**Effective:** *08/08/2022*
**Last Revised:** *08/08/2022*

**Responsible University Administrator:**
*Assistant Vice President, IT Security Services*

**Responsible University Office:**
*Information Technology Services*

**Policy Contact:**
*IT Security Services*
*security@nebraska.edu*

# ITS-07: Incident Response Standard

## Standard Contents

## 1. Purpose

The purpose of the Incident Response Standard is to define the organization's requirements for enforcing incident response and handling capabilities. This standard serves as a statement of objectives for the protection of information assets against security incidents.

## 2. Scope

This Standard shall apply to all University of Nebraska System ("University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of the University and to which this Standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this Standard.

## 3. Standard Statement

It is the intention of this Standard to establish incident response capabilities throughout the University to help the organization implement security best practices regarding identification, reporting, and handling of information security incidents. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (CISO) as defined in **ITS Policy Exception Standard**. The following subsections outline the Incident Response Standard.

## 4. Incident Response Requirements

### 4.1 Plan Incident Response

#### 4.1.1 Incident Response Plan Requirements

The University must maintain a documented Incident Response Plan to provide a well-defined and organized approach for handling any potential threat to systems and informational assets. The Incident Response Plan must ensure that appropriate leadership from organization entities (business owners, system owners, HR, physical security, legal, operations, procurement, risk executives, and others) and technical resources are established to coordinate incident response activities. Incident response activities that include Preparation, Identification (detection and analysis), Containment, Eradication, Recovery, and Lessons learned (post-incident activity) (PICERL). The incident response plan shall be reviewed and updated on an annual basis, as changes arise in the environment, and/or as lessons are learned from real-world incidents and training exercises.

#### 4.1.2 Incident Response Plan Requirements

The Incident Response Plan must establish, maintain, and follow documented incident management procedures to ensure rapid, effective, and consistent response to security incidents. The plan must include relevant topics including:

- Incident response planning and preparation
- Monitoring, detecting, analyzing, and reporting of information security events and incidents
- Establish an incident tracking system and the necessary reporting and contact forms
- Logging incident management activities with an established place and way to store these (encrypted)
- Handling of forensic evidence; Establish a place and way to store evidence (encrypted)
- Maintain a prioritization and severity rating for various events and incident types. Establish performance measures (SLA) for each
- Maintain pre-defined incident response actions for events and incidents; Review at least annually but this should be a living document that is updated regularly
- Maintain an internal contact roster or phone tree
- Establish and maintain an incident communications plan for use during an incident
- Establish hardware and software requirements for analyzing incidents and review annually
- Remediation runbooks of common security incident types
- Post-mortem and root cause analysis of the incident
- Maintain a roles and responsibilities matrix, including the definition of a designated Information Security Incident Response Team (CIRT) led by the Chief Information Security Officer
- Training requirements and frequency for each role. This should include any training for average users to identify suspicious behaviors and anomalous events
- Maintain a list of external authorities (local law enforcement, FBI, special interest groups, or forums that handle the issues related to information security incidents) who can assist in an incident and when contacting / notifying these authorities is appropriate.

## 4.2 Detect and Report Events

#### 4.2.1 Event Detection

An event is any observable occurrence on the network. Events can be detected in several ways such as loss of productivity, alarms & alerts from systems, notifications from other organizations, or results from various assessments. All security events must be investigated to determine if they are a security incident using the incident triage and response processes. This includes automated alerts and employee reported suspicious or anomalous events.

#### 4.2.2 Event Reporting

Employees and contractors detecting any anomalous or suspicious events are required to immediately report those events to the Help Center or a manager. Confirmed suspicious events must be reported to the Information Security team or the CISO. Individuals reporting a suspected security event should be provided feedback on its resolution whenever possible.

#### 4.2.3 Analyze and Triage Events

Establish a plan to analyze, triage, and prioritize (rate) events. This plan should contain a priority and rating scheme to support a quick resolution to events and if necessary, declare an incident. Once triage determines the priority of an event, the appropriate pre-planned response should be taken. Low priority or low impact events should result in closure of the event and no actions taken. High priority events should result in declaring an incident and the appropriate incident response plan activated.

## 4.3 Develop and Implement Responses to Incidents

#### 4.3.1 Develop Responses to Incidents

Pre-approved response actions and procedures that the incident responders can take without having to seek approval will improve incident response times. Pre-approved response actions and procedures to various incidents will be developed and made part of the incident response plan. New responses and procedures will be added/updated at least annually as new types of incidents become known and technologies change.

### 4.3.2 Track, Document, and Report Incidents

Documenting incidents creates the information necessary for evaluating incidents in detail, conducting forensics, evaluating trends, and updating incident response plans. Proper planning for secure communication, documentation transmission, and document storage is essential. A secure out-of-band communications plan and secure out-of-band central document repository will be established and maintained in a ready to use state in case an incident occurs. Tracking and documenting system security incidents includes maintaining records of each incident, documenting actions taken, and incident status.

Incident information can be obtained from a variety of sources including incident reports, IR teams, log monitoring, network monitoring, physical access monitoring, and user/administrator reports. This relevant information should be communicated and stored securely in a central repository for later examination and review.

Formal incident reporting requirements must be pre-defined for both internal (such as execs., affected business units, and other stake holders) and external (such as law enforcement, EO, directives, regulations, and policies) requirements. This should include the types of security incidents, who it should be reported to, level of content, and timelines for reporting.

## 4.4 Post Incident Review

### 4.4.1 Incident Root Cause Analysis

A post-incident review using root-cause analysis will be conducted within ten (10) working days following the closure of a security incident. This will include a formal examination of the causes of the incident and the responses to it. This examination will evaluate administrative, technical, and physical control weaknesses that may have allowed the incident to occur. Consideration of other processes that may have contributed should also be given (such as change management and configuration management).

After completion of the post incident analysis, the CIRT must develop an action plan that will reduce the likelihood of the incident's reoccurrence and improve organizational response capabilities. Actions to be taken may include:

- Updating response and recovery plans, policies, processes, and/or procedures
- Updating 3rd party tools
- New or modified technical controls or configurations
- Employee training and awareness topics

## 4.5 Incident Response Training

### 4.5.1 Incident Response Testing Requirements

Incident response exercises test incident response capabilities and help determine the effectiveness of incident response plans and help identify potential weaknesses or deficiencies. Incident response exercises should:

- Follow the appropriate incident response plan and any associated run books
- Address what happens during an incident
- Exercise as many roles and responsibilities as possible
- Include a debrief and feedback session
- End with updating the IR plans and procedures

Incident Response testing exercises will be performed at least annually to validate organizational preparedness to carry out the Incident Response Plan. Testing exercises should include representatives from as many stakeholder groups as possible, including senior management, legal, public affairs, and IT. Exercises can tabletop exercises or technical exercises of various incident response techniques. Participation can be company internal or externally hosted exercises such as an industry sponsored exercise. Exercise scenarios should be derived from real-world attack scenarios and lessons learned from exercises should result in updates to the incident response plan and procedures.

## 5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

## 6. Compliance

**Compliance Measurement**
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

**Exceptions**
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

**Non-Compliance**
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

## 7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

## 8. Approvals and Revision History

Approval of this Standard:

| | Name | Title | Date |
|---|---|---|---|
| Authored by: | Richard Haugerud | IT CISO | 08/08/2022 |
| Approved by: | Bret Blackman | IT CIO | 08/08/2022 |

Revision history of this Standard:

| Version | Date | Description |
|---|---|---|
| 1.0 | 08/08/2022 | Initial Standard Published |
| | | |