LB638
2023

LEGISLATURE OF NEBRASKA

ONE HUNDRED EIGHTH LEGISLATURE

FIRST SESSION

LEGISLATIVE BILL 638

Introduced by Albrecht, 17.

Read first time January 18, 2023

Committee: Education

A BILL FOR AN ACT relating to education; to adopt the Nebraska K-12 Cybersecurity and Data Protection Act; and to declare an emergency.

Be it enacted by the people of the State of Nebraska,

LB638
2023

Section 1. This act shall be known and may be cited as the Nebraska K-12 Cybersecurity and Data Protection Act.

Sec. 2. The purpose of the Nebraska K-12 Cybersecurity and Data Protection Act is to promote and institute protective cybersecurity measures in alignment with best practices which address prevention, mitigation, response, recovery, and establish systematized response relating to cybersecurity and data protection within the Nebraska school system.

Sec. 3. For purposes of the Nebraska K-12 Cybersecurity and Data Protection Act:

(1) Computer database means a representation of information, knowledge, facts, concepts, or instructions that is intended for use in a computer, computer system, or computer network that is being prepared or has been prepared in a formalized manner, or is being produced or has been produced by a computer, computer system, or computer network;

(2) Cybersecurity means the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information;

(3) Cybersecurity event means an event resulting in unauthorized access to, or the disruption or misuse of, an information system or of nonpublic information stored on an information system or network;

(4) Cybersecurity team includes, but is not limited to, identified individuals with the knowledge and expertise to understand encryption technology, and who electronically monitor Internet connectivity for a school or educational service unit to prevent electronic attacks or cybersecurity events, create plans that successfully deflect potential attacks, provide preventive, ongoing, state-of-the-art training to appropriate school and educational service unit staff members, and expeditiously respond to adverse cybersecurity events by successfully restoring data after a breach and return such system to a protected status;

LB638
2023

(5) Encrypted means the transformation of data into a form that results in a low probability of assigning meaning to the data without the use of a protective process or key;

(6) Information security means the administrative, technical, and physical safeguards that are used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information;

(7) Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information such as a student management system;

(8) Mitigation means identifying data and networks and developing plans to protect such data and networks through periodic updates to software, controlling account access, and leveraging hardware security measures;

(9) Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors:

(a) A knowledge factor, such as a password;

(b) A possession factor, such as a token or text message on a mobile phone; or

(c) An inherent factor, such as a biometric characteristic.

(10) Prevention means creating a cybersecurity strategy that includes, but is not limited to, developing cybersecurity policies, conducting regular, ongoing risk vulnerability assessments, providing awareness training to employees, including training on phishing campaigns, and installing and updating spam filters and anti-malware software;

(11) Ransomware means a computer or data contaminant, encryption, or lock that is placed or introduced without authorization into a computer, computer network, or computer system that restricts access by an

authorized person to a computer, computer data, computer system, or computer network in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock making a demand for payment of money or other consideration to remove the contaminant, encryption, or lock;

(12) Recovery means that a status has been achieved to ensure day-to-day business operations continue following an adverse cybersecurity event and that data is once again protected from future loss; and

(13) Response means a process that is followed after an adverse cybersecurity event that includes, but is not limited to:

(a) A comprehensive systemic audit including:

(i) How the adverse cybersecurity event was discovered;

(ii) A description of how nonpublic information was exposed, lost, stolen, or breached;

(iii) A description of the specific types of nonpublic information lost, stolen, or breached;

(iv) A list of any lost, stolen, or breached nonpublic information that was recovered and how the recovery occurred; and

(v) The source of the cybersecurity event, if available; and

(b) In the event of a cybersecurity attack involving the potential or actual breach of nonpublic information, response shall include complying with all applicable notification requirements pursuant to federal or state law.

Sec. 4. (1) The Educational Service Unit Coordinating Council shall establish a cybersecurity team to conduct a statewide needs analysis to determine appropriate cybersecurity measures and work to implement such cybersecurity measures with individual educational service units and schools in a manner that is respectful of each educational service unit's regional relationship with its member schools.

(2) The cybersecurity team shall establish a response plan designed to promptly respond to and recover from, a cybersecurity event in a

LB638
2023

public school providing instruction in elementary or high school grades that compromises the confidentiality, integrity, or availability of nonpublic information in the school's possession. Such response plan measures may include, but need not be limited to, the following:

(a) Placing access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(b) Identifying and managing the data, personnel, devices, systems, and facilities that enable the school to achieve its purposes in accordance with the relative importance of such data, personnel, devices, systems, and facilities to the school's objectives and risk strategy;

(c) Restricting access of nonpublic information stored in or at physical locations to authorized individuals only;

(d) Protecting, by encryption or other appropriate means, all nonpublic information while the nonpublic information is transmitted over an external network, and all nonpublic information that is stored on a laptop computer, a portable computing or storage device, or portable computing or storage media;

(e) Adopting secure development practices for in-house developed applications utilized by the school, and procedures for evaluating, assessing, and testing the security of externally developed applications utilized by the licensee;

(f) Modifying information systems in accordance with the information security program;

(g) Utilizing effective controls, which may include multi-factor authentication procedures for authorized individuals accessing nonpublic information;

(h) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(i) Developing assigned roles, responsibilities, and levels of

LB638
2023

decision-making authority for each level of the cybersecurity plan, including prevention, mitigation, response, and recovery;

(j) Assessing and identifying weaknesses found within information systems and associated quality controls, identifying nonpublic information that may have been compromised by the cybersecurity event, and overseeing reasonable measures to restore the security of compromised information systems in order to prevent further unauthorized acquisition, release, or use of nonpublic information that is in the district's possession, custody, or control;

(k) Documenting and reporting cybersecurity events and related incident response activities;

(l) Evaluating and revising the incident response plan, as appropriate, following a cybersecurity event; and

(m) Overseeing the provision of public school district personnel with cybersecurity awareness training that is updated as necessary based on emergent threats and industry recommendations.

(3) The Educational Service Unit Coordinating Council shall annually submit a written report electronically to the Education Committee of the Legislature providing updates on progress in implementing the provisions of the Nebraska K-12 Cybersecurity and Data Protection Act. Such report shall include updates on the level of adoption of identified cybersecurity practices in public school districts based on aggregated data from educational service units, and shall include recommendations for additional provisions to address and mitigate emerging, cybersecurity threats to schools.

(4) The State Board of Education may adopt and promulgate rules and regulations to carry out the Nebraska K-12 Cybersecurity and Data Protection Act. The Commissioner may take any enforcement action under the Commissioner's authority to enforce compliance with the Nebraska K-12 Cybersecurity and Data Protection Act.

Sec. 5. Since an emergency exists, this act takes effect when

LB638
2023

passed and approved according to law.