**Statewide Health Information Policy Manual (SHIPM) 3.1.2 – Incident Procedures**

*Compliance Review Tool #38*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact addressing Incident Procedures and Reporting? |  |  |
| 2 | Does the artifact(s) define what a Security Incident is for the organization’s business functions? |  |  |
| 3 | Does the artifact(s) list the possible types of Security Incidents and the required response for each type? |  |  |
| 4 | Does the artifact(s) identify who the Security Incident must be reported to within the organization? |  |  |
| 5 | Does the artifact(s) ensure immediate reporting to California Compliance and Security Incident Reporting System (Cal-CSIRS) in accordance with State Information Management Manual (SIMM) criteria and procedures?  |  |  |
| 6 | Does the artifact provide a description how to capture and log the incident – specifically indicating that the security log should include (at a minimum): | n/a |  |
| 6a | * Contact information for the person reporting the incident (to include name, email address and phone number)
 |  |  |
| 6b | * Description of incident
 |  |  |
| 6c | * Date, time and location of the incident
 |  |  |
| 6d | * Date, time and how the incident was discovered
 |  |  |
| 6e | * Evidence of the incident
 |  |  |
| 6f | * Make/model of the affected computer(s)
 |  |  |
| 6g | * Internet Protocol (IP) addresses of the affected computer(s)
 |  |  |
| 6h | * Assigned name of the affected computer(s)
 |  |  |
| 6i | * Operating system of the affected computer(s)
 |  |  |
| 6j | * Location of the affected computer(s)
 |  |  |
| 6k | * Actions taken to mitigate
 |  |  |
| 7 | Does the artifact(s) describe procedures to receive, process and respond (if needed) to BA reported incidents and breaches? |  |  |
| 8 | Does the artifact(s) describe how to mitigate, to the extent reasonable, the situation that caused the harmful effects and consult with system owners to quarantine the incident and limit damage? |  |  |
| 9 | Does the artifact(s) describe how to document the security incident, how the state entity responded, and the results (outcomes)? These procedures should include, but not limited to:  | n/a |  |
| 9a | * Incident Response Team. How the security incident is assigned, managed and investigated, along with the procedures for escalation, and internal reporting and response.
 |  |  |
| 9b | * Procedure for notifying individuals. How to manage security incidents involving breach of personal information, especially health information.
 |  |  |
| 9c | * Mobilizing emergency and third party investigation and response (if necessary).
 |  |  |
| 9d | * Consulting with personnel management/human resources (HR), if there is a violation of appropriate use policy by workforce member(s).
 |  |  |
| 9e | * Communicating with law enforcement, when actual or suspected criminal activity is involved.
 |  |  |
| 9f | * Handling of the incident that includes preparation, detection, analysis, containment, eradication, and recovery as well as coordinating with business continuity planning activities.
 |  |  |
| 10 | Does the artifact(s) describe how to evaluate security incidents as part of the state entity’s ongoing risk management activities?  |  |  |
| 11 | Does the artifact(s) indicate that the state entity is responsible to test their incident response capability to determine its effectiveness, document the results, and incorporate lessons learned to continually improve the incident response plan and procedures? |  |  |
| 12 | Does the artifact(s) indicate that the state entity is responsible to train their workforce members in the organization’s implemented security incident and response policies and procedures? |  |  |
| 13 | Does the artifact indicate retention period of 6 years for incident related documentation? |  |  |
| 14 | \* Does the artifact describe the reporting of serious cyber incidents to federal cyber security organizations (i.e., FBI, HC3, US-CERT) |  |  |
| 15 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 15a | * Effective Date?
 |  |  |
| 15b | * Revision Date?
 |  |  |
| 15c | * Document the authorizing (senior or executive) management approval?
 |  |  |

\* Industry best practice

Title(s) of Submitted Policy/Document/Artifact(s) Reviewed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Stored Location of, or link to Artifact(s) Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Overall CDII Reviewer Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of CDII Reviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_

Title of or link to Other Source(s) used (e.g., sources not in checklist, templates) – *optional*: