

## **N.D. Cent. Code, § 54-59.1-01**

Current through all legislation from the 68th Legislative Assembly - Special Session (2023).

*North Dakota Century Code Annotated > TITLE 54 State Government (Chs. 54-01 — 54-66) > CHAPTER 54-59.1 Cybersecurity Incident Reporting Requirements (§§ 54-59.1-01 — 54-59.1-07)*

### **54-59.1-01. Definitions.**

---

As used in this chapter, unless the context otherwise requires:

1. “Breach” means unauthorized access or acquisition of computerized data that has not been secured by encryption or other methods or technology that renders electronic files, media, or databases unreadable or unusable. Good-faith acquisitions of personal information by an employee or agent of the employee is not a breach of security of the system if the personal information is not used or subject to further unauthorized disclosure.
2. “Criminal justice information” means private or sensitive information collected by federal, state, or local law enforcement including the following:
  - a. Fingerprints or other biometric information;
  - b. Criminal background and investigation information; and
  - c. Personal information.
3. “Denial of service attack” means an attack against a computer system designed to make the system inaccessible to users.
4. “Department” means the information technology department.
5. “Entity” means an executive branch state agency or a political subdivision within the state.
6. “Financial information” means banking, credit, or other account information that, if accessed without being authorized, may result in potential harm to an individual and includes:
  - a. Account numbers or codes;
  - b. Credit card expiration dates;
  - c. Credit card security codes;
  - d. Bank account statements; and
  - e. Records of financial transactions.
7. “Health insurance information” means an individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify an individual.

- 8.** “Identity theft or identity fraud” means all types of crime in which an individual wrongfully obtains and uses another individual’s personal data in a way that involves fraud or deception, most commonly for economic gain.
- 9.** “Malware” means software or firmware intended to perform an unauthorized process that will have adverse effect on the confidentiality, integrity, or availability of an information system and includes a virus, worm, trojan horse, spyware, adware, or other code-based system that infects hosts.
- 10.** “Medical information” means an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- 11.** “Personal information” means an individual’s first name or first initial and last name in combination with the following when names and data are not encrypted, but does not include information available to the public from federal, state, or local government records:
- a.** The individual’s social security number;
  - b.** The operator’s license number assigned to an individual under section 39-06-14;
  - c.** A nondriver photo identification card number assigned to the individual under section 39-06-03.1;
  - d.** The individual’s financial institution account number, credit card number, or debit card number in combination with required security codes, access codes, or passwords that permit access to an individual’s financial accounts;
  - e.** The individual’s date of birth;
  - f.** The maiden name of the individual’s mother;
  - g.** Medical information;
  - h.** Health insurance information;
  - i.** An identification number assigned to the individual by the individual’s employer in combination with security codes, access codes, or passwords; or
  - j.** The individual’s digitized or other electronic signature.
- 12.** “Ransom” means a payment for services or goods to a malicious agent to:
- a.** Decrypt data on a computer system;
  - b.** Retrieve lost or stolen data; or
  - c.** Prevent the disclosure and dissemination of information.
- 13.** “Regulated information” means information and information technology resource protection requirements established by the federal government and regulating organizations.
- 14.** “Regulating organizations” means organizations that issue laws, regulations, policies, guidelines, and standards, including the:
- a.** Federal bureau of investigation;
  - b.** Internal revenue service;
  - c.** Social security administration;

- d. Federal deposit insurance corporation;
  - e. United States department of health and human services;
  - f. Centers for Medicare and Medicaid services; and
  - g. Payment card industry security standards council.
- 15. “Significant damage” means:
  - a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;
  - b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;
  - c. A financial loss of ten thousand dollars or more as estimated by the entity; or
  - d. Harm to individuals involving loss of life or serious life-threatening injuries.

## History

---

S.L. 2021, ch. 445, § 1, effective August 1, 2021.

North Dakota Century Code Annotated  
Copyright © 2024 All rights reserved.