DATA PROTECTION & SECURITY BREACHES

Definitions:
For the purpose of this policy:

- *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.
- *Private information* is defined as information protected under federal laws such as, but not limited to, the Family Educational Rights and Privacy Act (FERPA), information defined as confidential or exempt in NDCC Ch. 44-04, and data defined as "personal information" in NDCC 51-30-01(4). Private information does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.
- *Security system plan* includes:
    - Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, communications, or consultations relating directly to the physical or electronic security of a public facility, or any critical infrastructure, whether owned by or leased to the state or any of its political subdivisions, or any privately owned or leased critical infrastructure if the plan or a portion of the plan is in the possession of a public entity;
    - Information relating to cybersecurity defenses, or threats, attacks, attempted attacks, and vulnerabilities of cyber system operations relating directly to the physical or electronic security of a public facility, or any critical infrastructure, whether owned by or leased to the state or any of its political subdivisions, or any privately owned or leased critical infrastructure if the information is in the possession of a public entity;
    - Threat assessments;
    - Vulnerability and capability assessments conducted by a public entity, or any private entity;
    - Threat response plans; and
    - Emergency evacuation plans.

Data Protection
Yellowstone School District #14 will take reasonable security measures to guard against the foreseeable loss of private information. In determining the reasonableness of the district's security measures, the Board will consider the value of private information in the district's possession and the potential damages associated with the loss or compromise of this data. All security measures will be delineated in a security system plan, which is exempt from North Dakota open records law. Creation of, discussion of, and revision to this plan will occur in executive session in accordance with North Dakota law.

Security Breach
Any identified or suspected breach or cybersecurity incident that affects the confidentiality, integrity, or availability of information systems, data, or services must be reported immediately to the Superintendent. The Superintendent shall put procedures in place to notify state residents affected by the breach and any state agencies as required by law.

Complementing NDSBA Templates (may contain items not adopted by the Board)

- ACDA, Acceptable Use
- BCAD, Executive Session
- IDC-AR, Security Breach Procedure

End of Yellowstone Policy IDC ..... Adopted: 11/20/2023