Effective 5/6/2026

Part 9
LEA Cybersecurity Standards

53G-8-901 General provisions -- 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 same as that term is defined in Section 63A-16-1101.

(3) "UETN" means the Utah Education and Telehealth Network created in Section 53H-4-213.4.

Enacted by Chapter 170, 2026 General Session

53G-8-902 LEA compliance with cybersecurity standards -- Coordination.

(1) An LEA shall comply with the minimum cybersecurity standards established by the Cybersecurity Commission created in Section 63C-27-201 in rule made in accordance with Subsection 63C-27-202(9).

(2) An LEA shall comply with the minimum cybersecurity standards according to the phased implementation timeline established in rule under Subsection 63C-27-202(9).

(3) UETN, in consultation with the Cyber Center and the state board, shall:

(a) develop implementation guidelines and technical resources to assist LEAs in meeting the minimum cybersecurity standards;

(b) provide technical assistance and support to LEAs; and

(c) coordinate the provision of cybersecurity services and resources to LEAs.

(4)

(a) The Cyber Center, the state board, and UETN shall coordinate services to LEAs to:

(i) avoid duplication of efforts;

(ii) maximize the effectiveness of cybersecurity resources;

(iii) ensure LEAs receive consistent guidance and support; and

(iv) facilitate information sharing regarding cybersecurity threats and best practices.

(b) The coordination required under Subsection (4)(a) shall include:

(i) regular meetings among the entities to discuss LEA cybersecurity needs and initiatives;

(ii) joint development of training materials and resources;

(iii) coordinated response to cybersecurity incidents affecting LEAs; and

(iv) alignment of cybersecurity standards and network infrastructure requirements.

Enacted by Chapter 170, 2026 General Session

53G-8-903 Data breach reporting -- Coordination with Utah Cyber Center.

(1) An LEA shall report a data breach to the Cyber Center:

(a) in accordance with Section 63A-19-405; and

(b) consistent with standards and procedures established in rule under Subsection 63C-27-202(9).

(2) In addition to the requirements in Section 63A-19-405, an LEA shall:

(a) notify the state board within 24 hours of discovering the data breach;

(b) coordinate with UETN if the data breach involves network infrastructure or services provided by UETN; and

(c) cooperate with the Cyber Center's investigation and response efforts.

(3) The Cyber Center shall provide assistance to an LEA in responding to a data breach in the same manner the Cyber Center provides assistance to a governmental entity as described in Title 63A, Chapter 16, Part 11, Utah Cyber Center.

(4) An LEA shall:

(a) participate in cybersecurity information sharing initiatives coordinated by the Cyber Center;

(b) designate a primary point of contact for cybersecurity matters who shall interface with the Cyber Center, the state board, and UETN; and

(c) cooperate with statewide cybersecurity assessments and improvement initiatives.

(5)

(a) A regional education service agency, as that term is defined in Section 53G-4-410, may serve as the designated primary cybersecurity contact for multiple LEAs within the service area.

(b) If a regional education service agency serves as the primary contact under Subsection (5)(a), the agency shall:

(i) coordinate with the Cyber Center, the state board, and UETN on behalf of the participating LEAs;

(ii) ensure each participating LEA meets the minimum cybersecurity standards established under Subsection 63C-27-202(9); and

(iii) maintain documentation of cybersecurity services provided to each LEA.

Enacted by Chapter 170, 2026 General Session