UNIVERSITY OF SOUTH DAKOTA

Policy Number:	5.004
Originating Office:	Information Technology Services
Responsible Executive:	Vice President for Administration and Technology
Date Issued:	12/08/2010
Date Last Revised:	02/10/2012

Incident Handling

Policy Contents

I. REASON FOR THIS POLICY

The University of South Dakota (USD) has established a formal policy and supporting procedures regarding Incident Handling. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the university's needs and goals.

This policy also ensures USD's compliance with Payment Card Industry Data Security Standards (PCI DSS) requirements.

Policy last reviewed 8/5/15 by CIO Management Team

II. STATEMENT OF POLICY

USD will establish an Incident Handling Plan in order to ensure that response to 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.

This policy applies to all electronic resources under the care of the University.

III. DEFINITIONS

Incident - (ref. http://www.us-cert.gov/federal/incidentDefinition.html) An incident is the act of violating an explicit or implied security policy.

These include but are not limited to:

- attempts (either failed of successful) to gain unauthorized access to a system or its data

- unwanted disruption or denial of service

- the unauthorized use of a system for the processing or storage of data

- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent

Payment Brands - credit card companies or processors of credit cards (i.e. Visa)

Cardholder Data - the combination of a credit carholder's name, Primary Account Number (PAN), service code, and expiration date

IV. PROCEDURES

The Incident Handling Plan includes, at a minimum, roles, responsibilities and communication strategies in the event of a compromise.

The Incident Handling Plan includes specific incident response, business recovery and continuity procedures and data backup processes.

The Incident Handling Plan includes coverage and response mechanisms for all critical system components and all other I.T. resources deemed critical by the university.

The Incident Handling Plan also includes reference to, or inclusion of, incident response procedures from the payment brands as they relate to University responsibilities.

If the incident involves compromise of payment cardholder data, the plan will include legal requirements for reporting any compromises and notification of the payment brands.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Not Applicable