Cybersecurity

Each district shall adopt a cybersecurity policy to:

Policy

1. Secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents; and
2. Determine cybersecurity risk and implement mitigation planning.

A district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources (DIR) under Government Code Chapters 2054 and 2059.

Cybersecurity Coordinator

The superintendent shall designate a cybersecurity coordinator to serve as a liaison between the district and the Texas Education Agency (TEA) in cybersecurity matters.

Cyber Attack or Cybersecurity Incident

Report to TEA

A district shall report to TEA or, if applicable, the entity that administers the system established by TEA in coordination with DIR under Education Code 11.175(g), any cyber attack or other cybersecurity incident against the district's cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

Report to Parent

The district's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required to TEA involving the student's information.

Definitions

Breach of System Security

"Breach of system security" means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

Cyber Attack

"Cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity

"Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Education Code 11.175(a)-(f)

Training

Requirements

At least once each year, a district shall:

1. Identify district employees and elected and appointed board members who have access to a district computer system or database and use a computer to perform at least 25 percent of the employee's or board member's required duties; and

2. Require the employees and board members identified under item 1 to complete a cybersecurity training program certified under Government Code 2054.519 (state-certified cybersecurity training programs).

Gov't Code 2054.5191(a-1)

Notwithstanding Government Code 2054.5191 above, only the district's cybersecurity coordinator is required to complete the cybersecurity training on an annual basis. Any other school district employee required to complete the cybersecurity training shall complete the training as determined by the district, in consultation with the district's cybersecurity coordinator. *Education Code 11.175(h-1)*

Denial of Access The board or the board's designee may deny access to the district's computer system or database to an individual described by item 1 above who the board or the board's designee determines is noncompliant with the requirements of item 2. *Gov't Code 2054.5191(a-2)*

Exceptions The requirements above do not apply to employees and board members who have been:

1. Granted military leave;
2. Granted leave under the federal Family and Medical Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);
3. Granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee no longer has access to the district's database and systems;
4. Granted any other type of extended leave or authorization to work from an alternative work site if that employee no longer has access to the district's database and systems; or
5. Denied access to a district's computer system or database by the board or the board's designee for noncompliance with the requirements of item 2 at Training, Requirements, above.

Gov't Code 2054.5191(f)

Program The board may select the most appropriate state-certified cybersecurity training program for employees and board members of the district to complete. The board shall:

1. Verify and report on the completion of a cybersecurity training program by district employees and board members to the DIR; and

2. Require periodic audits to ensure compliance with these provisions.

Gov't Code 2054.5191(b)

Security Breach Notification

A district that owns, licenses, or maintains computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the district determines that the breach occurred, except as provided at Criminal Investigation Exception, below, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

To Individuals

Resident of Other State

If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person that owns or licenses computerized data to provide notice of a breach of system security, the notice of the breach of system security required under Notice, below, may be provided under that state's law or under Notice, below.

To the Owner or License Holder

A district that maintains computerized data that includes sensitive personal information not owned by the district shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notice

A district may give the required notice to individuals or the owner or license holder by providing:

1. Written notice at the last known address of the individual;
2. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001 (electronic records and signatures); or
3. If the district demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the district does not have sufficient contact information, by:
    a. Electronic mail, if the district has electronic mail addresses for the affected persons;

b. Conspicuous posting of the notice on the district's website; or

c. Notice published in or broadcast on major statewide media.

Information Security Policy

A district that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice described above complies with the notice requirements if the district notifies affected persons in accordance with that policy.

To the Attorney General

A district that is required to disclose or provide notification of a breach of system security under these provisions shall notify the attorney general of that breach as soon as practicable and not later than the 30th day after the date on which the district determines that the breach occurred if the breach involves at least 250 residents of this state. The notification must be submitted electronically using a form accessed through the attorney general's internet website and must include:

1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;

2. The number of residents of this state affected by the breach at the time of notification;

3. The number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;

4. The measures taken by the district regarding the breach;

5. Any measures the district intends to take regarding the breach after the notification described at Notice, above; and

6. Information regarding whether law enforcement is engaged in investigating the breach.

To a Consumer Reporting Agency

If a district is required to notify at one time more than 10,000 persons of a breach of system security, the district shall also notify each consumer reporting agency, as defined by 15 U.S.C. 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The district shall provide the notice without unreasonable delay.

Criminal Investigation Exception

A district may delay providing the required notice to individuals or the owner or license holder at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law en-

forcement agency determines that the notification will not compromise the investigation.

Business and Commerce Code 521.053; Local Gov't Code 205.010

Definitions

For purposes of security breach notifications, the following definitions apply:

Breach of System Security

"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner*. Business and Commerce Code 521.053(a)*

Sensitive Personal Information

"Sensitive personal information" means:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or
    c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
2. Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health-care to the individual.

"Sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Business and Commerce Code 521.002(a)(2), (b)

Security Incident Notification

"Security incident" means a breach or suspected breach of system security as defined by Business and Commerce Code 521.053, above, and the introduction of ransomware, as defined by Penal Code 33.023 into a computer, computer network, or computer system.

"Sensitive personal information" has the meaning assigned by Business and Commerce Code 521.002, above.

A district that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a security incident:

1. Comply with the notification requirements of Business and Commerce Code 521.053 [see Security Breach Notification, above];
2. Not later than 48 hours after the discovery of the security incident, notify:
    a. DIR, including the chief information security officer; or
    b. If the security incident involves election data, the secretary of state; and
3. Comply with all DIR rules relating to reporting security incidents.

Not later than the 10th business day after the date of the eradication, closure, and recovery from a security incident, a district shall notify DIR, including the chief information security officer, of the details of the security incident and include in the notification an analysis of the cause of the security incident.

Gov't Code 2054.603

Cybersecurity Information Sharing Act

A district may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the federal government a cyber threat indicator or defensive measure in accordance with the Cybersecurity Information Sharing Act, 6 U.S.C. Subchapter I (sections 1501-1510). *6 U.S.C. 1503(c)*

Removal of Personal Information

A district sharing a cyber threat indicator pursuant to these provisions shall, prior to sharing:

1. Review such indicator to assess whether it contains any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information

of a specific individual or information that identifies a specific individual and remove such information; or

2. Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

6 U.S.C. 1503(d)(2)

Definitions

For purposes of the Cybersecurity Information Sharing Act, the following definitions apply:

Cybersecurity Purpose

"Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. *6 U.S.C. 1501(4)*

Cybersecurity Threat

"Cybersecurity threat" means an action, not protected by the First Amendment to the United States Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. *6 U.S.C. 1501(5)*

Cyber Threat Indicator

"Cyber threat indicator" means information that is necessary to describe or identify:

1. Malicious reconnaissance, as defined in 6 U.S.C. 1501(12), including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

2. A method of defeating a security control or exploitation of a security vulnerability;

3. A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

4. A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

5. Malicious cyber command and control, as defined in 6 U.S.C. 1501(11);

6. The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

7. Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

8. Any combination thereof.

6 U.S.C. 1501(6)

Defensive Measure — "Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure. *6 U.S.C. 1501(7)*

Information System — "Information system" has the meaning given the term in 44 U.S.C. 3502 and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. *6 U.S.C. 1501(9)*

Security Control — "Security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information. *6 U.S.C. 1501(16)*

Security Vulnerability — "Security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. *6 U.S.C. 1501(17)*