209 NAC 1 (DRAFT)
NEW CHAPTER FOR ADOPTON

TITLE 209 – INFORMATION TECHNOLOGY COMMISSION

CHAPTER 1 – RECORDS RELATING TO THE NATURE, LOCATION, OR FUNCTION OF CYBERSECURITY

001. AUTHORITY. Neb. Rev. Stat. § 84-712.05(26).

002. RECORDS RELATING TO THE NATURE, LOCATION, OR FUNCTION OF CYBERSECURITY. For purposes of Neb. Rev. Stat. § 84-712.05(26), records relating to the nature, location, or function of cybersecurity include items that a reasonable person, knowledgeable of cybersecurity best practices, would conclude that public disclosure of such items would create a substantial likelihood of endangering the security of the public entity's information technology infrastructure. Such items include but are not limited to the following:

002.01 PERSONNEL. (a) The identity of personnel responsible for configuring or maintaining cybersecurity systems and assets; and (b) the identity of personnel in leadership roles who have direct responsibility or oversight of cybersecurity system and assets.

002.02 RISK MANAGEMENT. (a) Risk assessment reports; (b) vulnerability assessments; and (c) penetration testing reports.

002.03 COMPLIANCE AND LEGAL DOCUMENTATION. (a) Contract language that describes or defines cybersecurity related services and capabilities; (b) regulatory compliance documentation; and (c) technology audit reports.

002.04 TECHNICAL CONTROLS AND CONFIGURATIONS. (a) Firewall configurations; (b) network segmentation plans; (c) access control policies; (d) encryption and key management policies; and (e) endpoint security settings and controls.

002.05 MONITORING AND LOGGING. (a) Log management plans; (b) security information and event management (SIEM) reports or data; (c) intrusion detection/prevention system (IDS/IPS) logs; (d) vulnerability scanning logs; (e) endpoint defense logs; and (f) firewall logs.

002.06 INCIDENT RESPONSE AND FORENSICS. (a) Incident handling documentation; (b) incident response plans; (c) forensics analysis reports; and (d) evidence collection procedures.

002.07 EMPLOYEE AWARENESS AND TRAINING. (a) Security awareness training materials; (b) phishing simulation reports; and (c) training attendance records.

002.08 SOFTWARE AND PATCH MANAGEMENT. (a) Software inventory; (b) patch management records; and (c) configuration management documentation.

002.09 ACCESS CONTROL AND AUTHENTICATION. (a) Identity and access management policies; (b) password policies; and (c) multi-factor authentication (MFA) policies.

002.10 DATA PROTECTION DOCUMENTATION. (a) Backup strategy documentation; (b) business continuity and disaster recovery (BCDR) plans; (c) data loss prevention (DLP) configurations and documentation; and (d) secure data storage and disposal documentation.

002.11 THIRD-PARTY AND VENDOR MANAGEMENT. (a) Third-party security assessments; and (b) vendor risk management documentation.