



SECURITY INCIDENT RESPONSE AND REPORT PLAN

CONFIDENTIAL

A security incident response plan is used to support the organized response to security incidents. It documents the roles and responsibilities and the steps that will be taken to identify, contain, eradicate, and recover from security incidents.

The steps include preparation, identification, containment, eradication, recovery, and lessons learned.

Organizations must have a formal, focused and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing incident response capability. Every organization needs a plan that meets its unique requirements, which relate to the organization's mission, size, structure, and functions. The plan must establish the necessary resources and administrative support.

Table of Contents

Purpose and Scope 4

 Purpose 4

 Scope 4

Responsibilities 5

Definitions 6

Roles and Responsibilities 6

 Internal Contacts 6

 Contactos Externos..... 8

 Organizaciones relacionadas 9

Team organizational chart 10

Incident type..... 10

Gravity Matrix..... 11

Incident Management Process..... 13

Approvals 18

 Responsible Resources 18

References..... 19

REVISIONS

Contact:	Title:	Date:	Comments:
Janet Rios Colon	Chief Executive Officer	May 2018	
Janet Rios Colon	Chief Executive Officer	Nov 2018	
Janet Rios Colon	Chief Executive Officer	April 2020	

Jose Miranda	ISSO	June 2021
Jose A. Miranda	ISSO	June 2022
Jose A. Miranda	ISSO	Jan 2023
Jose A. Miranda	ISSO	Jan 2024

This Security Incident Response Plan must be reviewed at least once a year, as established in the SECUREHIT policies.

Purpose and Scope

Purpose

This Security Incident Response Plan exists to ensure that the Secure Health Information Technology Corp. (SecureHIT) is prepared to handle cyber incidents effectively and efficiently. Security incidents are more frequent and sophisticated than ever. No organization worldwide is immune to attacks. Organizations must ensure that they are prepared to respond to incidents, as well as to prevent and detect them. By having a plan, a team, and conducting exercises, organizations will be better prepared for unavoidable incidents and will be able to contain the damage and mitigate additional risk to the organization. Resources must be deployed in an organized manner with skills exercised and communication strategies.

This document describes the general plan for responding to security incidents at SECUREHIT. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to prepare, identify, contain, eradicate, recover, and carry out lessons learned in order to minimize the impact of security incidents.

The goal of the Security Incident Response Plan is to ensure that organizations are organized to respond to security incidents effectively and efficiently.

Scope

This security incident response plan applies to all networks, systems, and data, as well as organization members, employees, and contractors, as well as vendors who access the networks, systems, and data. Members of the organization who may be called upon to lead or participate as part of the Security Incident Response Team should be familiar with this plan and be prepared to collaborate with the goal of minimizing adverse impact on the organization.

This document helps the organization establish incident response and/or incident management capabilities to determine the appropriate response to common security incidents that will arise. This document is not intended to provide a detailed list of all activities that must be performed to combat security incidents.

Responsibilities

Responsibility for the security of protected health information rests with the Executive Director of SecureHIT, Janet Ríos. During times when a high or critical security incident occurs, this responsibility is entrusted to the SecureHIT ISSO.

All members of the workforce will be responsible for:

Security Incident Response and Report Plan



- Prevent potential security incidents
- Identify any potential safety incident
- Report any security incident to the Information System Security Officer
- Assist the Information System Security Officer in dealing with the incident and
- mitigate its damaging damages, if possible

The Information System Officer, under the delegated authority of the Chief Executive Officer, will be responsible for:

- Maintain and update all policies and procedures related to security incidents
- Classify all incidents as serious or not serious as established in this policy
- Maintain and update procedures to respond to security incidents
- Document all reported incidents and their resolution

The Information Systems Security Officer, under the supervision of the Director of Information Systems, will be responsible for:

- Implement and maintain the controls and safeguards established in this policy.
- Maintain the necessary procedures to support this policy.
- Ensure and support compliance by the workforce.

All members of the workforce, contractors, volunteers, and/or students will be responsible for complying with the requirements of this policy.

Definitions

Event observable incident in a system or network. Events include, for example, a user connecting to a file share (share folder), a server receiving a request for a web page, or a user sending an email.

Incident an adverse event in an information system and/or network, or the threat of such an event occurring. An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It implies harm or intent to harm.

Roles and Responsibilities

Internal Contacts

SecureHIT Key Personnel

Security Incident Response and Report Plan



SecureHIT Key Personnel		
Key Personnel	Contact Information	
Incident Director	Work	787-231-7031
<i>Janet Ríos Colón, CIO</i>	Home	
<i>PO Box 1666 Sabana Seca PR 00952</i>	Cellular	787-562-7036
<i>Insert City, State, and Zip Code</i>	Email	jrios@securehitpr.com
Incident Director – Alternate	Work	787-231-7031
José A. Miranda Báez, ISSO	Home	jmiranda@securehitpr.com
	Cellular	787-553-3354
	Email	jmiranda@securehitpr.com
Incident Coordinator	Work	787-231-7031
Maria J. Díaz, Customer Service Officer	Home	
	Cellular	787-392-5799
	Email	mdiaz@securehitpr.com
Incident Coordinator – Alternate	Work	787-231-7031

Security Incident Response and Report Plan



SecureHIT Key Personnel		
Samuel Rivera, ISO	Home	
	Cellular	787-234-4330
	Email	srivera@securehitpr.com
Incident Team – Team Lead	Work	787-231-7031
José A. Miranda Báez, ISSO	Home	
	Cellular	787-553-3354
	Email	jmiranda@securehitpr.com
Incident Team – Team Members	Work	787-231-7031
José A. Miranda, ISSO	Cellular	787-553-3354
Samuel Rivera, ISO	Cellular	787-234-4330
	Email	support@securehitpr.com

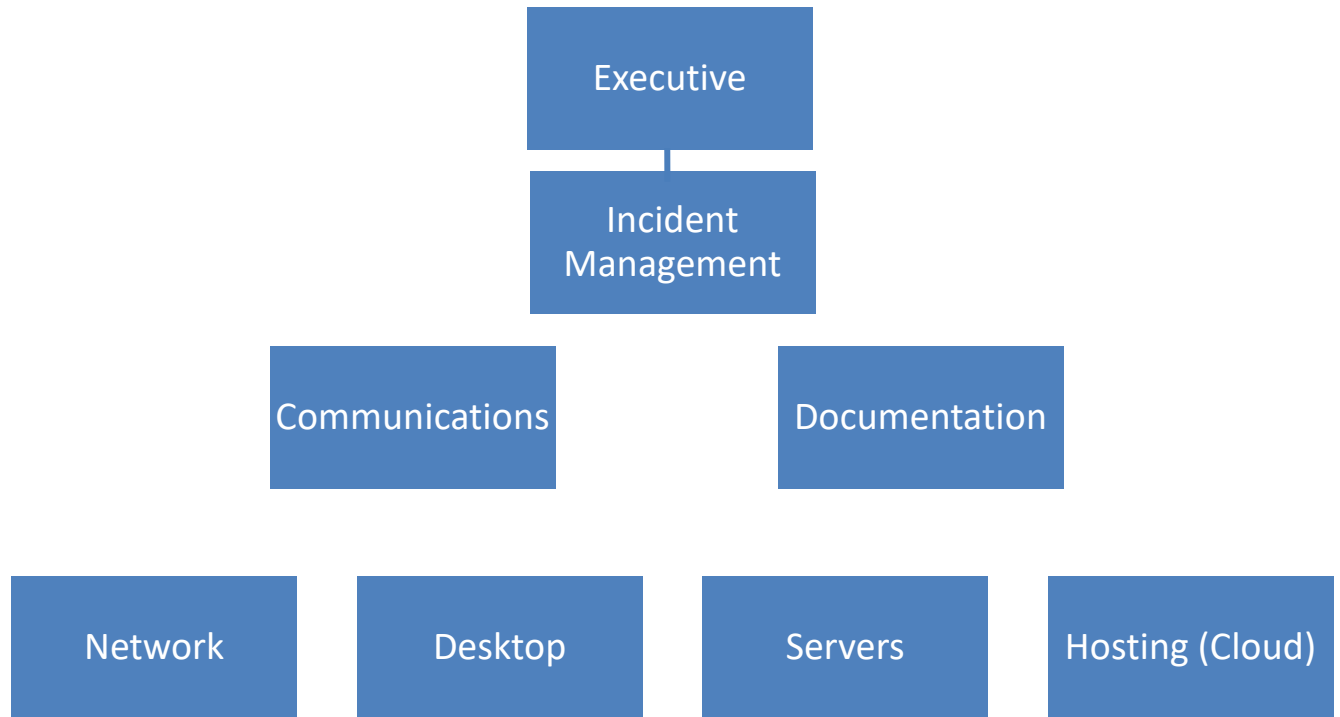
Contactos Externos

Role	Organización	Nombre	Teléfono	Email or URL
Autoridades (local)	Policía de Puerto Rico	Asesor legal de crímenes cibernéticos	787 793-1234	
Autoridades (local)	Departamento de Justicia de Puerto Rico	Unidad investigativa de crímenes cibernéticos.	787 721-2900	http://internetseguro.pr.gov/vicc@justicia.pr.gov
Autoridades (federal)	FBI	Puerto Rico	787 766-5656	
Autoridades (federal)	Health and Human Service Department	Secretario de Salud Federal		https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

Organizaciones relacionadas

Role	Organización	Nombre	Título	Teléfono	Email
Customers/ Clients					
Shareholders					
Board of Directors	Junta de Directores SECUREHIT	Janet Ríos Colón	President	787-562-7036	jrios@securehitpr.com

Team organizational chart



Incident type

Type	Description
Unauthorized access or use	Physical or logical access to the network, System or data without permission
Interruption of service or denial of service	Attack that prevents access to the service or impairs normal operation
Malicious code	Installation of malicious software (eg virus, worm, Trojan, or other code)
Network Failure (widespread) failures	An incident affecting the confidentiality or integrity or availability of networks
Application Systems Failures	An incident that affects the confidentiality, integrity or availability of applications or systems.
Unauthorized disclosure or loss	An incident that affects the confidentiality, integrity or availability of data.
Privacy violation	Incident involving actual or suspected loss of personal information
Information Security/Data Loss	Incident involving actual or suspected loss of confidential information
Others	Any other incident that affects networks, systems or data.

Gravity Matrix

The Incident Response Team will determine the severity of the incident taking into account whether a single system is affected or multiple, the criticality of the affected systems, if it affects a single person or several, if it affects a single team or several, or impacting the entire organization. The Incident Response Team will consider whether it is a single or multiple operational area and the impact of the incident. The Incident Manager must consider the relevant operational context and what else is going on with the business at the time to fully understand the impacts and urgency of remediation. The Incident Response Team will consider available information to determine the known magnitude of the impact compared to the estimated size along with the probability and speed of spread. The Incident Response Team will determine the potential impacts to the organization, whether it be economic damage or damage to name and reputation or other damage. The incident may be the result of a sophisticated or unsophisticated threat, a manual or automated attack, or it may be a nuisance/vandalism.

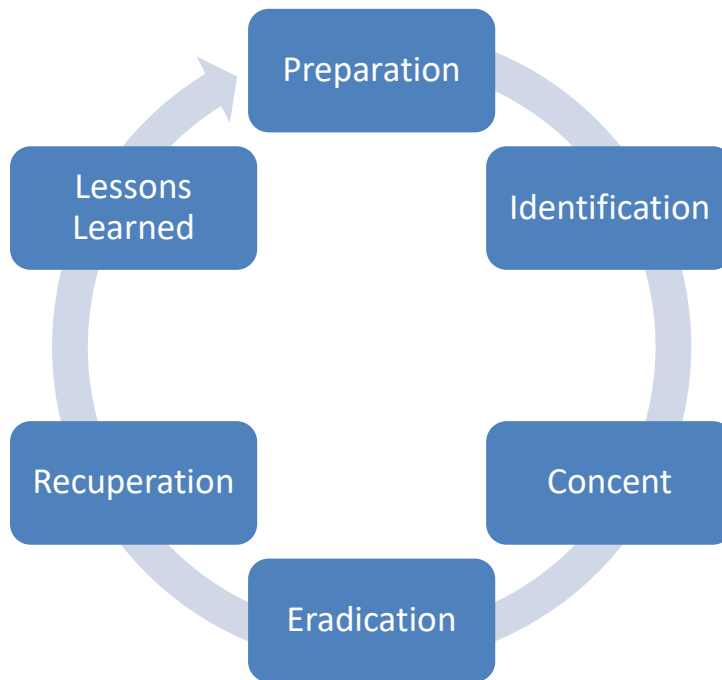
The Incident Response Team will determine if a vulnerability exists, if there is an exploit (exposure), if there is evidence that the vulnerability is being exploited, and if there is a known patch. Finally, the team will determine if this is a new threat (for example, day zero) or a known threat and the estimated effort to contain the problem.

Categoría	Indicadores	Alcance	Acción
1 – Critical	Data loss, malware. Highly Potential Serious Event.	Widespread or on critical servers, Loss of sensitive data	Implement the Incident Response team, activate the security incident response plan throughout the organization.
2 – High	Theoretical threats become active. Event Not Serious, potentially Serious.	Widespread or on critical servers, Loss of sensitive data	Implement the Incident Response team, create an incident to document the event, take measures to mitigate the chances of recurrence and in case of Serious Event activate the security incident response plan throughout the organization.
3 – Medium	Phishing email, active spread infection. Non-Serious, potentially Serious Event.	Widespread	Implement Incident Response, create incident to document the event, take steps to mitigate the

Categoría	Indicadores	Alcance	Acción
			likelihood of recurrence, and in the event of a Serious Event activate the security incident response plan across the organization.
4 - Low	Malware o phishing email	Individual host or person	Notify the Incident Response team, create incident to document the event, take steps to mitigate the likelihood of recurrence.

Incident Management Process

In the event of a security incident, the security incident response team will adhere to the Preparedness-Identification-Awareness-Eradication-Recovery-Lessons Learned process known by its acronym, PICERL as follows:



Preparation

- Develop an incident response plan
 - Establish mandate, delegate authority, decision-making process and chain of command
 - Review/update annually
- Make sure you have an incident response team
 - Dedicated, virtual or retained (identified)
 - Provide training as needed
- Document roles and responsibilities
 - Delegate authority
 - Provide training as needed
- Perform exercises, drills regularly
 - Please note that most types of incidents are known in advance
 - Prepare for the known so you can focus on the unknown
 - Test your plan, team, and tools
- Understanding the environment (architecture)
 - Diagrams, data location, and critical systems
 - Ensure adequate visibility into networks and systems to respond to an incident.
 - Supplier environment and responsibilities
 - Understand vendor dependencies
- Understand the controls that exist
 - Are they sufficient to mitigate the risk to an acceptable level?
- Understand impact
 - Determine maximum tolerable downtime (MTD) and acceptable interrupt window?
 - Prioritized list of assets and downtime
- Prepare the war room and/or conference lines
 - Require a physical and/or virtual location to convene (whatever options apply)
 - Make sure the location is safe and properly equipped
- Establish a communications department in advance
- Establish agreements in advance
 - E.g. Telecommunications Incident Response
 - Ensure the review/update of the annual plan
 - Perform regular exercises
 - Documentation and/or familiarity with the environment beforehand
 - Preferred prices (pre-determined rates to supplier support)
 - Copying Service Level Agreements (SLAs) for Response Time

Notifications

- If an incident is reported SecureHIT will respond to a successful intrusion or attack from the Internet within 2 hours of alarm generation or notification.
- The required action will be documented, depending on the reported incident.
- The intrusion log and policy/procedure manual that will detail the action to be taken for different types of intrusion.
- Ensure there is a central point of contact for employees to report actual or suspected security incidents
- Ensure all employees are required to report security incidents
- Make sure all employees know they should report security incidents and how
- Ensure all employees report security incidents in a timely manner

Call

- Gather those who are aware of the incident
- Involve the members of the Incident Response Team
- Remind yourself of the full responsibility to maintain the need to know
 - Otherwise, it leads to the management of disinformation.
- Communicate effectively and efficiently
- Convene in the war room or conference lines
 - Make sure the location is safe and properly equipped
- Often more than one location is required for different needs (e.g. technical and management equipment)

Identification

- Determine if an incident has occurred
 - Serious Incident or Non-Serious Incident
 - A non-serious incident has the following characteristics:
 - It did not have a malicious intent, or the attack was not directly targeted at the SECUREHIT and,
 - It was determined that the sensitive information of the SecureHIT, specifically ePHI, was not used, disclosed, or damaged.
 - A serious incident has the following characteristics:
 - Had a malicious intent or the attack was directed directly at the SECUREHIT and,
 - It was determined that sensitive information from SecureHIT, specifically ePHI, may have been used, disclosed, or damaged.
 - Look for correlated information to increase confidence that an actual incident exists.
- Perform classification and ensure a common understanding of how it was detected and who is aware
- Analyze indicators and/or precursors
- Conduct research, e.g. search engines, knowledge base
- Document research and evidence collection.
- Prioritize incident management based on relevant factors (functional impact, information impact, recovery effort, etc.
- Determine severity, urgency, and initial impact
- Review information and actions taken to date
- Report the incident to appropriate internal staff and external organizations.

Communications

- Invoke Communications Plan respecting the need to know
- Develop a stakeholder engagement map to determine the level of stakeholder engagement.
- Ensure that reported information is factual based on evidence available at the time
- Ensure that a point of contact knows the current status at all times
- In the event of a Serious, reportable Event, the Federal Secretary of Health must be notified of the non-compliance;

A covered entity must notify the Secretary if it discovers a breach of unsafe protected health information. See 45 C.F.R. § 164.408. All notifications should be sent to the Federal Secretary of Health using the web portal below.

https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

A covered entity's non-compliance notification obligations differ depending on whether the breach affects 500 or more people or less than 500 people. If the number of people affected by a breach is uncertain at the time of submission, the covered entity must provide an estimate and, if it discovers additional information, send updates in the manner specified below. If there is only one option available in a particular shipping category, the covered entity must choose the best option and can provide additional details in the free text portion of the shipment.

If a covered entity discovers additional information that supplements, modifies or clarifies a notice previously submitted to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an appendix to the initial report, using the transaction number provided, after the submission of the initial non-compliance report.

Review the instructions on the federal government portal for sending notifications of non-compliance.

Containment

- Implement the procedures set forth in the incident response manual
- Prevent the damage and the problem from getting worse by containing the incident.
- Determine the source, what vulnerability was exploited and plug the holes
- Continue with the impact/damage assessment and confirm the extent of the incident
- Determine what was changed, for example, files, connections, processes, accounts, access.
- Acquire, preserve, secure and document evidence and preserve the chain of custody
- Continue to take notes, making sure a detailed record of what was found and what you did about it

Eradication

- Eradicate the incident
- Remove all traces of infection or other incident
 - Identify and mitigate all vulnerabilities that were exploited
 - Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered, for example, new malware infections, be sure to perform the identification steps in the newly identified examples, then contain
- Make sure the incident does not happen again
- Better understand the attack vector
- Keep up-to-date documentation and detailed logs
- Make sure any compromised machines are removed or formatted before you put them into service
 - Ensure that the necessary evidence has been collected



Recovery

- Return affected systems to a ready operating state, one by one
- Establish monitoring to make sure the incident does not happen again or does not continue
- Ensure that systems are restored from a trusted source
- Confirm that the affected systems are functioning normally
- Implement additional monitoring to look for related activities in the future if necessary

Lessons Learned

- Hold a lessons learned meeting within 2 weeks of the incident ending
- Create a follow-up report
- Review and review the incident report, "play-by-play"
 - How was the incident detected, who did it, and when?
 - Severity of the incident
 - Methods used for containment and eradication
- Identify opportunities for improvement to better prepare for the next time
- Ensure accountability to follow up on identified opportunities

* Various sources, including NIST Special Publication 800-61 Revision 2 and SANS

Approvals

Responsible Resources

Responsibility for the security of protected information lies with the following responsible party:

Nombre y cargo de la parte responsable	Firma de la parte responsable
Janet Ríos Colón, CEO	


The Responsible Party has reviewed the Security Incident Response Plan and delegates responsibility for mitigating damage to the organization to the Incident Manager.

During the moments when a high security or critical incident occurs, this responsibility is entrusted to the Responsible for the Incident or its delegate.

Incident Manager

The Incident Manager has reviewed the Security Incident Response Plan and acknowledges that when a critical or high security incident occurs, the responsibility for managing the incident is entrusted to the Incident Manager or his or her delegate.

The Incident Handler or his or her delegate is expected to handle the incident in a manner that mitigates further exposure of the organization. The incident will be handled according to the process that includes identification, containment, eradication, recovery and lessons learned.

Nombre y cargo del Manejador de Incidentes	Firma del manejador de incidentes
Jose A. Miranda, ISSO	

References

National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revisión 2, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident>

SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>