East Haven Police Department	Type of Directive: **Policies & Procedures**	**No. 804.1**
	Subject/Title: **CJIS Events Incident Response Policy**	**Issue date:** **August 29, 2017**
		Effective Date: **September 15, 2017**
	Issuing Authority: **Honorable Board of Police Commissioners**	**Review Date:** **Annually**
References/Attachments: **Criminal Justice Information Services (CJIS) Security Policy**		**Rescinds:** **N/A**
		Amends: **N/A**

I. PURPOSE

A. The purpose of this directive is to set forth the policies and procedures of the East Haven Police Department (EHPD) regarding procedures dealing with incidents related to Criminal Justice Information (CJI).

II. POLICY

A. It is the policy of the East Haven Police Department to employ regulations to protect CJI and to establish procedures to handle incidents that include adequate preparation, detection, analysis, containment, recovery, and user response activities including tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

III. DEFINITIONS

A. CJI – Criminal Justice Information

B. CJIS – Criminal Justice Information Systems

C. CSA ISO - CJIS Systems Agency Information Security Officer

D. ISO – Information Security Officer

E. LASO – Local Agency Security Officer

IV. GENERAL GUIDELINES AND CONSIDERATIONS

A. The security risk of both accidental and malicious attacks against government and private agencies remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall do the following:
   1. Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities.

   2. Track, document, and report incidents to appropriate agency officials and/or authorities. Information Security Officers (ISOs) have been identified as the point of contact on security-related issues for their respective agencies and shall ensure Local Agency Security Officers (LASOs) institute the CSA incident response reporting procedures at the local level.

   3. Appendix F of the FBI CJIS Security Policy contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO. Refer to current version of the FBI CJIS Security Policy for additional incident response requirements related to mobile devices used to access CJI.

V. PROCEDURES

A. Reporting security events.
   1. The Department shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken.

   2. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the Department shall employ automated mechanisms to assist in the reporting of security incidents.

   3. All employees, contractors, and third party users shall be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of Department assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

B. Reporting Structure and Responsibilities

1. The FBI CJIS Division will manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
    a. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.

    b. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.

    c. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on www.FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.

    d. Track all reported incidents and/or trends.

    e. Monitor the resolution of all incidents.

2. The CSA ISO will assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
    a. Identify individuals who are responsible for reporting incidents within their area of responsibility.

    b. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

    c. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.

    d. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.

    e. Act as a single POC for their jurisdictional area for requesting incident response assistance.

C. Management of Security Incidents

1. A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

D. Incident Handling

1. The Department shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

2. Wherever feasible, the Department will employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

3. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

E. Collection of Evidence
   1. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence.

F. Incident Response Training
   1. The Department shall ensure general incident response roles responsibilities are included as part of required security awareness training.

G. Incident Monitoring
   1. The Department shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.