Cherokee Community School District

600 W. Bluff St

Cherokee, Iowa. 51012

(712) 225-6767

Data Incident Response Plan

This page outlines the evaluation and response procedures of a reported cybersecurity event. A cybersecurity event may or may not include Personally Identifiable Information (PII). PII includes information that can be used to distinguish or trace an individual's (student, parent, or employee) identity either directly or indirectly through linkages with other information including name, address, and/or identification numbers.

As recommended by the National Institute of Standards and Technology (NIST), the District's Data Incident Response Team focuses on the: Preparation, Detection, Analysis, Containment, Eradication, and Recovery of data. When a data incident is reported or discovered, this response plan is immediately set into motion.

1. ***IDENTIFY***

Validate the data breach:

- Examine the initial information to confirm that a breach has occurred.
- If criminal activity is suspected, notify law enforcement and follow any applicable federal, State, or local legal requirements relating to the notification of law enforcement (The decision to involve outside entities, including law enforcement, should generally be made in consultation with executive leadership and legal counsel).

If a breach has occurred:

- The Superintendent or designee will assign a District-level administrator, to serve as an incident manager to coordinate multiple organizational units and the overall incident response. {Typically, the team manager is the incident manager; alternatively, the team manager assigns another individual to lead the response activities);
- Determine if there was a breach of PII;
- If possible, identify the type of information disclosed and estimate the method of disclosure (internal/external disclosure, malicious attack, or accidental); and
- Begin breach response documentation and reporting process.

Assemble the District's Data Incident Response Team:

- Information Security and Data Protection Officer, Director of Instructional Technology, and appropriate other Administration and Staff.

2. DETECT AND PROTECT

- Immediately determine the status of the breach (on-going, active, or post breach).
- If the breach is active or on-going, take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserve evidence for investigation.
- Document all mitigation efforts for later analysis.
- Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise.

Determine the scope and composition of the breach:

- Identify all affected data, machines, and devices.
- Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination.
- Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.
- Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

Notify Law Enforcement (situation dependent):

- Consult legal counsel to examine any applicable federal, State, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements.
- Seek involvement of law enforcement when there is a reason to believe that a crime has been committed or to maintain compliance with federal, State, or local legal requirements for breach notification.
- In concert with District Administration and legal counsel, designate a single organizational representative authorized to initiate and/or communicate breach details to any party, including law enforcement.

3. ***RESPOND***

Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification:

- Determine whether notification is warranted and when it should be made.
- Notify affected individuals whose sensitive information, including PII, has been compromised, as required by applicable federal, State, and local laws.

4. ***RECOVER***

Collect and review any breach response documentation and analyses reports

- Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.
- Address and/or mitigate the cause(s) of the data breach.
- Solicit feedback from the responders and any affected entities.
- Review breach response activities and feedback from involved parties to determine response effectiveness.
- Make necessary modifications to the District's breach response strategy to improve the response process.
- Enhance and modify the District's information security and training programs, which includes developing countermeasures to mitigate and remediate previous breaches; lessons learned must be integrated so that past breaches do not reoccur.