Missoula County Public Schools
Non-Instructional Operations 8550
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 of 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 Staff Members
Individual Information Technology User
All staff 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 or Equivalent Position
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 are not limited to: School District information technology staff, a response team outlined in procedure, and access to forensics services.
Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The membership and responsibilities of the CSIRT shall be defined in the cyber incident response procedures.
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.
Policy History:
First Reading by Board on February 11, 2020 and posted for public comment
Adopted on: March 10, 2020