

Incident Handling Policy

Purpose

Dakota State University (DSU) has established a formal policy regarding incident handling. The purpose of this policy is to ensure that all incidents are recorded and acted on in a timely manner in accordance with the South Dakota Board of Regents (SDBOR), state, local, or federal policies, laws or regulations, as well as to be in compliance with the Payment Card Industry Data Security Standards (PCI-DSS).

Audience

This policy applies to all users of IT Systems, including but not limited to students, faculty, staff, affiliated campus organizations or non-profit groups, and other groups and organizations relying on the SDBOR as a host through contractual relationships. It applies to the use of all IT Systems and other SDBOR contracted entities.

This policy also applies to use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by the SDBOR while connected in any to IT Systems.

Policy

DSU formally adopts the SDBOR policy and procedure for incident handling in order to ensure that response to the compromise of electronic resources is performed in a comprehensive manner which:

- addresses the relevant aspects of the incident;
- stops the incident (with minimal impact to customers); and
- establishes a method to defend data against similar incidents.

Definitions

Incident – An incident is a suspected, observed or reported breach of the SDBOR Acceptable Use Policy whether observed directly, observed through monitoring of systems or networks, alleged by any person or suspected through analysis of logs or emails or other documents.

IT Systems – The computers, terminals, printers, networks, online and offline storage media and related equipment, software, and data files that are owned, managed, or

maintained by ITS and the SDBOR. For example, IT Systems include but are not limited to Universities and departmental information systems, faculty research systems, desktop computers, the campus network, and BOR general access computer clusters.

Related Policies

- SD Board of Regents' Acceptable Use of Information Systems Policy 7:1
- SD Board of Regents' Security of Information Technology Systems Policy 7:4
- SD Board of Regents' Incident Handling Policy
- DSU Computing Privileges Policy

Revision History

This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DSU's needs and goals.

Revision Date	Reviewed by
2014-03-14	Security Policy Committee