Northern Oklahoma College

Cybersecurity Incident Response Plan

Approval Date: 12/15/2021	Approved by the Northern Oklahoma College Board of Regents

Table of Contents

1 PURPOSE

The purpose of this Cybersecurity Incident Response Plan is to provide Northern Oklahoma College with a framework for responding to information security incidents which include but are not limited to system intrusions, disruption of service, system misuse, or any situation where confidentiality, integrity, or availability of sensitive data, may have been in question. It is essential to respond to cybersecurity incidents in an efficient and consistent manner to ensure college business continuity and minimize loss, corruption, or unintentional release of sensitive information. These procedures define standard methods for identifying, containing, eradicating and documenting the response to technology-based information security incidents.

Centralized notification and control of a cybersecurity incident investigation is necessary to ensure that immediate attention and appropriate resources are used to respond to incidents that could potentially disrupt the operation of all departments or compromise Northern Oklahoma College's data.

The primary goal of this plan is to restore normal service operation as quickly as possible and to minimize the adverse impact on Northern Oklahoma College operations while protecting its data.

2 SCOPE

All electronic devices owned or leased by Northern Oklahoma College or connected to Northern Oklahoma College's network including, but not limited to, computer workstations, servers, network switches, routers, and specialized computing devices, etc. are covered by this plan. Northern Oklahoma College may experience numerous events over time, but they may never reach the level of an incident or data breach. This plan covers incidents and data breaches. It does not cover events. See below for definitions.

DEFINITIONS

- **Event** – The National Institute of Standards and Technology (NIST) defines an event as "any observable occurrence in a system or network," such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection.
- **Incident** – A security incident violates or compromises the integrity, confidentiality or availability of an information asset. A cybersecurity incident is a violation or imminent threat of violation of technology security policies, acceptable use policies, or standard security practices. An incident may be a set of circumstances that threatens the confidentiality, integrity or availability of information, data or services at Northern Oklahoma College.
- **Breach** (aka **Data Breach** or **Personal Data Breach**) – An incident resulting in the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, and integrity of personal data. Data breaches may require notification to the affected individuals, regulatory authorities, credit reporting agencies or the media.
- **Personal Data** (aka **Personally Identifiable Information**) – Personal data is sometimes defined as an individual's first name or first initial and last name plus one or more of the following: SSN, Driver's License, Student ID, NOC access credentials, Credit Card or Debit card number combined with the security code, PIN, or password needed to access an account.

3 CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT)

Northern Oklahoma College's Cybersecurity Incident Response Team (CSIRT) consists of several key members. Below is a list of the current members of this Team and the definitions of each members role as well as a brief description of their responsibilities during a cybersecurity incident response.

As an incident progresses the core team will engage additional internal and external parties as deemed appropriate.

Incident Role	Name	Email	Phone
IT- Technical Lead	Michael Machia	michael.machia@noc.edu	580.628.6267
Incident Response Lead	Anita Simpson	anita.simpson@noc.edu	580.628.6237
Communications/ Public Relations	Sheri Snyder	sheri.snyder@noc.edu	580.628.6208
Physical Security	Jason Johnson	jason.johnson@noc.edu	580.628.2215
Human Resources	Shannon Cranford	shannon.cranford@noc.edu	580.628.6229
Additional Member(s)	Clark Harris	clark.harris@noc.edu	580.628.6200
	Linn Laughrey	linn.laughrey@noc.edu	580.628.6337
	Scott Cloud	scott.cloud@noc.edu	580.628.6444
	Shannon Lorg	shannon.lorg@noc.edu	580.628.6330

3.1 CSIRT ROLES AND RESPONSIBILITIES

Role	Responsibility	Actions
Cybersecurity Incident Response Team (CSIRT)	• Act as the lead function to investigate and coordinate incidents • Take appropriate steps to help contain and control the systems affected in an incident • Maintain inventory of incidents • Report incidents to the appropriate personnel • Act as the lead function to coordinate lessons learned and tests of this plan	Engaged in all information security incidents.
IT – Technical Lead	• Provide IT support and expertise to CSIRT • Take appropriate steps to help contain and control the systems affected in a security incident and preserve information that may be helpful during the investigation	IT is triggered when the incident involves a system they support or have expertise on.
Incident Response Manager	• Oversees and prioritizes actions during the detection, analysis, and containment of an incident • Conveys any special requirements to the rest of the CSIRT as well as communicating potential impact to the college President	Role is always established in any cybersecurity incident.
Communications	• Communicate (as necessary) with the media or outside sources • Communicate (as necessary) with employees, students or community	Communications are required when the incident involves the media or some public forum or when it involves internal employees or students.
Physical Security	• Communicate details to CSIRT when an incident occurs • Provide safety and security support	Physical security is required when the incident involves the safety of individuals, the preservation of evidence, or CSIRT needs their expertise to advise and act to contain and eradicate an incident.
Human Resources	• Coordinates employee communications regarding breaches of personal employee information • Assist in the communication of information to the state, legal offices or law enforcement concerning breaches in employee information • Direct any future inquiries to the CSIRT team	HR is required when a potential incident is identified concerning employee personal information.

RESPONSIBILITIES FOR ALL EMPLOYEES

- Making sure employees understand how to identify and report a suspected or actual security incident
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Cybersecurity Incident Response Team (CSIRT)
- Reporting any security related issues or concerns to their Division Chair or Department Manager, or to a member of the CSIRT
- Complying with the security policies and procedures of Northern Oklahoma College's IT Policies. This includes any updated or temporary measures introduced in response to a cybersecurity incident (e.g. for college continuity, incident recovery or to prevent recurrence of an incident)

4 INCIDENT RESPONSE PROCESS

There are a number of steps taken to respond to a cybersecurity incident. The following describes each step as part of the overall process. Note they are not always followed in sequence and sometimes may occur at the same time.

4.1 PREPARATION

It is essential to establish a Cybersecurity Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools. Tasks included in the Preparation phase include but are not limited to the following.

- Ensure appropriate parties are aware of incident reporting processes.
- Maintain and validate Network Diagrams and Asset Inventories.
- Review Penetration Test Reports and validate remediations to findings.
- Review Vulnerability Management Reports and validate remediation efforts.
- Ensure employees and students are aware and familiar with NOC IT Policies.
- Validate Logging, Alerting, and Monitoring policy compliance.
- Make sure systems and data backups are available in the event of loss of data, system corruption/virus infection or hardware failure.
- Consider what offline or alternative payment acceptance methods you could use if you were unable to take card payments on your ecommerce website, in-store or over the telephone using your usual methods.

4.2 DETECTION AND ANALYSIS

Detection and analysis represent the initial steps in identifying whether the occurrence is an incident or merely an event. This process will identify the severity and category it is, and who needs to be included depending on the situation. Any available information is captured and shared with the CSIRT. Efforts are focused on a rapid assessment rather than an in-depth investigation. The overriding goal of the detection and analysis phase is to inform the organization of the impact of an event, and whether it rises to the level of an incident.

INCIDENTS SEVERITIES

Severity I (High)

Severity I incidents are incidents that could result in damage to Northern Oklahoma College's reputation or brand equity, involve breach of employee data, raise regulatory or contractual compliance issues, impede Northern Oklahoma College's ability to conduct college business, or otherwise risk significant financial impact. Such incidents likely affect the entire institution. Examples of such incidents are a breach of credit card or other private data of multiple users, disablement of online services, or public disclosure of private employee or student information.

Severity II (Moderate)

Severity II incidents are incidents involving breach of sensitive information that are not likely to create a significant regulatory or contractual compliance issue and do not involve disclosure of data or private employee or student data. Additionally, impact to functionality of an isolated system is also classified as Severity II incident. The scope of such incidents is typically limited to a single department and does not significantly impact institution services. Examples of such incidents are disclosure of non-public data, disablement of a Point of Sale system at a single campus location, or a localized virus infection.

Severity III (Low)

Severity III incidents are isolated incidents that do not affect college business or sensitive information. Examples of such incidents are employee loss of college issued mobile devices that did not contain sensitive information, a suspected breach of sensitive information of a very limited number of employees or students that has been proven to be a non-systemic issue, or a phishing attack against an employee or student. Severity III incidents could be escalated to Severity I or II based on the results of preliminary investigation.

4.3 COMMUNICATION

All Information concerning an incident is to be considered confidential, and at no time should any information be discussed with anyone outside of the CSIRT unless approved by the college president and legal counsel.

Public or media statements must be carefully managed to ensure that any investigation/legal proceedings are not jeopardized, and reputational damage is minimized. Decisions concerning the disclosure and method of disclosure of incident information will only be made by the Vice President for Development/Community Relations or their designee.

Inquiries from media agencies must be directed to the Vice President for Development/Community Relations or their designee. Employees found to be discussing incidents without approval from the CSIRT or college president will be subject to disciplinary action, up to and including termination.

Updated communications will come from the Incident Response Manager. Any requests for information should be passed onto the Incident Response Manager. Communication with news media will be initiated by the Vice President for Development/Community Relations or their designee. Incoming news media calls and requests for information will be directed to the Vice President for Development/Community Relations or their designee.

4.4 CONTAINMENT

Containment refers to the effort to minimize any damage or expanded risk presented by the incident. Containment is an attempt to halt the spread of an incidents scope beyond the known affect. There may be technical containment mechanisms, policy containment mechanisms, procedural containment mechanisms or a

combination of these. As soon as the CSIRT has analyzed the situation they determine what needs to be done to contain the incident so no further harm is done. Third-party resources may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody.

The following describes the protocol for all compromised systems during a cybersecurity incident. They must be followed until CSIRT determines it's no longer necessary:

- Do not access or alter compromised systems
- Do not log on to the machine
- Do not log in as ROOT (type of Administration login for Unix and Linux systems), Administrator, or any other privileged account
- Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug network cable)
- Preserve logs and electronic evidence
- Log all actions taken
- Monitor all affected systems and alert on suspicious behavior
- If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised)
- Disable user accounts or change passwords

4.5 ERADICATION

Eradication is the effort to eliminate the risks posed by the cybersecurity incident. This phase is focused on correcting the errors or threats that are responsible for the incident. The CSIRT identifies the steps required to resolve the incident and tracks them until complete. Once the incident has been contained, eradication and recovery must be carefully executed. Failing to clean all affected systems prior to returning to college operations may allow the attacker to return to their initial state of compromise and initiate another incident.

4.6 RECOVERY

Once the incident has been contained and the cause eradicated, CSIRT identifies and tracks recovery of any systems affected or college processes that need to be modified to prevent it from occurring again. The CSIRT, in conjunction with the institution's Executive Council, will define the recovery goals and timelines. The Executive Council will assess the recovery results and validate a return to normal college business. The CSIRT is responsible for closing the incident and notifying identified key personnel.

RECOVERY STEPS MAY INCLUDE:

- Restoring systems from a clean backup
- Replacing corrupted data from a clean backup
- Restoring network connections and access rules
- Communicating with interested parties about changes related to increased security
- Increasing network and system monitoring activities (short or long-term)
- Increasing internal communication/reporting related to monitoring
- Engaging a third party for support in detecting or preventing future attacks

4.7 Post Incident Activities

Post incident activities refers to the efforts to gather the institutional knowledge gained during the incident and incorporate them into the collective policies, practices and procedures to ensure incident avoidance in the future. Efforts are taken to reflect on the issues and events that led to the incident, shortcomings in the college's response, and areas of improvement. Information security, in conjunction with the Executive Council and identified key personnel, will develop a strategy to mitigate any risks identified in the post-incident assessment. This strategy could include technology acquisition, procedural changes, or risk acceptance.

5 Notification Information

- PCI DSS
  Any security incident involving a breach of cardholder data should adhere to all notification and response requirements of the Payment Card Industry (PCI) Security Standards Council.
  https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

  Merchants and service providers that have experienced a suspected or confirmed security breach should take immediate action to help prevent additional damage and adhere to:
  Visa CISP requirements
  MasterCard Account Data Compromise User Guide
  Questions on Security or PCI Compliance: AskDataSecurity@discover.com
  American Express Data Security Operating Policy

- HIPAA
  Reference: http://www.hhs.gov/hipaa/for-professionals/breach-notification/
  The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

- FERPA
  Reference: https://studentprivacy.ed.gov/guidance
  Educational organizations have a legal and ethical responsibility to protect the privacy and security of education data, including personally identifiable information.
  https://studentprivacy.ed.gov/resources/data-breach-response-checklist

- State of Oklahoma
  https://cybersecurity.ok.gov/