

**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 |
|  |  |  |  |  |

**1.** **Overview** 5

**2.** **Purpose** 5

**3.** **Policy** 5

**3.1.** **45 CFR 164.308(a)(6)(ii)** 5

**3.2.** **Scope** 6

**3.3.** **Incident Priority** 6

**3.4.** **Definitions** 6

**4.** **Plan** 7

**4.1.** **Bishop Gadsden Mission** 7

**4.2.** **Staffing team and organizational structure** 7

**4.3.** **Communications plan** 7

**4.3.1.** **Media** 8

**4.3.2.** **Law enforcement** 8

**4.3.3.** **Vendors (ISP, owner of attacker IP, etc.)** 8

**4.3.4.** **BG departments including Human Resources (HR) and Executive Leadership** 8

**4.3.5.** **Victims** 8

**4.3.6.** **Regulatory bodies** 9

**4.4.** **Internal Activities and Contracted Services** 9

**5.** **Procedure(s)** 10

**5.1.** **Overview** 10

**5.2.** **Preparation** 10

**5.2.1.** **Jump Kit** 10

**5.2.2.** **Investigator laptops** 11

**5.3.** **Detection and Analysis** 11

**5.3.1.** **Indicators of Attack (IoA)** 11

**5.3.2.** **Indicators of Compromise (IoC)** 12

**5.3.3.** **Analysis** 13

**5.3.4.** **Incident Prioritization** 13

**5.3.5.** **Escalation Process** 13

**5.3.6.** **Documentation** 14

**5.4.** **Containment, Eradication, and Recovery** 15

**5.5.** **Post Incident Activity and Reporting** 16

6. Related Standards, Policies, and Processes 16

7. References 18

8. Point of Contact (PoC) 18

# **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. The Bishop Gadsden incident handling and response policy and procedures have been created according to standards defined in the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2.

# **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)**

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. 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**

The definitions used throughout this document have been taken directly from the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide[[1]](#footnote-1) or other NIST resources.

* **Event** – “An event is any observable occurrence in a system or network”
* **Adverse event** – “Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”
* **Incident** – “Computer security incident is a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices”
* **Breach –**  “Impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI.”

# **Plan**

## **Bishop Gadsden Mission**

Bishop Gadsden is the Southeast's leading life care retirement community, providing hospitality, healthcare, and assisted living services to more than 450 residents.

## **Staffing team and organizational structure**

Bishop Gadsden has a Director of Information Technology (IT) with 2 direct reports. Due to staffing constraints and the size of the organization, one of the direct reports serves part time as the Information Systems Security Officer. There is a separate Security Supervisor who handles physical security for the campus and it’s residents. The Director of IT and the Security Supervisor report to the Bishop Gadsden CEO and Environmental Services Director, respectively.

The Director of IT will lead a central incident response team operating from a single location at 1 Bishop Gadsden Way, Charleston SC 29412. Due to staffing constraints and the size of the organization, the incident response team will only include part time incident responders. Incidents may be reported by emailing [BGIT.SUPPORT@bishopgadsden.org](mailto:BGIT.SUPPORT@bishopgadsden.org) or opening a ticket in SpiceWorks.

The internal team will execute basic IR in house and use contractors for larger incidents, intrusion detection, forensics, and additional analysis. Non-disclosure agreements (NDAs) will be out in place before coordinating any effort with external contractors. All operational decision-making rests with the BG Director of IT; contractors cannot take action independently.

## **Communications plan**

Bishop Gadsden will coordinate with and communicate the status of incident response efforts with both internal stakeholders and external organizations as appropriate. All communications and correspondence will be at the discretion of the Bishop Gadsden President and CEO and will be consistent with Bishop Gadsden policy and HIPAA Breach Notification rule. Internal stakeholders and external organizations may include:

### **Media**

In the event of a breach of unsecured protected health information involving more that 500 residents, Bishop Gadsden will provide notification to prominent media outlets serving the state. The content of the notification will be drafted by the Bishop Gadsden Director of IT and approved by the President and CEO. The Public Affairs Officer (Kimberly Borts 843 406-6334) will disseminate the notification and serve as the Point of Contact for all media inquiries. Coordination and correspondence with the media will be consistent with Bishop Gadsden Policies and Procedures, including:

* + Notification to Media: Timeliness of Notification (45 CFR 164.406(b))
  + Notification to Media: Content of Notification (45 CFR 164.406(c))

### **Law enforcement**

Bishop Gadsden will coordinate with Local, State, and Federal law enforcement as appropriate. The Bishop Gadsden Security Officer will serve as the Point of Contact (POC) for all communication and correspondence. In the event that the incident involves Bishop Gadsden resources located in another state (ie. backup), the POC will engage that States’ law enforcement as appropriate.

### **Vendors (ISP, owner of attacker IP, etc.)**

Bishop Gadsden will coordinate with vendors and third party service providers throughout the incident handling process. This will include the Internet Service Provider (ISP) for the attacking IP. The data gathered will help to determine the scope and timeline for the breach

### **BG departments including Human Resources (HR) and Executive Leadership**

The Bishop Gadsden Director of IT, Information Systems Security Officer, and Security Supervisor will provide updates and status to Bishop Gadsden leadership. The frequency of the updates will depend on the severity of the incident and the current stage of the incident handling response. The Director of IT will maintain an official statement regarding the scope, severity, and status of the incident. This statement will serve as a living document that can be updated as the incident is investigated and closed.

### **Victims**

Coordination and correspondence with victims will be consistent with Bishop Gadsden Policies and Procedures, including:

* + Notification to Individuals: Timeliness of Notification (45 CFR 164.404(b))
  + Notification to Individuals: Content of Notification—Elements (45 CFR 164.404(c)(1))
  + Notification to Individuals: Content of Notification—Plain Language Requirement (45 CFR 164.404(c)(2))
  + Notification to Individuals: Methods of Individual Notification—Written Notice (45 CFR 164.404(d)(1))
  + Notification to Individuals: Methods of Individual Notification—Substitute Notice (45 CFR 164.404(d)(2))
  + Notification to Individuals: Methods of Individual Notification—Additional Notice in Urgent Situations (45 CFR 164.404(d)(3))

### **Regulatory bodies**

Coordination and correspondence with regulatory bodies will be consistent with Bishop Gadsden Policies and Procedures, including:

* + Notification to the Secretary: Breaches Involving 500 or More Individuals (45 CFR 164.408(a) & (b))
  + Notification to the Secretary: Breaches Involving Less than 500 Individuals (45 CFR 164.408(a) & (c))

## **Internal Activities and Contracted Services**

Bishop Gadsden will execute the following in support of the Incident Response process and procedures:

* + Communication with internal stakeholders and external organizations
  + Determination of severity, scope, and priority for the incident(s)
  + Initial log collection and analysis for affected endpoints and user accounts
  + Containment for affected endpoints and user accounts
  + Documenting incident details, timeline, and status
  + Gathering forensic evidence and artifacts including volatile and non-volatile storage
  + Eradication and Recovery

Bishop Gadsden may contract with Cybersecurity Service Providers for the following services depending on the severity and scope of the incident:

* + Forensic Analysis
  + Log Analysis
  + Timeline creation
  + Malware Analysis
  + Network Traffic Analysis
  + Event Correlation
  + Eradication and Recovery

# **Procedure(s)**

## **Overview**

As this capability matures, specific standard operating procedures (SOPs) may be added as appropriate. For example, there may be specific preferred methods and tools for gathering volatile storage or doing forensic analysis on a mobile device. However, for this initial increment a general outline for the incident handling procedure is detailed below.

## **Preparation**

These activities should be executed by the organization before an incident occurs. They will significantly reduce response times and avoid confusion when the incident occurs.

### **Jump Kit**

These items should be gathered and set aside specifically for handling incidents. There are several good resources[[2]](#footnote-2) for building a jump kit, however, the contents should always be built to fit the organization and it’s mission. Try not to “borrow” from the jump kit as those items might not be there when you really need them. Typical jump kit items include:

* + - * Notebooks
      * USB jump drives
      * Network switch with port mirror
      * External hard drives (1TB)
      * Blank DVDs
      * Forensic/Imaging software
      * Clean binaries
      * Trusted media (OS installs)
      * Cables and Adapters

### **Investigator laptops**

Whenever possible each investigator should have 2 laptops built from trusted media. The first will be for documenting the incident and communicating with team members, internal groups, and external organizations. Do not connect this laptop to the affected network/domain and utilize Out-of-Band (OOB) communications whenever possible. Until the scope and severity of an incident has been determined, you will want to avoid connecting the investigators’ laptops to the impacted network or domain. If the investigator laptops become infected, the attacker may discover details of the incident handling effort and make it that much more difficult to contain and eradicate the attackers from the network. The second laptop should be used to gather and analyze evidence, artifacts, and logs. For example, this laptop may be connected to a span port on a switch to observe network traffic. This laptop should fully patched and contain clean binaries built from trusted media.

## **Detection and Analysis**

Bishop Gadsden will leverage the existing threat matrix as well as host and network-based security controls to detect and analyze incidents. The threat matrix, which was created as part of the initial risk assessment, contains 17 adversarial and non-adversarial threat scenarios. These scenarios are considered the most likely threats based on previous incidents observed at Bishop Gadsden. Each scenario includes 1 or more events, which consider the resource being attacked, exploitable vulnerabilities, and the current security controls in place. The host-based (**Symantec**) and email (**Barracuda**) security controls will provide the basis for detection.

The incident handling procedures will focus on an initial set of Indicators of Attack (IoA) and Indicators of Compromise (IoC). These are **not comprehensive** lists; they are intended to evolve with changes in attacker tactics, techniques, and procedures (TTPs). Security controls should be tuned to provide defenders with the greatest probability for observing these IoAs and IoCs.

### **Indicators of Attack (IoA)**

* + - * 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**

Incidents are typically prioritized according to the three factors below. Other factors and alternative analysis may be considered at the discretion of Bishop Gadsden leadership. Incidents may be qualitatively scored as low, medium, and high.

* + - * **Functional impacts** – This includes the impact to Bishop Gadsden being able to execute its mission, which is to provide hospitality, assisted living, and healthcare services to its 450+ residents.
      * **CIA impacts** – These include impacts to the confidentiality (C), integrity (I), availability (A), of protected health information (PHI). These incidents will receive the highest priority.
      * **Recoverability** – This includes an evaluation of how easy or difficult it will be to recover from an incident and return to normal operations. (**ie.** Category 5 Hurricane vs. Ransomware vs. Planned power outage)

### **Escalation Process**

Incidents may be escalated as the analysis proceeds. Changes in scope and/or severity may warrant a change in incident priority. Analysis may also reveal criminal misconduct, which requires escalation to local, state, or federal law enforcement. The communications plan may be executed accordingly. Escalation will be at the discretion of the Director of IT and Bishop Gadsden leadership.

### **Documentation**

Maintaining accurate and timely documentation is critical to the incident handling process. This is especially the case when artifacts and data may be used in criminal or civil court. This is not a complete list, however, the checklist below will assist the handlers during an incident[[3]](#footnote-3).

* + - * Utilize logbooks. Document and timestamp each incident during the detection and analysis phase
      * Date and sign all documents and all log notebook pages
      * If including printed notes and figures, be sure to **staple** these into the logbook. Avoid tape whenever possible.
      * Manage the chain-of-custody for all evidence gathered. You will want to be able to account for the handler and location for any evidence gathered and presented in a court of law.
      * At a minimum, capture and update the following information for all incidents:
        + Current status of the incident (open/closed/re-opened)
        + Updated summary
        + Indicators related to the incident
        + Any 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 communications plan
        + Comments
        + Next Steps

A checklist[[4]](#footnote-4) has been included in Appendix A in order to assist the incident handlers.

Finally, the organization should maintain a log/list that captures basic metadata for each incident that occurs. Metadata may include time, date, incident name, priority, status, and remediation(s).

## **Containment, Eradication, and Recovery**

### **Containment**

The containment strategy is going to depend on the nature of the incident as well as the risk tolerance of the Bishop Gadsden organization. For example, in the event of a ransomware attack, one of the best approaches is to disconnect from the network and shut down the targeted resource. This minimizes the chances that the attack will spread and may make it possible to retrieve some content from the infected drive. Alternatively, for certain malware infections, it will be important to retrieve artifacts and data from volatile storage. In the target resource is shut down, the artifacts may be lost.

### **Eradication and Recovery**

Eradication and recovery activities are also going to depend on the nature of the incident. These can range from deleting a suspicious email on the Outlook server to rebuilding an entire domain. To a certain extent, recovery activities will also depend on the risk appetite of the organization. However, a good rule of thumb is that if there is any doubt wipe it clean and rebuild from trusted media

Eradication and Recovery activities include, but are not limited to:

* + - Identifying affected hosts
    - Disabling user accounts
    - Searching for and removing malware (files, services, subscriptions, registry keys, etc.)
    - 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**

Closing out and reporting on the incident provides Bishop Gadsden with an opportunity to develop and implement mitigations, improve existing security controls, and satisfy specific regulatory requirements. Each of these activities helps Bishop Gadsden to better prepare for repeated or similar attacks and incidents. Post Incident and reporting activities may include:

* + Determining business impacts
  + Updating the threat matrix
  + Revisiting the risk analysis
  + Implementing permanent mitigations and fixes
  + Developing lessons learned
  + Updating the incident logs
  + Gathering and documenting metrics including:
    - 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**

# **Appendix A – Incident Response Checklist**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | 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)

1. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [↑](#footnote-ref-1)
2. http://www.dshield.org/diary/Day%2B4%2B-%2BPreparation%3A%2B%2BWhat%2BGoes%2BInto%2Ba%2BResponse%2BKit/5125 [↑](#footnote-ref-2)
3. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [↑](#footnote-ref-3)
4. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [↑](#footnote-ref-4)