UN Digital Security Incident Response PCI Policy

POLICY CONTENTS

Scope
Policy Statement
Reason for Policy
Definitions
Related Information
History

Scope

This policy applies to all university personnel and entities handling credit card information and is to be followed by all university technical support staff and information asset owners.

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

Overview

The procedures contained within this policy are meant to provide parameters on how the University of Nebraska campuses will respond to cybersecurity incidents. Detailed procedures based on this policy have been developed to be used for responding to incidents and are documented.

When a potential or actual security incident or violation is observed, the individual will inform his supervisor who will request the Information Security Office to investigate the situation. The importance of immediate notification and reporting of a security incident is a prime factor in reducing the vulnerability of the enterprise and in recovering any assets that may be in question. To support this objective, the Information Security Office is on call at the following:

UNL: Report the incident at https://its.unl.edu/security/security-incident-reporting-form or at 402-472-5700

The reporting area is to assemble all relevant information and material identified with the incident, if possible. Any material involved shall be impounded to preserve and retain its authenticity for the investigation and evaluation process. Upon notification, the Information Security Office will assign a security officer to investigate the reported situation. The case handler will obtain the facts from individuals regarding the incident to file an information security incident report. The report shall not include interjection of personal or preconceived opinions and views of the incident. Any interjection of personal views may bias the veracity and completeness of the investigation.

While compiling all relevant information on the incident, the case handler will include a narrative description of events and actions associated with this incident. This should be in chronological sequence. The report will include a description section that should include time and location, beginning prior to and continuing through the incident. The description shall include the initial impact on the information system and/or impact to the enterprise service in the area of reliability or data integrity. Also included in the report are the detailed steps or actions by individuals (by title or area) in chronological sequence that may have been implemented to correct, control, or resolve the effects or results of the incident.

Analysis/Evaluation

Analysis or evaluation of a security incident must not be attempted until all relevant facts and information have been assembled. Any premature analysis or evaluation of an incident may produce a biased and incomplete result. Recommendations may or may not be appropriate or feasible to eliminate the recurrence of a specific incident. The information security incident report is to be completed within five working days.

The Incident Response procedures will be followed to report and respond to cybersecurity incidents that may adversely impact university IT assets.

Reason for Policy

The university's digital assets constitute a substantial university resource, and the university's mission relies significantly on the security and reliability of these assets. The prompt handling of digital asset-related incidents is necessary to protect other university assets, as well as the information stored by these assets.

Definitions

Digital Asset: A digital asset is any electronic system that stores, transports, contains or has access to university data.

Digital Security Incident: Any event, actual or reasonably suspected to have occurred, which destroys or degrades the availability, integrity and confidentiality of university digital resources, computer-based systems, computer-maintained data files, documents or procedures. Any digital event which threatens to harm the University's reputation, brand or put it out of compliance.

Related Information

Additional Contacts

- **Chief Information Officer (CIO):** The CIO has supervision of information assets at the university and provides oversight, direction, and support for information technology of the university.
- **Chief Information Security Officer (CISO)**: The CISO is appointed by the CIO and is responsible for coordinating responses to cybersecurity incidents and assembling teams in support of this goal. The CISO is responsible for providing oversight, direction, and management of the information security function at the university. The CISO is responsible for enforcing this policy.
- **Information Security Office:** This is the department within ITS which is charged with the responsibility for information security at the university.
- **Case Handler:** The case handler is a member of the Information Security Office team who has been assigned the task of coordinating the response to a digital security incident. The job of the case handler is to maintain the case's progress toward resolution.
- **Information Asset Owner**: The information asset owner is responsible for the operation and/or use of an information asset.
- **Information Asset Technical Contact:** The information asset technical contact works with the information asset owner to maintain the functionality of the information asset. This may or may not be the same person as the information asset owner.

NU Executive Memorandum 16
NU Executive Memorandum 26
State of Nebraska Consumer Notification of Data Security Breach Act of 2006

This policy covers the following sections of PCI-DSS 3.2:

- 11.1.2 Implement incident response procedures.
- 11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.
- 12.10 Implement an incident response plan.

History

This policy is a new policy created in 2017.