980 DATA BREACH RESONSE POLICY

I. PURPOSE

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy defines to whom it applies and under what circumstances, and includes the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be publicized and made available to all personnel whose duties involve data privacy and security protection.

Independent School District No. 182, Crosby-Ironton Public School's intentions for adopting a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how the school district's established culture of openness, trust and integrity should respond to such activity. Crosby-Ironton School District is committed to protecting its employees, patrons, partners and the school district from illegal or damaging actions by individuals, either knowingly or unknowingly.

II. REQUIRED ACTION

This policy mandates that any individual who suspects that a theft, breach or exposure of the district's protected or sensitive data has occurred shall immediately provide a description of what occurred via e-mail to support@crosbyironton.zendesk.com, by calling 545-8833, or through the use of the help desk reporting web page at http://crosbyironton.zendesk.com/. This e-mail address, phone number, and web page are monitored by the District's Technology Department. This team will investigate all reported thefts, data breaches and exposures to determine if a theft, breach or exposure has actually occurred. If a theft, breach or exposure has occurred, the Technology Department will follow the appropriate procedure.

III. SCOPE

This policy applies to all users that collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Crosby-Ironton School District members. Any agreements with vendors will contain language similar that protects personally identifiable information.

Users include all members of the Crosby-Ironton School District community to the extent they have authorized access to information resources, and may include staff, contractors, consultants, interns, temporary employees, parents, and students.

IV. POLICY CONFIRMED THEFT, DATA BREACH OR EXPOSURE OF PROTECTED DATA OR SENSITIVE DATA

As soon as a theft, data breach or exposure containing Crosby-Ironton School District protected or sensitive data is identified and verified, the process of removing all access to that resource will begin.

1. The Technology Coordinator will chair an incident response team to handle the breach or exposure.

The team will include members from the following (if applicable):

- Technology Department
- Administration
- Finance
- Legal
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Superintendent

2. Confirmed theft, breach or exposure of school district data

The Technology Coordinator and Superintendent will be notified of the theft, breach or exposure. The Technology Department, along with the designated forensic team, will analyze the breach or exposure to determine the root cause and extent of the breach.

3. Work with Forensic Investigators

Crosby-Ironton School District will provide access to forensic investigators and experts if deemed necessary that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

4. Develop a Communication Plan.

Work with Crosby-Ironton School District communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

V. ENFORCEMENT

Any school district personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated and be held legally responsible for any liability and associated costs incurred to correct the breach.

VI. DEFINITIONS

- Encryption or Encrypted Data – Encryption and encrypted data are the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
- Plain text – Unencrypted data.
- Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).
- Protected Health Information (PHI) - Under Unites States law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
- Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
- Protected data - See Personally Identifiable Information and Protected Health Information.
- Information Resource - The data and information assets of an organization, department or unit.
- Safeguards – Countermeasures or controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
- Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

References: SANS Institute August 17, 2016 Initial Version