CHAPTER 29
ELECTIONS TECHNOLOGY SECURITY

Chapter rescission date pursuant to Iowa Code section 17A.7: 1/1/28

721—29.1(47) Definitions. The following definitions are adopted.

"Breach" means a compromise of security processes that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

"Commissioner" means the county commissioner of elections as defined in Iowa Code chapter 47.

"Cybersecurity" means the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation.

"Elections technology" means the statewide voter registration database, voting system, electronic poll books, and other technologies used to register, maintain, or process voters or conduct any election. For purposes of this rule, these terms shall have the definitions as described in the administrative rules of the secretary of state.

"Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

"Incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

"I-Voters" means the statewide voter registration database.

"Office of the chief information officer" or *"OCIO"* means the state chief information officer.

"Registrar" means the county commissioner of registration as defined in Iowa Code section 48A.3.

"State commissioner" means the state commissioner of elections as described in Iowa Code chapter 47.

"State registrar" means the state registrar of voters as defined in Iowa Code chapter 48A.

"User" means anyone from the state registrar or county registrar or approved third-party vendor who accesses I-Voters.

[**ARC 4103C**, IAB 10/24/18, effective 11/28/18]

721—29.2(47) Cybersecurity training.

29.2(1) All users who access the I-Voters database must complete annual training programs on principles of cybersecurity. Upon completion of the training, a user shall transmit proof of completion to the state registrar. The state registrar shall maintain a list of approved training programs on the secretary of state's website. The state registrar shall consult with the OCIO or the federal Election Assistance Commission before adding trainings to the list of approved programs. If requested by the office of the chief information officer, the federal Election Assistance Commission, or a county registrar, the state registrar may review and add recommended cybersecurity training programs to the approved list.

29.2(2) The state registrar may disable any user account if the user does not complete the training within 30 days of access granted, or on the anniversary date set by the state registrar.

29.2(3) The state registrar may temporarily waive this requirement for any user if the state registrar believes it is necessary to the execution of the election.

[**ARC 4103C**, IAB 10/24/18, effective 11/28/18]

721—29.3(47) Cybersecurity incident or breach.

29.3(1) A commissioner who identifies or suspects an actual or possible cybersecurity incident or breach shall report the incident within 24 hours to the state commissioner. Upon receiving the report, the state commissioner shall alert the appropriate state or federal law enforcement agencies, including but not limited to the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the OCIO, and the vendor responsible for maintaining the affected technology. The

state commissioner may disseminate the information to other federal, state, and local agencies, or their designees, as the state commissioner deems necessary.

29.3(2) Information reported to the state commissioner under this rule shall be exempt from public records requests pursuant to Iowa Code section 22.7(50).

29.3(3) Nothing in this rule prohibits a commissioner from alerting local law enforcement prior to contacting the state commissioner in the event of an incident or breach.

[**ARC 4103C**, IAB 10/24/18, effective 11/28/18; **ARC 5036C**, IAB 5/6/20, effective 6/10/20]

721—29.4(47) Election security by the commissioners.

29.4(1) At the start of each calendar year, the commissioner shall provide to the state commissioner the following information:

a. The full personnel roster, phone numbers, and email addresses of the commissioner's office that identify who from the office will participate in election administration in any form throughout the year. This does not include precinct election workers.

(1) The roster will identify the personnel that the commissioner considers critical to the successful execution of elections.

(2) The roster will further identify a technical point-of-contact (POC) for the state commissioner. If the commissioner wishes to serve as the POC, the commissioner will also designate an additional POC. The POC needs to be a government employee but does not necessarily need to be a person within the commissioner's office.

b. A list of other county employees who may be involved in the event of an incident in the county.

29.4(2) Every commissioner shall be a member of the Elections Infrastructure Information Sharing and Analysis Center. The state commissioner shall provide information on how to become a member upon request by a commissioner.

29.4(3) In every odd-numbered year, every commissioner shall request the following services from CISA. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than CISA for substantively similar services. A failure of CISA to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Cyber resilience review.

b. Risk and vulnerability assessment.

c. External dependencies management assessment.

d. Remote penetration testing.

e. Protective security assessment.

29.4(4) Every commissioner shall utilize the following services from OCIO. The state commissioner shall provide information on how to request services upon request by a commissioner. A commissioner, with prior written approval from the state commissioner, may choose to use a vendor other than OCIO for substantively similar services. A failure of OCIO to provide properly requested services to a commissioner does not constitute a technical violation for purposes of Iowa Code section 39A.6.

a. Intrusion detection system.

b. Endpoint malware detection.

c. Cybersecurity training, including phishing assessments.

d. Vulnerability management.

29.4(5) Every commissioner shall request a weekly vulnerability scanning by CISA.

29.4(6) A commissioner shall remediate all critical or high-risk vulnerabilities identified by any assessment.

29.4(7) The state commissioner may require every commissioner and commissioner's staff to participate in phishing assessments.

29.4(8) Commissioners may choose to participate in any other assessments or testing from vendors approved by the state commissioner. Commissioners shall notify the state commissioner when any assessments are scheduled.

29.4(9) The state commissioner may require a commissioner and commissioner's staff to participate in any assessment or training that the state commissioner arranges.

29.4(10) A commissioner shall use only county-issued email for the conduct of elections. This applies to all full-time and part-time staff of the commissioner as well as the commissioner. No other email addresses are permitted for full-time and part-time employees of the county who assist in any part of the administration or security of elections for the conduct of elections. However, this does not apply to precinct election officials who are not normally employed by the county on a regular basis in another capacity. This prohibition includes forwarding election business emails to a personal email address. This does not include out-of-band emails created and authorized as a part of a continuity of government plan or an incident response plan.

29.4(11) Any county information technology infrastructure that is used to access or conduct any part of elections in the state is subject to the following requirements:

a. Passwords to access the county network must be compliant with the standards enumerated by either the National Institute of Standards and Technology, the OCIO, or guidance issued by the state commissioner.

b. Session-lock timeout standards must be compliant with the standards enumerated by either the National Institute of Standards and Technology or guidance issued by the state commissioner.

c. A current inventory of IT assets assigned to the commissioner's office shall be kept.

d. Daily, weekly and monthly data backups within the commissioner's office will be maintained and physically or logically separated from production data.

29.4(12) The website of a commissioner shall have a top-level domain of ".gov" and shall utilize secure socket layer or transport layer security certificates for all publicly facing websites. A commissioner's agreement with OCIO to use a subdomain of ".iowa.gov" is sufficient to satisfy this requirement. A commissioner's site that redirects traffic from a different top-level domain to a ".gov" domain is sufficient to satisfy this requirement.

29.4(13) If the state commissioner is satisfied that a county has an adequate alternative to any requirement in this rule, the state commissioner may waive that requirement. It is the sole discretion of the state commissioner whether a county qualifies for a waiver.

29.4(14) Except where otherwise exempted, failure by a commissioner to follow these rules constitutes a technical violation pursuant to Iowa Code section 39A.6.

[**ARC 5036C**, IAB 5/6/20, effective 6/10/20]

721—29.5(47) Emergency or incident response plans.

29.5(1) Every commissioner shall have an election security incident response plan. A commissioner whose election-specific plan is part of a larger county-level emergency response plan, continuity of government plan, or incident response plan satisfies this requirement.

29.5(2) Every commissioner shall review the plan at least annually and make updates as necessary.

29.5(3) A commissioner shall provide the plan to the state commissioner at the state commissioner's request.

29.5(4) Information shared under this rule shall retain protection as a nonpublic, confidential record pursuant to Iowa Code section 47.1(6).

[**ARC 5036C**, IAB 5/6/20, effective 6/10/20]

721—29.6(47) Social media accounts.

29.6(1) A commissioner using a social media account for official elections-related communication shall request "verified" or similar recognition. The state commissioner shall provide information on the subject upon request by a commissioner.

29.6(2) A commissioner using a social media account shall protect the account using multifactor authentication.

29.6(3) The state commissioner may require that commissioners use additional security measures for social media accounts, based on emerging best practices.

[**ARC 5036C**, IAB 5/6/20, effective 6/10/20]

These rules are intended to implement Iowa Code section 47.7(2).

[Filed ARC 4103C (Notice ARC 3914C, IAB 8/1/18), IAB 10/24/18, effective 11/28/18]
[Filed ARC 5036C (Notice ARC 4965C, IAB 3/11/20), IAB 5/6/20, effective 6/10/20]