Electronic Media Sanitization and Destruction

346.1 PURPOSE AND SCOPE

A large volume of electronic data is stored on electronic media used by computer systems throughout the Santa Ana Police Department. This data may contain sensitive information including criminal justice information and personnel records. The media that is of concern is classed as non-volatile, as defined in Section 346.2, below. Improper disposal of these non-volatile storage devices or the data contained therein may result in unauthorized access constituting a security breach. As such, all users of computer systems within the Department are responsible for ensuring the proper use and disposal of these devices.

The purpose of this policy is to establish proper methods for the disposal of media containing electronic data in accordance with applicable laws, regulations and the U.S. Department of Justice Criminal Justice Information Services (CJIS) Security Policy. The policy will also protect sensitive and classified data from persons not legally entitled to access the information.

346.2 DEFINITIONS

Volatile Data: Memory that loses all of its data when not in use.

Non-Volatile Data: Memory that retains its data after it is powered down.

Electronic Media: Any non-volatile, electronic storage device that is used to record information, including but not limited to hard disks and removable storage devices such as CD's, DVD's, USB memory devices, and flash memory cards/sticks commonly used in cameras.

346.3 MEDIA DISPOSAL METHODS

All forms of media disposal shall be completed in compliance with the City Records Retention Policy and applicable legal requirements.

346.3.1 OVERWRITING

Sanitization of electronic media via overwriting is the process of replacing the previously stored data on the media with a random set of binary data (i.e. ones and zeroes). Overwriting should be performed utilizing software designed for this purpose. For the process to be complete, three (3) passes over the media must be made by the software to ensure the effective erasure of all previous data. When practicable, a verification pass will also be made to confirm that the process was successful.

346.3.2 DESTRUCTION

Destruction of electronic media is the process of physically damaging a medium so that it is not accessible by any device that may normally be used to read electronic information on the media, such as a computer or audio/video player. Appropriate methods of destruction include: crushing; shredding; incinerating; physically disassembling the media and ensuring that the storage medium has been damaged to the extent that no data can be pulled; and any other physical means that will render the data on the medium permanently inaccessible.

346.3.3 DEGAUSSING

Degaussing is the process of magnetically erasing data from magnetic media, typically using a strong electromagnet. Degaussing of a hard drive is essentially a specialized form of destruction, as the drive is no longer usable once the process has been completed due to the device's functional programming being erased along with the data the drive contained. Once degaussing is complete, verification will be made that the data is no longer accessible.

346.4 MEDIA DISPOSITIONS

346.4.1 REUSE

Any media that is to be reused by individuals not authorized to possess or access sensitive information used the by the Department shall be sanitized via overwriting. This shall include, but is not limited to, equipment to be surplused, sold, donated, or transferred to another City department. If a medium cannot be successfully sanitized by overwriting due to damage or any other reason, then it shall be destroyed.

346.4.2 DISCARDING

Any media that is to be discarded (i.e. thrown away) shall be destroyed or degaussed. Reasons for discarding may include but are not limited to: damage, obsolescence, or the medium and/or its data no longer being necessary. All media that is to be discarded and cannot be overwritten (e.g. CD-ROM's, DVD-ROM's, locked flash memory devices, etc.) shall be destroyed.

346.5 MONITORING REQUIREMENT

The sanitization and/or destruction of Department electronic media shall be carried out or witnessed by authorized Department personnel.

346.6 DOCUMENTATION

The sanitization and/or destruction of Department electronic media shall be documented by authorized Department personnel. This documentation shall include at minimum:

- The date and time the process was carried out
- The authorized Department personnel that carried out or witnessed the process
- If the process was witnessed by Department personnel and carried out by an outside party (i.e. vendor), then the name of the party and any related process record information (e.g. invoice or work-order number, etc.)
- A description of the media including the manufacturer, capacity, and the model and serial number when possible
- The steps taken to sanitize or destroy the electronic media
- The name and version number of any software used in the sanitization of electronic media
- Any report generated by software used in the sanitization of electronic media