statute or state agency rule.
(d) "Website" means the Utah Public Notice Website created in this section.
(2) There is created the Utah Public Notice Website to be administered by the division.
(3) The website shall consist of an Internet website provided to assist the public to find posted public information.
(4) The Division of Archives and Records Service, with the technical assistance of the Division of Technology Services, shall create the website that shall:
(a) allow a public body, or other certified entity, to easily post any public information, including the contact information required under Subsections 17B-1-303(9) and 17D-1-106(1)(b)(ii);
(b) allow the public to easily search the public information by:

(i) public body name;
(ii) date of posting of the notice;
(iii) date of any meeting or deadline included as part of the public information; and
(iv) any other criteria approved by the Division of Archives and Records Service;
(c) allow the public to easily search and view past, archived public information;
(d) allow an individual to subscribe to receive updates and notices associated with a public body or a particular type of public information;
(e) have a unique and simplified website address;
(f) be directly accessible via a link from the main page of the official state website; and
(g) allow a newspaper to request and automatically receive a transmission of a posting to the website as the posting occurs;
(h) include other links, features, or functionality that will assist the public in obtaining and reviewing public information posted on the website, as may be approved by the division; and
(i) be guided by the principles described in Subsection 63A-16-202(2).
(5)
(a) Subject to Subsection (5)(b), the Division of Archives and Records Service and the governor's office shall coordinate to ensure that the website, the database described in Section 67-1-2.5, and the website described in Section 67-1-2.5 automatically share appropriate information in order to ensure that:
(i) an individual who subscribes to receive information under Subsection (4)(d) for an executive board automatically receives notifications of vacancies on the executive board that will be publicly filled, including a link to information regarding how an individual may apply to fill the vacancy; and
(ii) an individual who accesses an executive board's information on the website has access to the following through the website:
(A) the executive board's information in the database, except an individual's physical address, e-mail address, or phone number; and
(B) the portal described in Section 67-1-2.5 through which an individual may provide input on an appointee to, or member of, the executive board.
(b) The Division of Archives and Records Service and the governor's office shall comply with Subsection (5)(a) as soon as reasonably possible within existing funds appropriated to the Division of Archives and Records Service and the governor's office.
(6) Before August 1 of each year, the Division of Archives and Records Service shall:
(a) identify each executive board that is a public body that did not submit to the website a notice of a public meeting during the previous fiscal year; and
(b) report the name of each identified executive board to the governor's boards and commissions administrator.
(7) The Division of Archives and Records Service is responsible for:
(a) establishing and maintaining the website, including the provision of equipment, resources, and personnel as is necessary;
(b) providing a mechanism for public bodies or other certified entities to have access to the website for the purpose of posting and modifying public information; and
(c) maintaining an archive of all public information posted to the website.
(8) A public body is responsible for the content the public body is required to post to the website and the timing of posting of that information.

Renumbered and Amended by Chapter 84, 2021 General Session
Amended by Chapter 344, 2021 General Session, (Coordination Clause)

Renumbered and Amended by Chapter 344, 2021 General Session
Amended by Chapter 355, 2021 General Session

63A-16-602 Notice and training by the Division of Archives and Records Service.
(1) The Division of Archives and Records Service shall provide notice of the provisions and requirements of this chapter to all public bodies that are subject to the provision of Subsection 52-4-202(3)(a).
(2) The Division of Archives and Records Service shall, as necessary, provide periodic training on the use of the website to public bodies that are authorized to post notice on the website.

Amended by Chapter 435, 2023 General Session

Part 8
Single Sign-on Portal

63A-16-801 Definitions.
As used in this part:
(1) "Business data" means data collected by the state about a person doing business in the state.
(2) "Single sign-on business portal" means the web portal described in Section 63A-16-802.
(3) "Single sign-on citizen portal" means the web portal described in Section 63A-16-803.
(4) "Web portal" means an Internet webpage that can be accessed by a person that enters the person's unique user information in order to access secure information.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-802 Single sign-on business portal -- Creation.
(1) The division shall, in consultation with the entities described in Subsection (4), design and create a single sign-on business portal that is:
  (a) a web portal through which a person may access data described in Subsection (2), as agreed upon by the entities described in Subsection (4); and
  (b) secure, centralized, and interconnected.
(2) The division shall ensure that the single sign-on business portal allows a person doing business in the state to access, at a single point of entry, all relevant state-collected business data about the person, including information related to:
  (a) business registration;
  (b) workers' compensation;
  (c) beginning December 1, 2020, tax liability and payment; and
  (d) other information collected by the state that the department determines is relevant to a person doing business in the state.
(3) The division shall develop the single sign-on business portal:
  (a) using an open platform that:
    (i) facilitates participation in the web portal by a state entity;
    (ii) allows for optional participation by a political subdivision of the state; and
    (iii) contains a link to the State Tax Commission website; and
  (b) in a manner that anticipates the creation of the single sign-on citizen portal described in Section 63A-16-803.

(4) In developing the single sign-on business portal, the division shall consult with:
(a) the Department of Commerce;
(b) the State Tax Commission;
(c) the Labor Commission;
(d) the Department of Workforce Services;
(e) the Governor's Office of Planning and Budget;
(f) the Utah League of Cities and Towns;
(g) the Utah Association of Counties; and
(h) the business community that is likely to use the single sign-on business portal.
(5) The division shall ensure that the single sign-on business portal is fully operational no later than May 1, 2021.

Renumbered and Amended by Chapter 344, 2021 General Session
Amended by Chapter 382, 2021 General Session

63A-16-803 Single sign-on citizen portal -- Creation.
(1) The division shall, in consultation with the entities described in Subsection (4), design and create a single sign-on citizen portal that is:
(a) a web portal through which an individual may access information and services described in Subsection (2), as agreed upon by the entities described in Subsection (4); and
(b) secure, centralized, and interconnected.
(2) The division shall ensure that the single sign-on citizen portal allows an individual, at a single point of entry, to:
(a) access and submit an application for:
(i) medical and support programs including:
(A) a medical assistance program administered under Title 26B, Chapter 3, Health Care - Administration and Assistance, including Medicaid;
(B) the Children's Health Insurance Program under Title 26B, Chapter 3, Part 9, Utah Children's Health Insurance Program;
(C) the Primary Care Network as defined in Section 26B-3-211; and
(D) the Women, Infants, and Children program administered under 42 U.S.C. Sec. 1786;
(ii) unemployment insurance under Title 35A, Chapter 4, Employment Security Act;
(iii) workers' compensation under Title 34A, Chapter 2, Workers' Compensation Act;
(iv) employment with a state agency;
(v) a driver license or state identification card renewal under Title 53, Chapter 3, Uniform Driver License Act;
(vi) a birth or death certificate under Title 26B, Chapter 8, Part 1, Vital Statistics; and
(vii) a hunting or fishing license under Title 23A, Chapter 4, Licenses, Permits, Certificates of Registration, and Tags;
(b) access the individual's:
(i) transcripts from an institution of higher education listed in Section 53H-1-102; and
(ii) immunization records maintained by the Department of Health and Human Services;
(c) register the individual's vehicle under Title 41, Chapter 1a, Part 2, Registration, with the Motor Vehicle Division of the State Tax Commission;
(d) file the individual's state income taxes under Title 59, Chapter 10, Individual Income Tax Act, beginning December 1, 2020;
(e) access information about positions available for employment with the state; and

(f) access any other service or information the department determines is appropriate in consultation with the entities described in Subsection (4).

(3) The division shall develop the single sign-on citizen portal using an open platform that:

(a) facilitates participation in the portal by a state entity;

(b) allows for optional participation in the portal by a political subdivision of the state; and

(c) contains a link to the State Tax Commission website.

(4) In developing the single sign-on citizen portal, the department shall consult with:

(a) each state executive branch agency that administers a program, provides a service, or manages applicable information described in Subsection (2);

(b) the Utah League of Cities and Towns;

(c) the Utah Association of Counties; and

(d) other appropriate state executive branch agencies.

(5) The division shall ensure that the single sign-on citizen portal is fully operational no later than January 1, 2025.

(6)

(a) As used in this Subsection (6):

(i) "Digital verifiable credential" means the same as that term is defined in Section 63A-16-108.

(ii) "Digital verifiable record" means the same as that term is defined in Section 63A-16-108.

(iii) "Offender" means the same as that term is defined in Section 64-13-1.

(b) No later than January 1, 2027, the division shall ensure that a version of the single sign-on citizen portal is made available to an individual who:

(i) is a Utah resident; and

(ii)

(A) is an offender; or

(B) previously was an offender resulting from a conviction that occurred on or after January 1, 2027.

(c) The portal described in Subsection (6)(b) shall include:

(i) if possible, an electronic copy of, or link to, the individual's digital verifiable credentials and digital verifiable records; and

(ii) if available:

(A) information on the individual's debts such as restitution, court costs, fines, tax obligations, alimony, child support, other court-ordered payments, and similar debts; and

(B) links or another method to access more information concerning the debts listed in Subsection (6)(c)(ii)(A).

Amended by Chapter 9, 2025 Special Session 1

63A-16-804 Report.

(1) The division shall report to the Government Operations Interim Committee before November 30 of each year regarding:

(a) the progress the division has made in developing the single sign-on business portal and the single sign-on citizen portal and, once that development is complete, regarding the operation of the single sign-on business portal and the single sign-on citizen portal;

(b) the division's goals and plan for each of the next five years to fulfill the division's responsibilities described in this part; and

(c) whether the division recommends any change to the single sign-on fee being charged under Section 13-1-2.

(2) The Government Operations Interim Committee shall annually:

(a) review the single sign-on fee being charged under Section 13-1-2;
(b) determine whether the revenue from the single sign-on fee is adequate for designing and developing and then, once developed, operating and maintaining the single sign-on web portal; and
(c) make any recommendation to the Legislature that the committee considers appropriate concerning:
(i) the single sign-on fee; and
(ii) the development or operation of the single sign-on business portal and the single sign-on citizen portal.

Amended by Chapter 169, 2022 General Session

Part 9
Technology Innovation Act

63A-16-901 Definitions.

As used in this part:
(1) "Executive branch agency" means a department, division, or other agency within the executive branch of state government.
(2) "Governor's budget office" means the Governor's Office of Planning and Budget, created in Section 63J-4-201.
(3) "Review board" means the Architecture Review Board established within the department.
(4) "Technology innovation" means a new information technology not previously in use or a substantial adaptation or modification of an existing information technology.
(5) "Technology proposal" means a proposal to implement a technology innovation designed to result in a greater efficiency in a government process or a cost saving in the delivery of a government service, or both.

Renumbered and Amended by Chapter 344, 2021 General Session
Amended by Chapter 382, 2021 General Session

63A-16-902 Submitting a technology proposal -- Review process.

(1) Multiple executive branch agencies may jointly submit to the chief information officer a technology proposal, on a form or in a format specified by the division.
(2) The chief information officer shall transmit to the review board each technology proposal the chief information officer determines meets the form or format requirements of the division.
(3) The review board shall:
(a) conduct a technical review of a technology proposal transmitted by the chief information officer;
(b) determine whether the technology proposal merits further review and consideration by the chief information officer, based on the technology proposal's likelihood to:
(i) be capable of being implemented effectively; and
(ii) result in greater efficiency in a government process or a cost saving in the delivery of a government service, or both; and

(c) transmit a technology proposal to the chief information officer and to the governor's budget office, if the review board determines that the technology proposal merits further review and consideration by the chief information officer.

Renumbered and Amended by Chapter 344, 2021 General Session

63A-16-903 Chief information officer review and approval of technology proposals.

(1) The chief information officer shall review and evaluate each technology proposal that the review board transmits to the chief information officer.

(2) The chief information officer may approve and recommend that the division provide funding from legislative appropriations for a technology proposal if, after the chief information officer's review and evaluation of the technology proposal:

(a) the chief information officer determines that there is a reasonably good likelihood that the technology proposal:

(i) is capable of being implemented effectively; and

(ii) will result in greater efficiency in a government process or a cost saving in the delivery of a government service, or both; and

(b) the chief information officer receives approval from the governor's budget office for the technology proposal.

(3) The chief information officer may:

(a) prioritize multiple approved technology proposals based on their relative likelihood of achieving the goals described in Subsection (2); and

(b) recommend funding based on the chief information officer's prioritization under Subsection (3)(a).

(4) The division shall:

(a) track the implementation and success of a technology proposal approved by the chief information officer;

(b) evaluate the level of the technology proposal's implementation effectiveness and whether the implementation results in greater efficiency in a government process or a cost saving in the delivery of a government service, or both; and

(c) report the results of the division's tracking and evaluation:

(i) to the chief information officer, as frequently as the chief information officer requests; and

(ii) at least annually to the Government Operations Interim Committee.

(5) The division may expend money appropriated by the Legislature to pay for expenses incurred by executive branch agencies in implementing a technology proposal that the chief information officer has approved.

Amended by Chapter 169, 2022 General Session

Part 10
Criminal and Juvenile Justice Database

63A-16-1001 Definitions.

As used in this part:

(1) "Commission" means the State Commission on Criminal and Juvenile Justice created in Section 63M-7-201.

(2) "Criminal justice agency" means an agency or institution directly involved in the apprehension, prosecution, and incarceration of an individual involved in criminal activity, including law enforcement, correctional facilities, jails, courts, probation, and parole.
(3) "Division" means the Division of Technology Services created in Section 63A-16-103.
(4) "Grant" means a grant awarded under Section 63A-16-1003.
(5) "Program" means the public safety portal grant program created in Section 63A-16-1003.
(6) "Public safety portal" means the data portal created in Section 63A-16-1002.
(7) "State board" means the State Board of Education.

Amended by Chapter 108, 2024 General Session

63A-16-1002 Public safety portal.
(1) The commission shall oversee the creation and management of a public safety portal for information and data required to be reported to the commission and accessible to all criminal justice agencies in the state.
(2) The division shall assist with the development and management of the public safety portal.
(3) The division, in collaboration with the commission, shall create:
  (a) master standards and formats for information submitted to the public safety portal;
  (b) a gateway, bridge, website, or other method for reporting entities to provide the information;
  (c) a master data management index or system to assist in the retrieval of information from the public safety portal;
  (d) a protocol for accessing information in the public safety portal that complies with state privacy regulations; and
  (e) a protocol for real-time audit capability of all data accessed from the public safety portal by participating data source, data use entities, and regulators.
(4) The public safety portal shall be the repository for the statutorily required data described in:
  (a) Section 13-53-111, Recidivism reporting requirements;
  (b) Section 17-72-408, County jail reporting requirements;
  (c) Section 17E-2-201, Criminal Justice Coordinating Councils reporting;
  (d) Section 26B-1-427, Alcohol Abuse Tracking Committee;
  (e) Section 41-6a-511, Courts to collect and maintain data;
  (f) Section 53-10-118, Regarding driving under the influence data;
  (g) Section 53-25-301, Reporting requirements for reverse-location warrants;
  (h) Section 53-25-202, Sexual assault offense reporting requirements for law enforcement agencies;
  (i) Section 53E-3-516, School disciplinary and law enforcement action report;
  (j) Section 53-25-501, Reporting requirements for seized firearms;
  (k) Section 53-25-502, Law enforcement agency reporting requirements for certain firearm data;
  (l) Section 63M-7-214, Law enforcement agency grant reporting;
  (m) Section 63M-7-216, Prosecutorial data collection;
  (n) Section 63M-7-216.1, Prosecutorial data collection regarding certain prosecutions, dismissals, and declinations to prosecute;
  (o) Section 63M-7-220, Domestic violence data collection;
  (p) Section 64-14-204, Supervision of sentenced offenders placed in community;
  (q) Section 64-13-25, Standards for programs;
  (r) Section 64-13-45, Department reporting requirements;
  (s) Section 64-13e-104, County correctional facility reimbursement program for state probationary inmates and state parole inmates;

(t) Section 77-7-8.5, Use of tactical groups;
(u) Section 77-11b-404, Forfeiture reporting requirements;
(v) Section 77-20-103, Release data requirements;
(w) Section 77-22-2.5, Court orders for criminal investigations;
(x) Section 78A-2-109.5, Court data collection on criminal cases;
(y) Section 80-6-104, Data collection on offenses committed by minors; and
(z) any other statutes that require the collection of specific data and the reporting of that data to the commission.

(5) Before October 1, 2025, the commission shall report all data collected to the Law Enforcement and Criminal Justice Interim Committee.

(6) The commission may:
(a) enter into contracts with private or governmental entities to assist entities in complying with the data reporting requirements of Subsection (4); and
(b) make, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, rules to administer this section, including establishing requirements and procedures for collecting the data described in Subsection (4).

Amended by Chapter 17, 2025 Special Session 1

63A-16-1003 Public safety portal grant program.

(1)
(a) There is created within the commission the public safety portal grant program.
(b) The purpose of the program is to award grants to assist entities in complying with the data reporting requirements described in Subsection 63A-16-1002(4).
(c) The program is funded with existing appropriations previously designated for the purpose of facilitating data collection and any ongoing appropriations made by the Legislature for the program.

(2) An entity that submits a proposal for a grant to the commission shall include details in the proposal regarding:
(a) how the entity plans to use the grant to fulfill the purpose described in Subsection (1)(b);
(b) any plan to use funding sources in addition to the grant for proposal;
(c) any existing or planned partnerships with another individual or entity to implement the proposal; and
(d) other information the commission determines is necessary to evaluate the proposal.

(3) When evaluating a proposal for a grant, the commission shall consider:
(a) the likelihood that the proposal will accomplish the purpose described in Subsection (1)(b);
(b) the cost of the proposal; and
(c) the viability and sustainability of the proposal.

(4) Subject to Subsection (2), the commission may make rules, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, to establish:
(a) eligibility criteria for a grant;
(b) the form and process for submitting a proposal to the commission for a grant;
(c) the method and formula for determining a grant amount; and
(d) reporting requirements for a grant recipient.

Enacted by Chapter 108, 2024 General Session

63A-16-1004 Software service required to be compatible with public safety portal.

(1) A vendor that operates a software service described in Subsection (2) shall:
(a) establish an automated connection to the commission's public safety portal; and
(b) ensure that the connection described in Subsection (1)(a) is operational within one year of the criminal justice agency's system that uses the software service becoming active.
(2) A software service is subject to Subsection (1) if the software service:
(a) is for use by a criminal justice agency within the state's criminal justice system; and
(b) collects and stores data required by statute to be reported to the commission.

Enacted by Chapter 252, 2025 General Session

Part 11
Utah Cyber Center

63A-16-1101 Definitions.

As used in this part:
(1) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.
(2) "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of:
(a) personal data affecting 500 or more individuals; or
(b) data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity.
(3) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
(4) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

Enacted by Chapter 426, 2024 General Session

63A-16-1102 Utah Cyber Center -- Creation -- Duties.

(1)
(a) There is created within the division the Utah Cyber Center.
(b) The chief information security officer appointed under Section 63A-16-210 shall serve as the director of the Cyber Center.
(2) The division shall operate the Cyber Center in partnership with the following entities within the Department of Public Safety created in Section 53-1-103:
(a) the Statewide Information and Analysis Center;
(b) the State Bureau of Investigation created in Section 53-10-301; and
(c) the Division of Emergency Management created in Section 53-2a-103.
(3) In addition to the entities described in Subsection (3), the Cyber Center shall collaborate with:
(a) the Cybersecurity Commission created in Section 63C-27-201;
(b) the Office of the Attorney General;
(c) the Utah Education and Telehealth Network created in Section 53H-4-213.4;
(d) appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;
(e) appropriate information sharing and analysis centers;
(f) information technology directors, cybersecurity professionals, or equivalent individuals representing political subdivisions in the state; and

(g) any other person the division believes is necessary to carry out the duties described in Subsection (4).

(4) The Cyber Center shall, within legislative appropriations:

(a) by June 30, 2024, develop a statewide strategic cybersecurity plan for governmental entities;

(b) with respect to executive branch agencies:

(i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;

(ii) coordinate cybersecurity resilience planning;

(iii) provide cybersecurity incident response capabilities; and

(iv) recommend to the division standards, policies, or procedures to increase the cyber resilience of executive branch agencies individually or collectively;

(c) at the request of a governmental entity, coordinate cybersecurity incident response for a data breach affecting the governmental entity in accordance with Section 63A-19-405;

(d) promote cybersecurity best practices;

(e) share cyber threat intelligence with governmental entities and, through the Statewide Information and Analysis Center, with other public and private sector organizations;

(f) serve as the state cybersecurity incident response repository to receive reports of breaches of system security, including notification or disclosure under Section 13-44-202 and data breaches under Section 63A-16-1103;

(g) develop incident response plans to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the state;

(h) coordinate, develop, and share best practices for cybersecurity resilience in the state;

(i) identify sources of funding to make cybersecurity improvements throughout the state;

(j) develop a sharing platform to provide resources based on information, recommendations, and best practices; and

(k) partner with institutions of higher education and other public and private sector organizations to increase the state's cyber resilience.

Amended by Chapter 9, 2025 Special Session 1

63A-16-1103 Assistance to governmental entities -- Records.

(1) The Cyber Center shall provide a governmental entity with assistance in responding to a data breach reported under Section 63A-19-405, which may include:

(a) conducting all or part of an internal investigation into the data breach;

(b) assisting law enforcement with the law enforcement investigation if needed;

(c) determining the scope of the data breach;

(d) assisting the governmental entity in restoring the reasonable integrity of the system; or

(e) providing any other assistance in response to the reported data breach.

(2)

(a) A governmental entity that is required to submit information under Section 63A-19-405 shall provide records to the Cyber Center as a shared record in accordance with Section 63G-2-206.

(b) The following information may be deemed confidential and may only be shared as provided in Section 63G-2-206:

(i) the information provided to the Cyber Center by a governmental entity under Section 63A-19-405; and

(ii) information produced by the Cyber Center in response to a report of a data breach under Subsection (1).

Renumbered and Amended by Chapter 426, 2024 General Session

Part 12
State-endorsed Digital Identity

63A-16-1201 Definitions.

As used in this part:

(1) "Biometric data" means the same as that term is defined in Section 13-61-101.

(2) "Chief privacy officer" means the chief privacy officer appointed in accordance with Section 63A-19-302.

(3) "Digital identity" means an electronic record that an individual may use to assert the individual's identity.

(4) "Governmental entity" means the same as that term is described in Section 63G-2-103.

(5)

(a) "Guardian" means an individual or entity authorized to act on behalf of an individual.

(b) "Guardian" includes:

(i) a representative designated by an individual;

(ii) the parent or legal guardian of an unemancipated minor; or

(iii) the legal guardian of a legally incapacitated individual.

(6)

(a) "Identity" means any attribute used to identify or distinguish a specific individual.

(b) "Identity" includes an individual's:

(i) personal data;

(ii) biometric data;

(iii) physical and non-physical characteristics;

(iv) image or likeness;

(v) signature; and

(vi) any other unique physical or digital identifier related to the individual.

(7) "Individual" means the same as that term is described in Section 63G-2-103.

(8)

(a) "Mobile communication device" means any wireless communication device with Internet capability capable of displaying or providing a state-endorsed digital identity.

(b) "Mobile communication device" includes a:

(i) cellular telephone; or

(ii) wireless tablet.

(9) "Office" means the Office of Data Privacy created in Section 63A-19-301.

(10) "Person" means the same as that term is defined in Section 63G-2-103.

(11) "Personal data" means the same as that term is defined in Section 63A-19-101.

(12) "Physical identity" means a physical record that an individual may use to prove the individual's identity issued by:

(a) a governmental entity;

(b) the equivalent of a governmental entity in another state;

(c) the federal government; or

(d) another country.

(13) "State-endorsed digital identity" means an individual's digital identity that:

(a) is controlled by the individual; and
(b) has been officially recognized by the state.
(14) "State-endorsed digital identity program" means a state initiative which is designed to develop methods, policies, and procedures to endorse an individual's digital identity.
(15) "System" means the technological infrastructure, processes, and procedures used to create, store, manage, and validate a state-endorsed digital identity.

Enacted by Chapter 352, 2025 General Session

63A-16-1202 State digital identity policy.
(1) It is the policy of Utah that:
(a) each individual has a unique identity;
(b) the state does not establish an individual's identity;
(c) the state may, in certain circumstances, recognize and endorse an individual's identity;
(d) the state is obligated to respect an individual's privacy interest associated with the individual's identity;
(e) the state is the only governmental entity that may endorse an individual's digital identity for the purpose of establishing a state-endorsed digital identity;
(f) the state may only endorse an individual's digital identity if the state-endorsed digital identity program is expressly authorized by the Legislature;
(g) an individual whose digital identity has been endorsed by the state is entitled to:
(i) choose:
(A) how the individual discloses the individual's state-endorsed digital identity;
(B) to whom the individual discloses the individual's state-endorsed digital identity;
(C) which elements of the individual's state-endorsed digital identity to disclose;
(D) where the individual's state-endorsed digital identity is stored; and
(E) whether to use a state-endorsed digital identity or physical identity to prove the individual's identity;
(ii) allow a governmental entity or a person to use information related to the individual's use of the individual's state-endorsed digital identity for a purpose other than the primary purpose for which the governmental entity or person collected the information; and
(iii) have a guardian obtain or use a state-endorsed digital identity on the individual's behalf;
(h) a governmental entity or person that accepts a state-endorsed digital identity shall:
(i) collect, use, and retain an individual's state-endorsed digital identity in a secure manner; and
(ii) comply with the requirements of this part through technological means;
(i) a governmental entity may not:
(i) convey a material benefit upon an individual for using a state-endorsed digital identity instead of a physical identity; or
(ii) withhold services or benefits from an individual if the individual uses a physical identity or is otherwise unable to use a state-endorsed digital identity; and
(j) a governmental entity or a person may not require an individual to surrender the individual's mobile communication device to verify the individual's identity.
(2) The state may not endorse an individual's digital identity unless:
(a) the state has verified an individual's identity before endorsement;
(b) the state-endorsed digital identity:
(i) incorporates state-of-the-art safeguards for protecting the individual's identity;
(ii) includes methods to establish authenticity;
(iii) is easy for an individual to adopt and use; and

(iv) is compatible with a wide variety of technological systems without sacrificing privacy or security;
(c) the state provides clear information to an individual regarding how the individual may:
(i) maintain and control the individual's state-endorsed digital identity;
(ii) use the individual's state-endorsed digital identity;
(iii) limit access to:
(A) the individual's state-endorsed digital identity; and
(B) any elements of the individual's identity disclosed by the state-endorsed digital identity; and
(iv) obtain a new state-endorsed digital identity if the individual's state-endorsed digital identity is compromised;
(d) the state ensures that when an individual uses a state-endorsed digital identity:
(i) any record of the individual's use:
(A) is only used for the primary purpose for which the individual disclosed the state-endorsed digital identity; and
(B) is not disclosed, shared, or compared by the governmental entity or person receiving the state-endorsed digital identity; and
(ii) the use is free from surveillance, visibility, tracking, or monitoring by any other governmental entity or person; and
(e) the state-endorsed digital identity enables an individual to:
(i) selectively disclose elements of the individual's identity; and
(ii) verify that the individual's age satisfies an age requirement without revealing the individual's age or date of birth.
(3) The state may only revoke or withdraw the state's endorsement of an individual's state-endorsed digital identity if:
(a) the state-endorsed digital identity has been compromised;
(b) the state's endorsement was:
(i) issued in error; or
(ii) based on fraudulent information; or
(c) the individual requests that the state revoke or withdraw the endorsement of the individual's state-endorsed digital identity.

Enacted by Chapter 352, 2025 General Session

63A-16-1203 Department duties.
(1) The department shall:
(a) explore ways in which the state may implement a state-endorsed digital identity program consistent with the state policy expressed in Section 63A-16-1202;
(b) study and identify best practices regarding the use of a digital identity;
(c) propose policies, procedures, standards, and technology that should be incorporated in the state-endorsed digital identity program;
(d) examine how the state-endorsed digital identity program may be implemented in the most cost-effective manner possible using state resources that are already available; and
(e) evaluate and make recommendations regarding any changes to existing statutes, rules, or policies that may be necessary to facilitate the creation of a state-endorsed digital identity program.
(2) In performing the duties described in Subsection (1), the department shall consult with:
(a) the chief information officer;

(b) the chief privacy officer;
(c) the Utah League of Cities and Towns;
(d) the Utah Association of Counties; and
(e) individuals who have relevant expertise, including representatives from:
(i) governmental entities;
(ii) other states; and
(iii) the private sector.

(3) The department shall report to the Public Utilities, Energy, and Technology Interim Committee regarding the duties described in Subsection (1) and recommendations for the implementation of a state-endorsed digital identity program on or before October 31 of each year.

Enacted by Chapter 352, 2025 General Session