8-801. Incident response.

Computer systems are subject to a wide range of mishaps from corrupted data files, to viruses, to natural disasters. These incidents can occur at any time of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other ways (e.g., disaster recovery plans). Responses to an incident can range from recovering compromised systems to the collection of evidence for a variety of forensic requirements. Preparation and planning for incidents, and ensuring the right resources are available, are critical to the state's ability to adequately detect, respond and recover from security incidents.

The security policy requires the establishment and maintenance of a computer security incident response capability that is in effect 24x7. This document identifies key steps for reporting security incidents and establishes formal reporting requirements for all such instances to the state's senior management and agency officials responsible for reporting to federal offices.

These procedures also describe the way Office of the CIO or agency technical staff will aid the in the eradication, recovery, and permanent remediation of the root cause of the incident. This is important to preserve as much evidence as practical while keeping in mind that prevention of damage is of the highest priority.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-801.pdf