UNIVERSITY OF NEBRASKA AT OMAHA

Effective: 01-31-2015
Last Revised: 08-31-2016

Responsible University Administrator:
Chief Information Officer

Responsible University Office:
Information Security

Policy Contact:
Information Security • security@unomaha.edu

Digital Security Incident Response

POLICY CONTENTS

Scope

This policy applies to all university personnel and entities and is to be read by all university technical support staff and information asset owners.

Policy Statement

Overview

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

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 number: 402.554.2492. You may also send an email to security@unomaha.edu to report an incident.

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 two major items or concerns required for the evaluation. A narrative description of events and actions associated with this incident. This should be in chronological sequence. The description 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. 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 procedures listed in the following sections are in place to report and respond to cybersecurity incidents that may adversely impact university IT assets.

Reason for Policy

UNO'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.

Procedures

1. Incident Alert and Notification
When a cybersecurity incident has occurred on an information asset which is reasonably believed to have had the security compromised or has been used in a manner that is contrary to applicable University policies, state, or federal statutes, the incident will be reported to the Information Security Office. The incident will then be assigned to a case handler and entered into and tracked in the case management system, which will aid in managing and resolving the case as well as providing a history of incidents and actions that have been taken during case resolution. The case management system will also aid in assigning tasks to individuals investigating the case.

2. Assessment/Triage
Incident responses are classified into categories depending on the type of data, the type of incident, and the number of users supported by the information asset. The classification of the asset will be determined by the case handler, with input from the information asset owner and technical support with the approval of the Chief Information Security Officer (CISO). The response level will largely determine the steps that need to be taken to resolve the incident. The assignment of a response level is not fixed during the entire case. In the course of the investigation, the case handler or the CISO may choose to escalate or de-escalate the response level, based on information obtained during the investigation. As a part of this phase, the information asset may be denied access to other information assets if deemed necessary to protect other assets and University data.

3. Investigation of Scene
This phase includes the determination of the root cause and extent of the cybersecurity incident. In higher response level cases, careful preservation of evidence is critical, given that legal or University disciplinary action become necessary. Also in higher level cases, forensic analysis may be conducted by an outside contractor to ensure accuracy and unbiased results. In cases where the seizure of an information asset is necessary, the seizure will be conducted by UNO Campus Security, in conjunction with the CISO. If necessary, the seized information asset will be turned over to the proper investigating authorities.

4. Actions/Forensics
A cybersecurity incident's response actions are determined by the level of the case, the nature of the incident, and the personnel involved with the investigation of the case. Higher response level cases may require an outside contractor to perform forensic analysis on an information asset. In these cases, the level of forensic analysis to be completed will be determined by the Information Security Officer, in conjunction with the Digital Security Incident Response Team (DSIRT). In all other cases, the case handler, in conjunction with the information asset owner or the information asset technical contact, will determine the actions necessary to remedy the information asset and prevent future occurrences of cybersecurity incidents. Actions may include the inspection of the information asset by an individual or a system to verify the security of the asset.

5. Service Restoration
Information assets represent a vital part of the University operations. In the wake of a cybersecurity incident, a high level of importance is placed on restoring connectivity and functionality to the affected information asset(s). Service restoration must be completed in a timely manner, but in a way that maintains the security, confidentiality, and reliability of the University information assets. If the affected information asset is sent away for forensic analysis, it may become necessary to implement a temporary replacement for the affected asset. When restoring service, it is important to ensure that the information asset is secure and properly configured and any necessary action steps have been completed prior to service being restored in order to avoid repetition of the incident or other incidents. In some cases, the reporting phase may need to be completed and signed off before service is restored.

6. Reporting
Completion of proper reporting for each cybersecurity incident is vital. The level of reporting is dependent on the level of response, as well as input from the case handler and the Information Security Officer. Some levels of reporting may require an information asset owner to obtain dean or department head documented approval before service is restored. Higher level responses that may involve confidential data could require assembly of the CIRT to evaluate the possibility of a breach notification. Assembly of the DSIRT will be made by the CISO or designate. A case report will be required for each case.

7. Case Analysis/Follow Up
Upon completion of the cybersecurity incident investigation, the incident report will be distributed to those involved for their review. Review of the incident report will provide valuable insight. The case notes contained within the incident report will be used to determine if a change in network or system policies is needed to prevent future occurrences of similar incidents. The case notes will also be used to determine if there are additional follow-up actions needed to resolve this incident; including determining if the recommendations from the incident report have been implemented. And finally, the incident report will be used to determine if cybersecurity incident procedures are functioning correctly and if any changes are required to make the procedures more effective or efficient.

8. Breach Notification

The CISO will, in consultation with the DSIRT, determine if a notification is necessary and to what degree (e.g. whether legal should be notified).

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 UNO 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.

Digital Security Incident Response Team (DSIRT): The DSIRT is assembled by the CISO and will be composed of representatives from several key UNO departments, which could include, but are not limited to: Information Services (IS), UNO Public Safety, University Communications, Academic Affairs, Business and Finance, and the Chancellor's Office. The team's responsibility is to determine appropriate responses to priority incidents as deemed necessary. The individuals composing the team will be chosen according to the nature of the case, the data involved, and the ownership of the source system.

Incident Response Levels

Level 3 Response - Critical Response
A Level 3 response is applied to a digital security incident when an information asset is suspected of having access to regulated data, as defined by the UNO Regulated Data Security Policy, University of Nebraska policy, and state or federal statutes. Digital security incidents may also require a Level 3 response if the information asset has been used in a way contrary to applicable University policies and state or federal statutes (which may result in university disciplinary action and civil or criminal sanctions) or it is apparent that a deliberate malicious attack is being conducted upon university information assets.

Level 2 Response – Standard Response
A Level 2 response is applied to a digital security incident when there is no apparent breach of regulated data as defined by University of Nebraska policy and state or federal statutes. A Level 2 response also applies to information assets that support multiple users or have affected the normal operation of other assets including affecting the availability of information resources. A Level 2 response may also be triggered if a deliberate attack on information assets is found but the risk profile or quantity of attacks is low enough to not warrant a Level 3 response.

Level 1 Response – Basic Response
A Level 1 response is applied to a digital security incident where the affected information asset is a single-user system which has not affected the normal operation of other assets. That is, the incident has not affected the widespread availability or compromise of institutional data.

Related Information

Additional Contacts

Chief Information Officer (CIO)
The CIO has supervision of information assets at UNO 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 UNO. The CISO is responsible for enforcing this policy.

Information Security Office
This is the department within IS which is charged with the responsibility for information security at UNO.

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

UNO Regulated Data Security Policy

UNO Security Manual

History

This policy is an update to the Security Incident Response Plan that was previously updated in 2015.
