

Kirk A. Cullimore proposes the following substitute bill:

State-Endorsed Digital Identity Program Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kirk A. Cullimore

House Sponsor: Paul A. Cutler

LONG TITLE

General Description:

This bill creates the State-Endorsed Digital Identity Program.

Highlighted Provisions:

This bill:

- defines terms;
- establishes a digital identity bill of rights;
- creates the State-Endorsed Digital Identity Program within the Department of Government Operations;
- establishes requirements for state-endorsed digital identities;
- establishes application and eligibility requirements for obtaining a state-endorsed digital identity;
- establishes identity proofing standards;
- establishes requirements for governmental entities, health care providers, digital wallet providers, verifiers, and relying parties;
- creates a duty of loyalty related to processing identity attributes;
- provides for complaint and enforcement procedures;
- provides for a one-time audit by the Office of the Legislative Auditor General;
- provides for severability; and
- makes technical and conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

29 **63A-19-501**, as last amended by Laws of Utah 2025, Chapter 475

30 ENACTS:

31 **63A-20-101**, Utah Code Annotated 1953

32 **63A-20-201**, Utah Code Annotated 1953

33 **63A-20-202**, Utah Code Annotated 1953

34 **63A-20-203**, Utah Code Annotated 1953

35 **63A-20-301**, Utah Code Annotated 1953

36 **63A-20-302**, Utah Code Annotated 1953

37 **63A-20-303**, Utah Code Annotated 1953

38 **63A-20-304**, Utah Code Annotated 1953

39 **63A-20-305**, Utah Code Annotated 1953

40 **63A-20-401**, Utah Code Annotated 1953

41 **63A-20-501**, Utah Code Annotated 1953

42 **63A-20-601**, Utah Code Annotated 1953

43 **63A-20-701**, Utah Code Annotated 1953

44 **63A-20-702**, Utah Code Annotated 1953

45 **63A-20-801**, Utah Code Annotated 1953

46 **63A-20-802**, Utah Code Annotated 1953

47 **63A-20-901**, Utah Code Annotated 1953

48 REPEALS:

49 **63A-16-1201**, as enacted by Laws of Utah 2025, Chapter 352

50 **63A-16-1202**, as enacted by Laws of Utah 2025, Chapter 352

51 **63A-16-1203**, as enacted by Laws of Utah 2025, Chapter 352



53 *Be it enacted by the Legislature of the state of Utah:*

54 Section 1. Section **63A-19-501** is amended to read:

55 **63A-19-501 . Data privacy ombudsperson.**

56 (1) The governor shall appoint a data privacy ombudsperson with the advice of the
57 governing board.

58 (2) The ombudsperson shall:

59 (a) be familiar with the provisions of:

60 (i) this chapter;

61 (ii) Chapter 12, Division of Archives and Records Service and Management of
62 Government Records;

96 endorsed by the state.

97 (5) An individual has a right to state endorsement of the individual's digital identity upon
98 meeting objective, uniform standards for eligibility and verification established by law,
99 and a right to not have such endorsement arbitrarily or discriminatorily withheld or
100 revoked.

101 (6) An individual has a right to have the state's operation of digital identity systems
102 governed by clear standards established by the Legislature, including for eligibility,
103 issuance, endorsement, acceptance, revocation, or interoperability of digital identity
104 assertions.

105 (7) An individual has a right to transparency in the design and operation of a state digital
106 identity, including the right to access, read, and review the standards and technical
107 specifications upon which the state digital identity is built and operates.

108 (8) An individual has the right to choose what identity attributes are disclosed by the
109 individual's state digital identity in accordance with standards established by the
110 Legislature.

111 (9) An individual has the right to any service or benefit to which the individual is otherwise
112 lawfully entitled based on the individual's choice of a lawful format or means of identity
113 assertion without denial, diminishment, or condition.

114 (10) An individual has a right to be free from surveillance, profiling, tracking, or persistent
115 monitoring of the individual's assertions of digital identity by the state, except as
116 authorized by law.

117 (11) An individual has a right to not be required by the state to surrender the individual's
118 device in order to present the individual's digital identity.

119 Section 3. Section **63A-20-201** is enacted to read:

120 **Part 2. Definitions and Program Creation**

121 **63A-20-201 . Definitions.**

122 As used in this chapter:

123 (1) "Cross-context correlation" means the ability of a person to link, associate, or infer that
124 the presentation of a state-endorsed digital identity originating with the same or another
125 person relates to the same individual.

126 (2) "Data privacy ombudsperson" means the data privacy ombudsperson created in Section
127 63A-19-501.

128 (3)(a) "Digital guardian" means a person authorized to act in the best interest and on
129 behalf of another individual.

- 130 (b) "Digital guardian" includes a:
- 131 (i) representative designated by the individual as described in the rules made by the
- 132 department;
- 133 (ii) custodial parent of an unemancipated minor;
- 134 (iii) legal guardian of a minor appointed under Section 75-5-202; or
- 135 (iv) legal guardian of an incapacitated person appointed under Section 75-5-301.
- 136 (4)(a) "Digital identity" means an electronic record that:
- 137 (i) an individual may use to assert an individual's identity or identity attributes; and
- 138 (ii) can be mathematically verified.
- 139 (b) "Digital identity" does not include an electronic record that relies on shared
- 140 authentication information to verify an individual's identity, including a username,
- 141 password, personal identification number, or one-time code.
- 142 (5) "Digital wallet" means an application, hardware device, software, or service that
- 143 securely stores, organizes, and manages a state digital identity.
- 144 (6) "Digital wallet provider" means a person that creates, develops, maintains, supports, and
- 145 makes available a digital wallet for a state digital identity.
- 146 (7) "Governmental entity" means the same as that term is defined in Section 63A-19-101.
- 147 (8) "Health care provider" means the same as that term is defined in Section 78B-3-403.
- 148 (9) "Holder" means:
- 149 (a) an individual whose identity attributes are contained in the state digital identity; or
- 150 (b) a digital guardian who manages and presents a state digital identity on behalf of the
- 151 individual.
- 152 (10) "Identity" means the qualities, features, or characteristics that identify or distinguish an
- 153 individual.
- 154 (11) "Identity attribute" means a specific quality, characteristic, fact, or information related
- 155 to an individual's identity.
- 156 (12) "Identity proofing" means the process of collecting, validating, and verifying
- 157 information about an individual to establish confidence in the individual's claimed
- 158 identity.
- 159 (13) "Identity proofing entity" means an entity authorized by the department to conduct
- 160 identity proofing for the purpose of issuing a state-endorsed digital identity.
- 161 (14) "Individual" means a human being.
- 162 (15) "Minor" means an individual who is under 18 years old.
- 163 (16) "Offline presentation" means a presentation that does not involve the internet.

- 164 (17) "Online presentation" means a presentation that utilizes the internet or other computer
165 network.
- 166 (18) "Parent" means an individual who has established a parent-child relationship with a
167 child as described in Section 81-5-201.
- 168 (19) "Person" means an individual, corporation, organization, association, governmental
169 entity, or other legal entity.
- 170 (20) "Personal digital identifier" means an identifier that is:
171 (a) unique;
172 (b) created by or at the direction of an individual;
173 (c) mathematically provable to be under a holder's control; and
174 (d) transportable to technical infrastructure of the holder's choosing.
- 175 (21) "Physical identity" means a physical record that an individual may use to assert the
176 individual's identity issued by:
177 (a) a governmental entity;
178 (b) the equivalent of a governmental entity in another state;
179 (c) the federal government; or
180 (d) another country.
- 181 (22) "Presentation" means the disclosure of an individual's identity attributes from the
182 individual's state digital identity to a verifier or relying party.
- 183 (23) "Process" means any operation or set of operations performed on an individual's
184 identity attributes.
- 185 (24) "Program" means the state-endorsed digital identity program described in Section
186 63A-20-202.
- 187 (25) "Program manager" means the individual appointed under Section 63A-20-203.
- 188 (26) "Relying party" means a person that relies on a verifier's assertion of an individual's
189 identity or identity attribute that a state digital identity provides.
- 190 (27) "Secure electronic device" means a device capable of securely storing, presenting, or
191 displaying a state-endorsed digital identity, including physical tokens and accessible
192 devices.
- 193 (28) "State digital identity" means:
194 (a) a state-endorsed digital identity; or
195 (b) an electronic license certificate or identification card issued in accordance with
196 Section 53-3-235.
- 197 (29) "State-endorsed digital identity" means an individual's digital identity that:

198 (a) includes a personal digital identifier; and

199 (b) the department has issued.

200 (30) "Verifier" means a person that mathematically verifies a state digital identity to
201 evaluate the state digital identity's authenticity and integrity.

202 Section 4. Section **63A-20-202** is enacted to read:

203 **63A-20-202 . Digital identity program -- creation -- duties.**

204 (1) There is created within the department the State-Endorsed Digital Identity Program.

205 (2) The department shall design, implement, administer, and issue a state-endorsed digital
206 identity in compliance with the requirements in Part 3, State-Endorsed Digital Identity.

207 (3)(a) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act,
208 the department shall make rules to:

209 (i) administer this chapter;

210 (ii) establish technological standards and best practices for governmental entities
211 regarding:

212 (A) the creation, issuance, use, and acceptance of a state-endorsed digital identity;

213 and

214 (B) the collection, processing, storage, and disclosure of individual identity or
215 identity attributes; and

216 (iii) establish procedures for an individual to:

217 (A) apply for a state-endorsed digital identity; and

218 (B) designate a digital guardian.

219 (b) The department shall:

220 (i) accept public comment for a period of 45 days from the day the proposed rule is
221 published in the Utah State Bulletin as described in Section 63G-3-301; and

222 (ii) issue a response to substantive comments submitted by the public before making
223 the proposed rule effective.

224 (4) In furtherance of these duties the department may consult with:

225 (a) governmental entities;

226 (b) government entities in other states;

227 (c) technology experts; or

228 (d) organizations that establish technology standards.

229 (5) The department may:

230 (a) establish fees in accordance with Section 63J-1-504 for issuing, renewing, or
231 replacing a state-endorsed digital identity; or

- 232 (b) apply for, accept, allocate, and administer grants, funds, or awards from any public
233 or private source for the purpose of implementing this chapter.
- 234 (6) Beginning on January 1, 2027, the department shall annually report before June 1 to the
235 Economic Development and Workforce Services Interim Committee regarding:
- 236 (a) program implementation and adoption metrics;
237 (b) security incidents and remediation steps taken in response;
238 (c) comments submitted to the program by the public;
239 (d) changes made to the program as a result of comments submitted by the public;
240 (e) vendor ecosystem status, including number of conformant digital wallets and verifier
241 tools; and
242 (f) any recommended statutory changes.

243 Section 5. Section **63A-20-203** is enacted to read:

244 **63A-20-203 . Program manager -- appointment -- duties.**

- 245 (1) The executive director, with the approval of the governor, shall appoint an individual to
246 manage the program.
- 247 (2) The program manager shall be experienced in:
- 248 (a) government administration;
249 (b) data privacy;
250 (c) cybersecurity; and
251 (d) information technology.
- 252 (3) The program manager is responsible for implementing a state-endorsed digital identity
253 in accordance with this chapter.

254 Section 6. Section **63A-20-301** is enacted to read:

255 **Part 3. State-Endorsed Digital Identity**

256 **63A-20-301 . State-endorsed digital identity requirements.**

- 257 (1) A state-endorsed digital identity shall:
- 258 (a) incorporate state-of-the-art safeguards for protecting an individual's identity,
259 including compromise detection, recovery mechanisms, and cross-context correlation
260 protections;
- 261 (b) include methods to establish authenticity and integrity;
262 (c) be compatible with a wide variety of technological systems while maintaining strong
263 privacy and security;
- 264 (d) support online and offline presentation;
265 (e) enable a holder to:

- 266 (i) selectively disclose an individual's identity attributes; or
267 (ii) demonstrate that the individual meets a specified minimum age without
268 disclosing the individual's age or birth date;
- 269 (f) allow a holder to choose a digital wallet that conforms with the requirements
270 established by the department; and
- 271 (g) be easy for a holder to adopt and use.
- 272 (2) The department shall:
- 273 (a) validate verification of an individual's identity provided by an identity proofing
274 entity;
- 275 (b) comply with the requirements of this chapter through technological means where
276 possible;
- 277 (c) ensure any technical infrastructure used to control the issuance or revocation of a
278 state-endorsed digital identity is maintained within a state-controlled data center
279 located within the state;
- 280 (d) ensure that a state-controlled data center located within the state shall use best
281 practices in collection, processing, storage, and disclosure of all individual identity
282 and identity attributes;
- 283 (e) select open technological standards for the creation, issuance, use, and acceptance of
284 a state-endorsed digital identity that are:
- 285 (i) publicly available; and
- 286 (ii) free from:
- 287 (A) licensing fees; and
- 288 (B) patent restrictions;
- 289 (f) verify and endorse a specific set of identity attributes including an individual's:
- 290 (i) name;
- 291 (ii) birth date;
- 292 (iii) image; and
- 293 (iv) Utah residence address; and
- 294 (g) create a process for:
- 295 (i) a holder to:
- 296 (A) obtain, maintain, and control an individual's state-endorsed digital identity;
- 297 (B) use an individual's state-endorsed digital identity;
- 298 (C) limit access to an individual's state-endorsed digital identity and identity
299 attributes;

- 300 (D) obtain a new state-endorsed digital identity if the individual's state-endorsed
301 digital identity is compromised; and
- 302 (E) migrate a state-endorsed digital identity to another digital wallet compliant
303 with this chapter;
- 304 (ii) a holder to request that an individual's identity attributes be amended or corrected;
305 and
- 306 (iii) appointment of a digital guardian to obtain or use a state-endorsed digital identity
307 on an individual's behalf.
- 308 (3) A state-endorsed digital identity may not include a mechanism that allows the
309 department to monitor, surveil, or track the presentation of a state-endorsed digital
310 identity to another entity.
- 311 (4) Information provided by an individual to the state to obtain a state-endorsed digital
312 identity may only be:
- 313 (a) used for the purpose of issuing and managing a state-endorsed digital identity;
314 (b) used as authorized by the individual;
315 (c) retained as long as necessary to issue and manage a state-endorsed digital identity;
316 (d) maintained within a state-controlled data center located within the state; or
317 (e) disclosed to:
- 318 (i) the subject of the record or the subject's digital guardian; or
319 (ii) a person with a warrant or court order.
- 320 (5) The department may only revoke an individual's state-endorsed digital identity if:
321 (a) the state-endorsed digital identity has been compromised;
322 (b) the department's endorsement was:
- 323 (i) issued in error; or
324 (ii) based on fraudulent information; or
325 (c) the holder requests that the department revoke the individual's state-endorsed digital
326 identity.
- 327 (6) The department shall report a data breach regarding individual identity or identity
328 attributes in accordance with Section 63A-19-405.
- 329 Section 7. Section **63A-20-302** is enacted to read:
- 330 **63A-20-302 . Application and eligibility for state-endorsed digital identity.**
- 331 (1) An individual who is at least 18 years old, or is an emancipated minor, may apply to the
332 department for a state-endorsed digital identity.
- 333 (2) An individual who is under 18 years old, and is not an emancipated minor, may apply to

- 334 the department for a state-endorsed digital identity only with the consent of the
335 individual's digital guardian.
- 336 (3)(a) If an individual is unable to apply for a state-endorsed digital identity due to the
337 individual's youth or incapacitation, the application may be made on behalf of that
338 individual by the individual's digital guardian.
- 339 (b) A digital guardian applying on behalf of a minor or incapacitated person shall
340 provide:
- 341 (i) identification, as required by the department; and
342 (ii) the consent of the incapacitated person, as required by the department.
- 343 (4) The department shall make rules, in accordance with Title 63G, Chapter 3, Utah
344 Administrative Rulemaking Act, establishing:
- 345 (a) the form and manner of an application under this section;
346 (b) identity proofing requirements and procedures; and
347 (c) procedures for denial, correction, reissuance, and compromise recovery consistent
348 with this part.
- 349 (5) An individual is not required to apply for or obtain a state-endorsed digital identity.
- 350 (6) To apply for a state-endorsed digital identity, an applicant shall:
- 351 (a) have lawful presence in the United States;
352 (b) be a resident of Utah; and
353 (c) successfully complete the department's identity proofing process established under
354 this part.
- 355 (7)(a) The department may not require collection of information that is not necessary to
356 verify identity or eligibility.
- 357 (b) Required information may include, as determined by the department and documented
358 by rule:
- 359 (i) the applicant's true and full legal name;
360 (ii) date of birth;
361 (iii) Utah residence address;
362 (iv) evidence of lawful presence in the United States;
363 (v) evidence of Utah residency; and
364 (vi) other information strictly necessary to complete identity proofing.
- 365 Section 8. Section **63A-20-303** is enacted to read:
- 366 **63A-20-303 . Identity proofing.**
- 367 (1)(a) The department shall establish and maintain identity proofing requirements for the

- 368 issuance of a state-endorsed digital identity that:
- 369 (i) follow a generally accepted identity proofing standard;
- 370 (ii) are commensurate with the risks of impersonation, fraud, and misuse associated
- 371 with the credential; and
- 372 (iii) are consistent with the privacy, civil liberties, and security requirements of this
- 373 chapter.
- 374 (b) The identity proofing process shall be designed to establish, at a minimum, that:
- 375 (i) the applicant is a real individual;
- 376 (ii) the applicant is the individual the applicant claims to be;
- 377 (iii) the applicant's birth date is the date the applicant claims it to be; and
- 378 (iv) the applicant meets the eligibility requirements of Section 63A-20-302.
- 379 (c) The department shall ensure that the identity proofing process results in a credential
- 380 that provides a level of confidence in the individual's identity that is:
- 381 (i) sufficiently robust to support reliance by governmental entities and private-sector
- 382 relying parties where required by law or policy for online age assurance; and
- 383 (ii) appropriate for use in both online and offline presentations.
- 384 (d) Identity proofing processes shall be designed so that the state's endorsement:
- 385 (i) reflects verification at a point in time; and
- 386 (ii) does not require:
- 387 (A) continuous monitoring; or
- 388 (B) tracking.
- 389 (2)(a) An applicant shall provide true and accurate information as required under this
- 390 part.
- 391 (b) Knowingly providing materially false information for the purpose of obtaining a
- 392 state-endorsed digital identity constitutes fraud and may result in denial, revocation,
- 393 and other remedies provided by law.
- 394 (3)(a) Obtaining or holding a state-endorsed digital identity does not affect an
- 395 individual's physical identity documents.
- 396 (b) An individual is not required to surrender, cancel, or replace any physical identity
- 397 document as a condition of applying for or holding a state-endorsed digital identity.
- 398 (4)(a) The department shall define by rule, in accordance with Title 63G, Chapter 3,
- 399 Utah Administrative Rulemaking Act, the identity proofing standards and processes
- 400 required for issuance of a state-endorsed digital identity.
- 401 (b) The rules shall, at a minimum:

- 402 (i) specify the objectives the identity proofing process is intended to achieve;
403 (ii) describe the acceptable methods of identity proofing, including:
404 (A) in-person, remote, or hybrid methods, and the conditions under which each
405 may be used; and
406 (B) minimum evidence requirements and validation methods;
407 (iii) align with generally accepted identity proofing practices; and
408 (iv) establish requirements and a process to become an identity proofing entity.

409 Section 9. Section **63A-20-304** is enacted to read:

410 **63A-20-304 . Requirements for governmental entities.**

- 411 (1) A governmental entity may not:
412 (a) convey a material benefit upon an individual for using a state digital identity instead
413 of a physical identity;
414 (b) withhold services or benefits from an individual if the individual uses a physical
415 identity or is otherwise unable to use a state digital identity; or
416 (c) require a holder to surrender the holder's secure electronic device in the course of a
417 presentation.
418 (2)(a) A governmental entity that, on or after May 6, 2026, implements a new system
419 that accepts a digital identity shall, within three months after the day on which the
420 department issues the first state-endorsed digital identity, accept a state-endorsed
421 digital identity.
422 (b) A governmental entity is not required to accept a state-endorsed digital identity
423 within the time frame described in Subsection (2)(a) if the governmental entity:
424 (i)(A) demonstrates to the satisfaction of the department that accepting a
425 state-endorsed digital identity at that time is not technically feasible; and
426 (B) provides a plan for accepting a state-endorsed digital identity as soon as
427 feasible; or
428 (ii) is required by law to only accept a specific form of state digital identity.

429 Section 10. Section **63A-20-305** is enacted to read:

430 **63A-20-305 . Requirements for health care providers.**

- 431 (1) Within two years from the date the first state-endorsed digital identity is issued, a health
432 care provider that receives at least \$10,000,000 a year in public funding shall accept a
433 state-endorsed digital identity if the health care provider has a program or system that
434 accepts a digital identity.
435 (2) A health care provider is not required to accept a state-endorsed digital identity within

- 436 the time frame described in Subsection (1) if the health care provider:
- 437 (a)(i) demonstrates to the satisfaction of the department that accepting a
- 438 state-endorsed digital identity at that time is not technically feasible; and
- 439 (ii) provides a plan for accepting a state-endorsed digital identity as soon as feasible;
- 440 or
- 441 (b) is required by law to only accept a specific form of state digital identity.

442 Section 11. Section **63A-20-401** is enacted to read:

443 **Part 4. Digital Wallet Providers**

444 **63A-20-401 . Requirements for digital wallet providers.**

- 445 (1) A digital wallet produced by a digital wallet provider shall:
- 446 (a) incorporate state-of-the-art safeguards for protecting an individual's identity;
- 447 (b) process an individual's identity attributes in a secure manner;
- 448 (c) comply with the requirements of this part through technological means where
- 449 possible;
- 450 (d) be tamper resistant;
- 451 (e) support online and offline presentation of a state-endorsed digital identity;
- 452 (f) maintain a secure log:
- 453 (i) with sufficient information for the holder to know:
- 454 (A) what identity attributes were provided; and
- 455 (B) the verifier or relying party the identity attributes were provided to;
- 456 (ii) accessible only to the holder;
- 457 (iii) exportable only by the holder; and
- 458 (iv) deletable only by the holder;
- 459 (g) enable a holder to:
- 460 (i) selectively disclose an individual's identity attributes; or
- 461 (ii) demonstrate that the individual meets a specified minimum age without
- 462 disclosing the individual's age or birth date; and
- 463 (h) allow a presentation of a state-endorsed digital identity by a digital guardian.
- 464 (2) A digital wallet provider may only process an individual's identity attributes from a state
- 465 digital identity if:
- 466 (a) the processing is necessary for a presentation;
- 467 (b) the holder has received conspicuous notice of:
- 468 (i) what identity attributes are collected from the state digital identity;
- 469 (ii) how the identity attributes are used;

- 504 (3) A verifier may not require a holder to surrender the holder's secure electronic device in
505 the course of a presentation.
- 506 (4) Nothing in this section relieves a verifier from complying with the requirements of Title
507 13, Chapter 44, Protection of Personal Information Act, or Title 13, Chapter 61, Utah
508 Consumer Privacy Act.

509 Section 13. Section **63A-20-601** is enacted to read:

510 **Part 6. Relying Parties**

511 **63A-20-601 . Requirements for relying parties.**

- 512 (1) A relying party shall:
- 513 (a) incorporate state-of-the-art safeguards for protecting an individual's identity in the
514 verification process;
- 515 (b) comply with the requirements of this part through technological means where
516 possible;
- 517 (c) process an individual's identity attributes in a secure manner;
- 518 (d) process only the minimum identity attributes reasonably necessary to achieve a
519 specified purpose; and
- 520 (e) accept a presentation by a digital guardian.
- 521 (2) A relying party may only process an individual's identity attributes from a state digital
522 identity if:
- 523 (a) authorized by the holder;
- 524 (b) the processing is necessary for a specified purpose;
- 525 (c) the holder has received conspicuous notice of:
- 526 (i) what identity attributes are collected;
- 527 (ii) how the identity attributes are used;
- 528 (iii) the purpose for which the identity attributes are processed; and
- 529 (iv) how long the identity attributes are retained; and
- 530 (d) the holder consents to the processing of the identity attributes.
- 531 (3) A relying party may not require a holder to surrender the holder's secure electronic
532 device in the course of a presentation.
- 533 (4) A relying party may accept a state-endorsed digital identity as proof of an individual's
534 identity or identity attributes unless a different method of proof is required by law.
- 535 (5) Nothing in this section relieves a relying party from complying with the requirements of
536 Title 13, Chapter 44, Protection of Personal Information Act, or Title 13, Chapter 61,
537 Utah Consumer Privacy Act.

538 Section 14. Section **63A-20-701** is enacted to read:

539 **Part 7. General Requirements**

540 **63A-20-701 . Duty of loyalty.**

541 The department, a digital wallet provider, a verifier, a relying party, and a digital
542 guardian shall refrain from practices or activities related to the processing of an individual's
543 identity attributes from a digital identity that:

- 544 (1) conflict with the best interests of an individual;
545 (2) take advantage of or otherwise exploit an individual;
546 (3) result in a disproportionate risk to an individual;
547 (4) are to an individual's detriment; or
548 (5) cause harm to an individual.

549 Section 15. Section **63A-20-702** is enacted to read:

550 **63A-20-702 . Processing restrictions.**

- 551 (1) Any record of a presentation of a state digital identity may only be processed by a
552 digital wallet provider, a verifier, or a relying party:
553 (a) for the primary purpose for which the presentation was performed; or
554 (b) if required by law.
555 (2) Information provided by a holder, verifier, or relying party to a verifier or relying party
556 in the course of a presentation may only be:
557 (a) processed for the primary purpose for which the holder disclosed the information; and
558 (b) used, retained, sold, or shared:
559 (i) following conspicuous notice to and express authorization by the holder; or
560 (ii) if required by law.

561 Section 16. Section **63A-20-801** is enacted to read:

562 **Part 8. Enforcement and Audit**

563 **63A-20-801 . Complaints and enforcement.**

- 564 (1) An individual may submit a complaint to the data privacy ombudsperson alleging a
565 violation of this chapter by:
566 (a) the department;
567 (b) a digital wallet provider;
568 (c) a verifier; or
569 (d) a relying party.
570 (2) The data privacy ombudsperson may receive and review a complaint described in

- 571 Subsection (1).
- 572 (3) If, after reviewing a complaint, the data privacy ombudsperson has reasonable cause to
573 believe that a violation of this chapter has occurred, the data privacy ombudsperson may
574 refer the complaint to the attorney general.
- 575 (4) Upon receiving a referral under Subsection (3), or when the attorney general has
576 reasonable cause to believe that a violation of this chapter has occurred, the attorney
577 general is authorized to:
- 578 (a) issue civil investigative demands for depositions, documents, and requests for
579 information in the time and manner prescribed by the attorney general; and
- 580 (b) bring a civil action in a court of competent jurisdiction to:
- 581 (i) enjoin a violation of this chapter;
- 582 (ii) obtain declaratory relief regarding compliance with this chapter; or
- 583 (iii) recover damages, restitution, and disgorgement on behalf of an individual injured
584 by a violation of this chapter.
- 585 (5) The attorney general shall treat all information received in accordance with Subsection
586 (4) as non-public and confidential unless confidentiality is waived by the providing
587 party, or upon the filing of an enforcement action.
- 588 (6) In an action brought under Subsection (4), the court may award:
- 589 (a) injunctive relief;
- 590 (b) declaratory relief;
- 591 (c) equitable relief including restitution and disgorgement;
- 592 (d) actual damages;
- 593 (e) costs; and
- 594 (f) reasonable attorney fees.
- 595 Section 17. Section **63A-20-802** is enacted to read:
- 596 **63A-20-802 . Auditing.**
- 597 (1) Subject to prioritization of the Legislative Audit Subcommittee created in Section
598 36-12-8, the Office of the Legislative Auditor General shall conduct an audit of the
599 program beginning on January 1, 2028.
- 600 (2) The audit shall evaluate:
- 601 (a) the department's compliance with this chapter;
- 602 (b) whether the department has met the restrictions on monitoring, surveillance, and
603 tracking described in Section 63A-20-301;
- 604 (c) the effectiveness of the program in meeting the objectives established in this chapter;

- 605 (d) the appropriate long-term placement of the program within state government; and
606 (e) recommended statutory changes to improve the program.
607 (3) The Office of the Legislative Auditor General shall:
608 (a) complete the audit report by October 31, 2028;
609 (b) provide the audit report to the Legislature; and
610 (c) present the audit findings to the Legislative Audit Subcommittee at the
611 subcommittee's next meeting after completion of the audit report.

612 Section 18. Section **63A-20-901** is enacted to read:

613 **Part 9. Severability**

614 **63A-20-901 . Severability.**

615 (1) If any provision of this chapter or the application of any provision to any person or
616 circumstance is held invalid by a final decision of a court of competent jurisdiction, the
617 remainder of this chapter shall be given effect without the invalid provision or
618 application.

619 (2) The provisions of this chapter are severable.

620 Section 19. **Repealer.**

621 This bill repeals:

622 Section **63A-16-1201, Definitions.**

623 Section **63A-16-1202, State digital identity policy.**

624 Section **63A-16-1203, Department duties.**

625 Section 20. **Effective Date.**

626 This bill takes effect on May 6, 2026.