Incident Response Policy Template

# PURPOSE AND OBJECTIVE

The purpose of this policy is to define (insert organization name) Incident Response Program. Its goal is to establish a framework for the organization to respond quickly, decisively, and appropriately to limit the impact of an adverse event on clients and information resources. The policy is also intended to facilitate timely correction of any damage caused by an incident and provide for effective investigation and follow-up actions.

The National Institute of Standards and Technology defines cybersecurity as “the process of protecting information by preventing, detecting and responding to attacks.” This policy covers cybersecurity and all technology related incidents.

This Incident Response Program is supported by procedures and practices that include the following:

* Assessing the nature and scope of an incident, and identifying what business, sensitive and confidential data the organization manages;
* Notifying any regulators or funders (where required and as advised by counsel) as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive client information;
* Notifying appropriate law enforcement authorities;
* Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of client information, while preserving records and other evidence; and
* Notifying clients when warranted.

# BACKGROUND

Security incidents have the potential to occur in an unpredictable manner and may impact the organization’s physical, electronic, and human resources. Such incidents may adversely affect the confidentiality, availability, and integrity of the assets and information belonging to the organization and its clients. To the greatest extent possible, (insert organization name) strives to minimize the potential for security incidents to occur. However, the organization also recognizes that, even with its existing controls and practices, security incidents of varying severity may materialize. Accordingly, the organization has adopted this policy and supporting procedures to define the steps that will be taken in response to an incident. These steps are defined for the purpose of ensuring that rapid and appropriate actions will be taken to minimize any harm to the assets and information of the organization and its clients.

# SCOPE

# This policy applies to physical and electronic information systems operated by (insert organization name). The policy also addresses any information systems that are operated by third party service providers or agents on the organization's behalf (i.e. donor management systems, case management systems, volunteer management systems). All organization employees, including temporary employees, part-time employees, and contractors are covered by this policy.

# POLICY

## General Requirements

This policy establishes the following general requirements:

* + An (insert organization name) Incident Response Team (IRT) will be implemented. By approving this policy, the board grants the IRT authority to act and make decisions as necessary to appropriately respond to an incident.
	+ (Insert organization name) IRT members have defined roles and responsibilities, which are outlined in the Incident Response Procedures. These responsibilities will take priority over normal duties in the event of a security incident.
	+ An event classification system, which defines incidents by their level of severity, will be used to manage the incident response process and provide guidance for escalation.
	+ Whenever a security incident of a physical or electronic nature is suspected or confirmed, all parties covered by this policy are expected to follow appropriate procedures and instructions given by the IRT.

## Incident Identification and Definition

The term “incident” is defined as any irregular or adverse event that occurs to any client record or personally identifiable information, or that involves the availability and integrity of the organization's systems or network. It is noted that incidents can be of a physical or electronic nature. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, any kind of damage to a system, or the intentional or unintentional compromise of client records or information. Some possible scenarios for security incidents include:

* Attempts (either failed or successful) to gain unauthorized access to a system or its data.
* Unwanted disruption or denial of service.
* The unauthorized use of a system for the processing or storage of data.
* Destructive malware – used to compromise data or render systems inoperable
* Criminals obtaining large volumes of credentials (usernames, passwords, e-mail addresses) and other forms of identification used by customers, employees and third parties to authenticate to systems.
* Changes to system hardware, firmware, or software characteristics without the management’s knowledge, instruction, or consent.
* Internet fraud or phishing.
* Suspected impropriety by service provider/vendor.
* Suspected pre-text phone calling or social engineering.
* Unintentional loss of credentials, equipment, tapes, USB devices.

## Incident Response Team

By approving this policy, the Board of Directors has authorized an Incident Response Team to take appropriate actions as outlined in this document and the Incident Response Procedures. Members of the

IRT include:

**IRT Members:**

**Define who should be on the IRT for your organization. Include an IRT team captain. Consider representatives from the following:**

* **Team leader—coordinates all incident response team activities.**
* **Communications—manages communications across the organization and with third parties. Should be trained in or supported by public relations.**
* **Lead Investigator—gathers and analyzes technical evidence, determines the cause of the attack, and directs other analysts and IT components to implement system and service recovery.**
* **Analysts/Researchers—support the investigator providing the threat intelligence and context for an incident. Cyber forensic analysts may be necessary to perform deep autopsies on compromised systems.**
* **Legal representation—it is essential to have HR and legal guidance to address any negotiations or potential criminal charges derived from the incident.**

## Incident Identification, Classification, and Escalation

Once a suspected incident has been detected, it is the responsibility of the respective individual to report it, as outlined in this policy. The nature and severity of the incident will determine the appropriate response strategy. Severity levels are as follows:

**High** – A high level event is an event that can cause significant damage, corruption, or loss (compromise) of confidential, critical and/or strategic organization and client information. The event can result in potential damage and liability to the organization and to its public image. Examples of high level events include computer intrusions, compromise of critical information, widespread virus infection, attacks against the IT infrastructure (e.g., domain name servers, firewalls and backup systems), and denial-of-service attacks that disable a critical service or impede business performance.

**Medium** – A medium level event is an event that may cause damage, corruption, or loss of replaceable information without compromise or may have a moderate impact on the organization's operations or reputation. Examples of medium level events include misuse or abuse of authorized access, accidental intrusion, confined virus infection, unusual system performance or behavior, system crashes, installation of unauthorized software, unexplained access privilege changes, or unusual after- hour activities.

**Low** - A low level event is an event that causes inconvenience, aggravation, and/or minor costs associated with recovery, unintentional actions at the user or administrator level, or unintentional damage or minor loss of recoverable information. The event will have little, if any, material impact on the organization’s operations or reputation. Examples of low level events include sharing of passwords, and policy or procedural violations.

## Incident Reporting

All (insert organization name) colleagues and contractors are responsible for helping to ensure the security of the information systems that they use and operate. Part of this responsibility is the duty to report any confirmed or suspected security problem in a timely manner. **Define how people should report issues and who they report them to. (Sample wording: Staff must report actual or suspected data breaches to the IRT within one hour of discovery. The report should include the following information:**

**• Time of discovery;**

**• Date and time (or best estimate) that Breach occurred;**

**• Nature of Breach or Suspected Incident (e.g., network Hacked, thumb drive or laptop stolen, email Hacked, hardcopy document containing PII taken);**

**• Description of PII or Company- or Business-Identifiable Information Breached; and**

**• Office responsible for data, if clear.)**

## Incident Response and Escalation

Detection and identification of a suspected incident represents the first step of the incident response process. The response process is characterized by four phases:

* Identification - The incident is recognized, reported, and confirmed.
* Assessment - The incident is evaluated and an initial severity rating is assigned.
* Response - An appropriate strategy is executed and revised as needed.
* Follow-up - Damage is corrected, vulnerabilities are identified and remedied, summary reports are prepared.

The decision to escalate the process between phases is made by the IRT team based on the evolving circumstances of the incident.

## Internal and External Communication

To ensure that information is disseminated consistently and expediently, specific responsibilities for communications inside and outside the organization are outlined below. I

* **Decide who is responsible for notifying the organization president and the members of the IRT and initiating the appropriate incident management action including steps outlined in the Incident Response Procedures.**
* **Decide who is responsible for reporting the incident to appropriate local, state, or federal law officials as required by applicable regulations.**
* **Decide who is responsible for coordinating communications or directing communication**

**with outside organizations (e.g., insurance companies, law enforcement, vendors).**

* **Consider listing every organization that should be contacted.**
* **Decide who is responsible for coordinating communications within the organization.**

## Decide who is responsible for communication with the media and the public.

**Collection/Protection of Information and Reporting**

**Decide who is responsible for determining what evidence should be gathered as part of the incident investigation.** The organization must take precautions to ensure that evidence is accounted for at all times and the passage (chain of custody) of evidence is fully documented. The organization must make sure that the evidence is preserved.  Depending on the nature of the incident, a suspicious activity report may need to be filed with law enforcement.

## Lessons Learned/Post Mortem

The IRT Team Captain is responsible for initiating, completing, and documenting the incident investigation with assistance from the IRT. A report must be prepared which includes the following information:

* The type of incident – this may include denial of service attacks, vandalism, unauthorized access, disclosure or theft of information, etc.
* The response strategy - including all actions that were taken by all parties to manage the incident.
* How the incident occurred - including weaknesses in process, procedures and vulnerabilities in computer systems and physical controls.
* Recommendations for preventing such incidents arising in the future.

## Involvement of Third Party Service Providers

Depending on the nature of the incident and the information systems, assets, and facilities affected, the involvement of third party service providers may be necessary. (Insert organization name) has identified potential legal and forensic vendors to assist with high risk incidents as follows: **Insert potential vendors in table below.**

|  |
| --- |
| **Insurance** |
|  |
| **Legal** |
|  |
| **Data Breach response services** | **Available services** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## RESPONSIBILITY - Decide who is responsible for what. Items that you might mention:

Responsibility for administering the information security functions within the organization and for coordinating the response process.

Responsible for all decisions to halt and/or re-enable a computer/system or network service.

Responsibility for implementing and updating this policy.

Responsibilities of the IRT (Sample wording: The IRT is a team of highly skilled personnel, designated by the organization's Board, who are responsible for responding to computer security incidents. Members will be on call twenty-four hours a day, and be capable of responding within a nominal amount of time. There will be backups available when members are out of town or on vacation. A list of team members and contact information is documented in the Incident Response Procedures.)

Responsibilities of employees and users (Sample wording: All employees and other users are responsible for protecting information to which they have access from unauthorized activities. Employees and other users are responsible for reporting any suspected security incidents, abuses, and violations of policy. All employees and other users are responsible for familiarizing themselves with the organization’s Incident Response Procedures and their role in the response process.)

Responsibilities of the Board of Directors (Sample wording: The Board is responsible for reviewing and approving this policy. The Board is also responsible for the appointment of the IRT. The Board is responsible for governing cybersecurity, reviewing incident reports and evaluating the organization’s leadership with respect to cybersecurity.)