Charlo School District

Cyber Incident Response

A cyber incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

The School District is prepared to respond to cyber security incidents, to protect District systems and data, and prevent disruption of educational and related services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

Responsibilities of Specific Staff Members

Individual Information Technology User:
All users of District computing resources shall honor District policy and be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

District Information Technology Director
Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of School District information systems. Incident response support resources may include, but is not limited to: School District information technology staff, a response team outlined in this policy, and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. CSIRT responsibilities shall be defined in the School District position descriptions.

District Superintendent:
Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Procedures

Designated officials within the District shall review and approve incident response plans and procedures at least annually. The incident response plans and/or procedures shall:

- Provide the District with a roadmap for implementing its incident response capability
- Describe the structure and organization of the incident response capability
- Provide a high-level approach for how the incident response capability fits into the overall organization

- Meet the unique requirements of the District, which relate to mission, size, structure, and functions
- Define reportable incidents
- Provide metrics for measuring the incident response capability within the organization
- Define the resources and management support needed to effectively maintain and mature an incident response capability

Upon completion of the latest incident response plan, designated officials shall:

- Distribute copies of the incident response plan/procedures to incident response personnel.
- Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.
- Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.
- Test the incident response capability for the information systems they support at least annually to determine effectiveness.
- Track and document information system security incidents.
- Promptly report cyber security incident information to appropriate authorities in accordance with reporting procedures.

Policy History:
Adopted on: 12/19/19
Reviewed on:
Revised on: