**Name of Organization**

**Incident Response Standard**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Response Standard is designated For Official Use Only (FOUO) and is the property of (Name of Organization), only (Name of Organization) representatives may distribute the handbook to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. The document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc88583205)

[II. Scope 5](#_Toc88583206)

[III. Requirements 6](#_Toc88583207)

# Introduction and Purpose

Information Security Incident Response is a vital component of adequate cyber risk management. Recognizing that effective incident response is a complex undertaking whose success depends on planning and resources, this Incident Response Standard (“the Standard”) establishes the minimum requirements for an Organization’s Information Security Incident Response Program and the Information Security Incident Response Plan (“the Plan”).

The primary focus of this Standard is to provide assistance to locations/offices and organizational units as they develop their Incident Response Plans. The secondary goal of this Standard is to guide organizations in developing their overall Information Security Incident Response Program.

The incident response process outlined in this Standard encompasses four phases: Preparation; Detection and Event Analysis; Containment, Eradication and Recovery; and Post-Incident Activity. The dynamic relationship between those phases is defined in NIST SP 800-61 (Computer Security Incident Handling Guide). This Standard aligns with the NIST Cyber Security Framework.

Organizations, locations/offices and organizational units may extend their plans beyond this Standard to meet requirements for specific use cases, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI), state specific Data Privacy laws, the European Union General Data Protection Regulation (GDPR), specific contracts and certain grants.

# Scope

All information security incidents are to be handled according to this Standard and in a manner consistent with applicable laws and regulations. This Standard applies to any information security incident or policy violation involving IT resources at (Name of Organization), whether initiated from internal or external, and are either malicious or accidental. It applies to all (Name of Organization) IT resources, whether centrally or locally administered; to all users; auxiliary organizations; third parties; visitors; anyone else with access to (Name of Organization) information assets; and to personally-owned computers with access to (Name of Organization) networks and data. While mainly intended to address violations of (Name of Organization) ‘s Information Security Program and Responsible Use Policy, this Standard applies to any information security-related incident involving (Name of Organization).

# Requirements

Any (Name of Organization) person discovering an event or incident are required to follow the incident handling process below:

**Notification**

* Anyone who discovers an event should report it to the IT Service Desk and/or Human Resources immediately and await further instructions before continuing to use the computing device or media. The Incident Handling Team (IHT) will subsequently be notified.
  + Anyone who becomes aware of the loss or theft of an (Name of Organization) computing device or media should report the loss or theft to (Name of Organization), IT Service Desk or Human Resources department immediately. The Incident Handling Team (IHT) will subsequently be notified.
* IT support personnel should follow the internally published procedures provided by the IHT to determine if the event could be a security incident.
* If anyone suspects that an incident has occurred, they should:
  + Notify the (Name of Organization) IHT upon discovery.
  + In the event of the loss or theft of a computing device or media that contains (Name of Organization) information, report the loss to the IT Service Desk immediately, who will contact the IHT.
  + The IHT will work with the Cybersecurity Incident Response Team (CIRT) on containment and forensics imaging (memory and disk, where necessary), following internally published procedures.
* The IHT may initiate an investigation if it becomes aware of an incident independently without being notified through the incident handling process.
  + The IHT will notify CIRT as appropriate.
* If necessary, the IHT via the Incident Commander will invoke the Critical Incident Management Process/Emergency – aligned with DHS/FEMA requirements.

**Incident Assessment**

1. The Chief Information Officer and Incident Commander or their designee, will consider the following in determining the severity and appropriate response to an incident:

* How widespread is the incident?
* What is the impact to college operations?
* What data is at risk?
* How difficult is it to contain the incident?
* How fast is the incident propagating?
* What is the estimated financial impact to the organization?
* How will this incident affect the organization’s image?
* Is law enforcement involvement needed or required?

1. Appropriate measures will be initiated by CIRT via the IHT to prevent additional loss or harm to information resources.
2. The Incident Commander will determine the nature, scope, and cause of the incident, and identify required corrective actions.
3. Incidents will be classified as:
   1. Critical
   2. Serious
   3. Important
   4. Informational

**Critical Incidents**

* Critical incidents are defined as having a serious potential impact on organizational information resources. Managers or users of resources involved will be explicitly instructed not to use the resources until receiving further instruction from the IHT
* Critical incidents must be responded to within one hour of notification or observation. The Incident Commander will direct restoration efforts. Communication will flow from the Chief Information Officer or Incident Commander, or their designee(s), to keep the appropriate organizational personnel apprised of the status of restoration efforts. Critical incidents are characterized as follows:
  + The incident is one that has a high impact on the confidentiality, integrity or availability of information and will increase in scope and impact if the incident is not mitigated.
  + The incident, because of the immediacy of its effect on critical business functions or information, requires a resolution (for example: a change) on an immediate-response basis.

**Serious Incidents**

* Serious severity incidents are identified as having non-intrusive impacts on current services and represent passive attacks or monitoring of critical communication.
* Serious incidents will be responded to within 24 hours of notification or observation. The IHT using CIRT personnel will direct restoration efforts. Communication will flow from the IHT, or their designee(s), to keep the appropriate organizational personnel apprised of the status of restoration efforts. Serious incidents are characterized as follows:
  + The incident or can materially affect business operations, causing a substantial impact.
  + The effect of the incident is such that it does not require immediate resolution, but it does require a resolution to be executed on a date and time in the near future (e.g., patching during next emergency patch window).

**Important Incidents**

* Important level incidents are identified as those that do not present an immediate threat to multiple hardware or software systems and do not involve sensitive, restricted, or critical data.
* Due to the relatively minor nature of Important incidents, appropriate response times and communications will be determined after initial investigation and based on priorities at the time. Important incidents are characterized as follows:
  + The incident does not materially affect business operations and does not cause a substantial impact on confidentiality, integrity, or availability of information. The incident does have the potential to do so if not resolved expeditiously.
  + The effect of the incident is such that it does not require an immediate resolution, but it does require that a resolution (for example: a configuration change) executed on an agreed date by asset and business operations owner (e.g., payroll server is to be configured after payroll has been done and back up completed).

**Informational Incidents**

* Information level incidents are identified as those that present limited threat to single hardware or software systems and do not involve sensitive, restricted, or critical data.
* Informational incidents are characterized as follows:
  + The incident does not have an adverse impact on confidentiality, integrity or availability because of either the nature of the fault or the small extent of the fault and the fact that the incident will not increase in impact over time.
  + The effect of the incident is such that it does not require immediate resolution. A resolution (for example: a patching) may be required that can be planned for a date and time during normal maintenance or patching window.

**Investigation**

* The IHT should initiate an investigation.
* The investigation will determine if there is risk of harm (e.g., Private Information or credentials have been acquired by an unauthorized party), and then determine further steps.
* All parties connected with the incident should cooperate with and assist the IHT with the investigation according to procedures for incident handling.
  + The IHT may investigate, in compliance with the Privacy Policy and Incident Response Plan.
  + The IHT will communicate appropriately with affected parties.

**Containment**

* If CIRT determine an incident could spread to additional systems (e.g., involves credentials with administrative access to multiple computing devices, the threat is determined to be a worm, etc.), then personnel should assist in containment, including, but not limited to, providing forensic images (memory and disk) and baseline information as deemed necessary by the IHT.

**Eradication and Recovery**

* After providing requested information to the IHT, CIRT should attempt to remove the threat from (clean) the affected system or re-image the affected system and restore the system to service.
* If eradication is unsuccessful, or the incident recurs after re-imaging, CIRT personnel should notify the IHT and await further instructions.

**Resolution/Closure**

* The IHT will communicate resolution and lessons learned to management, personnel, and/or end users, as appropriate.