East Haven Police Department	**Type of Directive:** **Policies & Procedures**	**No. 802.2**
	Subject/Title: **Sensitive Media and Disposal/Sanitization**	**Issue date:** **December 22, 2015** **Effective Date:** **January 15, 2016**
	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 the proper disposal of media that contains sensitive data that is restricted to law enforcement and criminal justice agency use only.

II. POLICY

A. It is the policy of the EHPD to employ regulations to protect sensitive and classified information and to provide guidelines to employees on its use.

B. All employees shall follow the Criminal Justice Information Services (CJIS) Security Policy regulations as set forth by the Federal Bureau of Investigation and the Connecticut Department of Emergency Services and Public Protection.

C. Improper disposal of Connecticut On-Line Law Enforcement Communications Teleprocessing/National Crime Information Center (COLLECT/NCIC), EHPD non-public information, other government database information, and/or media may put employees, the agency and others at risk.

D. This policy applies to employees, contractors, temporary staff/volunteers/visitors, and/or other workers at the EHPD that have or may have access to sensitive and/or classified data and media.

E. This policy also applies to all equipment that processes classified and sensitive data that is owned, leased, or used by EHPD.

III. DEFINITIONS

A. Physical Media - items such as hard copy documents (papers, print-outs), diskettes, tape cartridges, ribbons, and other similar items used to process, print or store classified and/or sensitive data.

B. Electronic Media Equipment - Information technology systems that have processed, stored, or transmitted sensitive and/or classified information.

C. Electronic Media Sanitization - A process of making sensitive data non-retrievable by unauthorized persons by means of overwriting, degaussing, or destruction.

D. Overwrite - A process by which data is deleted. The process needs to be completed at least three times in order to safely prevent access to sensitive data by unauthorized personnel.

E. Degauss - To neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event that the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device. All media shall be degaussed with a National Institute of Standards and Technology (NIST) approved degausser.

F. Destruction - Destruction of magnetic media is to physically dismantle the portion of the device that contains the sensitive electronic data, and to incinerate or otherwise destroy that media so that sensitive data is no longer accessible/retrievable.

IV. PROCEDURES

A. When no longer usable, physical media shall be shredded immediately or placed in properly marked locked shredding bins.

B. When no longer usable, electronic media equipment shall be sanitized by overwriting at least three times, degaussing, or destruction. After hardware has been determined to be unusable or scheduled to be returned, any storage media will be removed and sanitized. This includes but not limited to: fax machines, printers, copiers, computers, tablets, smart cellular phones, etc.

C. Employees will send all electronic media equipment to be decommissioned to the Property Officer to be properly disposed.

D. Equipment that is being moved to another location must have authorized personnel present (COLLECT/NCIC certified). If equipment is to be removed from the custody of authorized personnel (such as for equipment repair/service), the storage memory must be overwritten at least three (3) times per CJIS Security Policy.