

30 This chapter is known as "Data Security Management Council."

31 Section 2. Section **63F-2-102** is enacted to read:

32 **63F-2-102. Data Security Management Council -- Membership -- Duties.**

33 (1) There is created the Data Security Management Council composed of nine
34 members as follows:

35 (a) the chief information officer appointed under Section [63F-1-201](#), or the chief
36 information officer's designee;

37 (b) one individual appointed by the governor;

38 (c) one individual appointed by the speaker of the House of Representatives and the
39 president of the Senate from the Legislative Information Technology Steering Committee; and

40 (d) the highest ranking information technology official, or the highest ranking
41 information technology official's designee, from each of:

42 (i) the Judicial Council;

43 (ii) the State Board of Regents;

44 (iii) the State Office of Education;

45 (iv) the Utah College of Applied Technology;

46 (v) the State Tax Commission; and

47 (vi) the Office of the Attorney General.

48 (2) The council shall elect a chair of the council by majority vote.

49 (3) (a) A majority of the members of the council constitutes a quorum.

50 (b) Action by a majority of a quorum of the council constitutes an action of the council.

51 (4) The Department of Technology Services shall provide staff to the council.

52 (5) The council shall meet monthly, or as often as necessary, to:

53 (a) review existing state government data security policies;

54 (b) assess ongoing risks to state government information technology;

55 (c) create a method to notify state and local government entities of new risks;

56 (d) coordinate data breach simulation exercises with state and local government
57 entities; and

58 (e) develop data security best practice recommendations for state government that
59 include recommendations regarding:

- 60 (i) hiring and training a chief information security officer for each government entity;
- 61 (ii) continuous risk monitoring;
- 62 (iii) password management;
- 63 (iv) using the latest technology to identify and respond to vulnerabilities;
- 64 (v) protecting data in new and old systems; and
- 65 (vi) best procurement practices.

66 (6) A member who is not a member of the Legislature may not receive compensation
67 or benefits for the member's service but may receive per diem and travel expenses as provided
68 in:

- 69 (a) Section [63A-3-106](#);
- 70 (b) Section [63A-3-107](#); and
- 71 (c) rules made by the Division of Finance under Sections [63A-3-106](#) and [63A-3-107](#).

72 Section 3. Section **63F-2-103** is enacted to read:

73 **63F-2-103. Data Security Management Council -- Report to Legislature --**

74 **Recommendations.**

75 (1) The council chair or the council chair's designee shall report annually no later than
76 October 1 of each year to the Public Utilities and Technology Interim Committee.

77 (2) The council's annual report shall contain:

- 78 (a) a summary of topics the council studied during the year;
- 79 (b) best practice recommendations for state government; and
- 80 (c) recommendations for implementing the council's best practice recommendations.