

**Incident Handling and Response Policy**

**Bishop Gadsden**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Date** | **New version** | **Previous Version** | **Name** | **Edit(s)** |
| 2017.02.21 | 1.0 | n/a | B. Krafsig | created |
|  |  |  |  |  |
|  |  |  |  |  |

# Overview

The incident handling and response policy and procedures provides a detailed plan of action for responding to cybersecurity incidents and breaches. The plan includes an overall policy as well as general procedures and guidance that help to minimize the impact of a breach and safely restore systems, services, and applications that support critical business functions.

# Purpose

The incident handling and response policy and procedures are designed to minimize damage, restore information technology services, and mitigate and manage organizational risk. The policies and procedures also address the regulatory requirements specified in the HIPAA Security Rule. The incident handling and response policy has been reviewed and implemented at the direction of the Bishop Gadsden President and Chief Executive Officer (CEO).

# Policy

## 45 CFR 164.308(a)(6)(ii) Statement

Bishop Gadsden will develop and implement security incident *Response and Reporting* procedures for identifying, responding to, mitigating, documenting, and reporting on security incidents. Our organization has designed a reporting mechanism for workforce members and business associates to report immediately to our Security Official a suspected or known security incident, namely, whenever this is a breakdown in administrative, physical, and technical safeguards for protecting electronic networks, systems, applications, devices, and media that contain electronic protected health information that actually or potentially compromises the *confidentiality, integrity, or availability* of the electronic protected health information that our organization creates, receives, maintains, or transmits. The Security Official shall investigate the security incident and initiate our organization’s response team and authorize reasonable and appropriate resources to mitigate any harms resulting from the incident and restore confidentiality, integrity, and availability, as applicable, of our organization’s electronic protected health information. The Security Official shall document each security incident, response, and outcome, and provide such documentation as input in the risk analysis process to strengthen our organization’s administrative, physical, and technical safeguards in order to minimize the likelihood of such security incidents in the future. The Security Official also shall report on each security incident according to the response and notification requirements of the Breach Notification Rule (see ***HIPAA Integrity*®** BN, N series of policies and procedures). Our workforce members are required to comply with our organization’s security incident *Response and Reporting* policies and procedures, and are subject to our organization’s sanction policy for failure to comply. Business associate representatives in our facility or facilities are required to report a known or suspected security incident to our Security Official as soon as discovered. A business associate that discovers a security incident pertaining to our organization’s electronic protected health information in its care is responsible for reporting the incident to our Security Official under requirements of the Breach Notification Rule (45 CFR 164.410, at BN, N.4.1) and Security Rule (45 CFR 164.314(a)(2)(i)(C) at SR, BAA.1.0).

## Scope

The incident handling policies and procedures detailed in this document are applicable all Bishop Gadsden personnel, systems, services, applications, workstations, servers, and mobile devices that support business functions. The communication guidelines below detail the circumstances and information flow for interactions with third parties, business partners, service providers, and vendors both during or after a cybersecurity incident.

## Incident Priority

Cybersecurity incidents are prioritized according to the criticality levels of the affected resources involved as well as the impacts to business functions and resident data. Incidents and breaches that impact the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) are assigned the highest priority. Critical business resources and current threats are documented in the asset inventory and threat matrix, respectively. Incidents may be escalated in priority as analysis proceeds and new data and evidence is gathered. Incident priority will be communicated according to the communications and reporting procedures below.

## Definitions

* Event
* Adverse event
* Incident
* Breach

## Metrics

## Reporting

# Plan

## Bishop Gadsden Mission

## Staffing team and organizational structure

* Central Incident Response team operating from a single location
* BG Employees. Part-time responsibilities and Incident Responders. On-call 24x7? All 3 may serve part time. Bernard K will act as both the incident and technical elad.
* Partially outsourced. Perform basic IR in house and use on-call contractors for widespread incidents, intrusion detection, forensics, and analysis. In-house personnel have lots of organizational detail that must be shared. NDAs must be used.
* Operational decision making rests with the BG Director of IT. Contractors cannot take action independently. They will provide data and recommendations.

## Communications plan

* + Media
    - Breach Notification requirements
    - Single Security Officer
    - POC will redirect all inquiries to the Public Affairs Office
    - Maintain a living document describing the current status for the incident
  + Law enforcement
    - Establish POCs for local and state law enforcement
    - Are all BG resources located in state?
    - Make sure that other state law enforcement agencies are considered if any data resides in a different state
  + Vendors (ISP, owner of attacker IP, etc.)
  + BG departments including HR, Facilities Security, and Executive Leadership
  + Victims
  + Regulatory bodies
    - Breach Notification Requirements
* Internal services
  + Intrusion detection using host and network-based security controls
  + Education and awareness
* Contracted services

# Procedure(s)

* Overview
* Preparation
  + - Summary
    - Activities
      * 2 laptops per incident handler
      * Communications
      * Jump-Kit
      * Hardware/Software
      * Incident Analysis
* Detection and Analysis
  + - Utilize threat matrix. Focus on detection and response for those 17 scenarios
    - Indicators of Attack (IoA) – This is not a comprehensive list
      * Web Server (external) access logs indicate network and/or vulnerability scanning activity
      * Multiple ( >= 3) failed authentication attempts for a single OWA user within a short period of time
      * Multiple ( >= 3) failed authentication attempts for multiple OWA users (password spraying) within a short period of time
      * Multiple ( >= 3) failed authentication attempts for server administrator (www.bishopgadsden.org ) within a short period of time
      * Multiple ( >= 3) failed authentication attempts for multiple users (www.bishopgadsden.org ) (password spraying) within a short period of time
      * A large number of emails with file attachments containing malicious payloads are detected, stripped, and stopped by the email security gateway
      * Host-Based Security controls detect and quarantine malicious files on one or more workstations
      * One or more users browse/connect to a known malicious web-site.
    - Indicators of Compromise (IoC)
      * A large number of emails with file attachments containing malicious payloads are sent from a compromised Bishop Gadsden user account
      * Multiple authentication attempts for a single user across a large number of domain resources (>= 3) within a short period of time
      * Enumeration and information gathering commands are executed on a victim workstation. This behavior is inconsistent with the roles and responsibilities for the target user (ie. Human Resources). Commands may include net.exe (user, group, etc.), wmic.exe, cmd.exe, powershell.exe, dsquery.exe, ipconfig, and arp –a.
      * New windows services are created on a workstation or server
      * Changes to and/or new registry keys (run, run once, etc) have been edited/created on one or more work stations
      * Critical resources including internal servers and databases are initiating outbound connections to the internet.
      * Host-Based Security controls detect and quarantine malicious files on one or more workstations
      * A workstation on the internal domain is transferring an unusually large amount of data to an unknown IP address.
    - Analysis Activities will depend on the incident and the indicators observed. This may be contracted out. Activities may include:
      * Creating disk images for affected hosts
      * Capturing volatile data including memory or rotated logs
      * Log analysis
      * Malware analysis
      * Network traffic analysis
      * Event correlation. For example, registry changes on multiple systems or network connections from multiple systems to a common IP address
    - Incident Prioritization
      * Functional impacts
      * CIA impacts
      * Recoverability
    - Escalation Process
    - Documentation
      * Logbooks. Document and timestamp each incident during the detection and analysis phase
      * Date and sign all documents
      * Manage the chain-of-custody for all evidence gathered
      * The following information for the incident should be captured and changed as the incident proceeds
        + Current status
        + Summary
        + Indicators related to the incident
        + Other similar incidents
        + Actions taken by the incident handlers
        + Chain of custody for all evidence gathered

Identifying information for the evidence gathered

POC information for all individuals who collected or handled evidence

Time and date

Location where evidence is stored

* + - * + Access restrictions for gathered data
        + Impact assessment
        + Contact information for the protected communications plan
        + Comments
        + Next Steps
      * Checklist
      * Incident Log
      * Develop and refine SOPs as needed
    - Notifications
* Containment, Eradication, and Recovery
  + Containment
    - Choosing containment strategy
    - Identify the attacking hosts
  + Eradication and Recovery – This will depend on the details and severity of the incident
    - Identifying affected hosts
    - Disabling user accounts
    - Searching for and removing Malware
    - Mitigating/patching vulnerabilities
    - Restoring from back-up
    - Rebuilding from trusted media
    - Rebuilding domain resources from scratch
    - Making changes to system configurations and/or security controls
* Post Incident Activity and Reporting
  + Determining business impacts
  + Updating threat matrix
  + Revisiting risk analysis
  + Implementing permanent mitigations and fixes
  + Developing lessons learned
  + Update incident logs
  + Gather and document metrics:
    - Number of incidents handled
    - Man-hours spent per incident
    - Average man-hours spent per incident
    - Timeline
    - Time-to-Detection
    - Time-to-Recovery

# Related Standards, Policies, and Processes

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | Action |  |  | Completed |  |
|  | Detection and Analysis | | | | | | |  |
| 1. | | | Determine whether an incident has occurred | | |  | | |
| 1.1 | | | Analyze the precursors and indicators | | |  | | |
| 1.2 | | | Look for correlating information | | |  | | |
| 1.3 | | | Perform research (e.g., search engines, knowledge base) | | |  | | |
| 1.4 | | | As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence | | |  | | |
| 2. | | | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) | | |  | | |
| 3. | | | Report the incident to the appropriate internal personnel and external organizations | | |  | | |
|  | Containment, Eradication, and Recovery | | | | | | |  |
| 4. | | | Acquire, preserve, secure, and document evidence | | |  | | |
| 5. | | | Contain the incident | | |  | | |
| 6. | | | Eradicate the incident | | |  | | |
| 6.1 | | | Identify and mitigate all vulnerabilities that were exploited | | |  | | |
| 6.2 | | | Remove malware, inappropriate materials, and other components | | |  | | |
| 6.3 | | | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them | | |  | | |
| 7. | | | Recover from the incident | | |  | | |
| 7.1 | | | Return affected systems to an operationally ready state | | |  | | |
| 7.2 | | | Confirm that the affected systems are functioning normally | | |  | | |
| 7.3 | | | If necessary, implement additional monitoring to look for future related activity | | |  | | |
|  | Post-Incident Activity | | | | | | |  |
| 8. | | | Create a follow-up report | | |  | | |
| 9. | | | Hold a lessons learned meeting (mandatory for major incidents, optional otherwise) | | |  | | |

# References

# Point of Contact (PoC)