**DUBLIN POLICE DEPARTMENT**

**STANDARD OPERATING PROCEDURE**

**SECTION: C-003 GCIC/NCIC DISPOSAL OF MEDIA**

**POLICY AND PROCEDURES**

**EFFECTIVE DATE: 11 NOV 2016 NUMBER OF PAGES: 2**

**REVISED DATE: 09 AUG 2023 DISTRIBUTION AUTHORIZATION:**

**STANDARD COVERED: *CHIEF KEITH MOON***

**N/A**

**Disposal of Media Policy and Procedures**

**Purpose**

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at the Dublin Police Department. These rules are in place to protect sensitive and classified information, employees, and the Dublin Police Department. Inappropriate disposal of Dublin Police Department, FBI, or GBI Criminal Justice Information (CJI) and media may put employees, Dublin Police Department, FBI, or GBI at risk.

**Scope**

This policy applies to all Dublin Police Department employees, contractors, temporary staff, and other workers at Dublin Police Department, with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by the Dublin Police Department.

**Policy**

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store, and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by Dublin Police Department.

Physical media (printouts and other physical media) shall be disposed of by one of the following methods:

* shredding using Dublin Police Department-issued shredders.
* Place in locked shredding bins for [private contractor name] to come on-site and shred, witnessed by Dublin Police Department personnel throughout the entire process.
* incineration using Dublin Police Department incinerators or witnessed by Dublin Police Department personnel onsite at the agency or at contractor incineration site if conducted by non-authorized personnel.

Electronic media (hard drives, tape cartridges, CDs, printer ribbons, flash drives, printer, and copier Hard-drives, etc.) shall be disposed of by one of the methods:

Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are weak and cannot effectively degauss magnetic media.

Destruction – a method of destroying magnetic media. As the name implies, the destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI or GBI CJI and/or sensitive and classified information shall not be released from Dublin Police Department control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.