STANDARD OPERATING PROCEDURE: 2007-13

DATE ISSUED: May 31, 2007 **REVISION DATE:** October 23, 2015
November 27, 2013
December 10, 2012

SUBJECT: Confidential Information and the Disposal of Confidential or Sensitive Information

ISSUED BY: Donald J. Winsock, Jr., Deputy Administrator, Operations
Jeffrey A. Horwitz, Deputy Administrator, Systems

APPROVED BY: Bill K. Kang, Administrator

REFERENCE: NCIC/VCIN Operating Manuals, FBI Security Policy 5.3, and
VCIN Access TAC Memo dated October 13, 2015

I. GENERAL:

The Emergency Communications Center has access to confidential and sensitive information through various computerized data banks and through written or verbal communications from other departments and agencies. As a condition of this access, ECC must comply with the standards and procedures to ensure confidential and sensitive information is not relayed or disseminated outside the intended or permitted recipients.

II. PROCEDURE:

A. No employee shall divulge confidential or sensitive information. The official business of the department shall be treated as confidential.

B. All information obtained through National Crime Information Center (NCIC), Virginia Criminal Information Network (VCIN), Department of Motor Vehicles (DMV), Interstate Identification Index (III), National Law Enforcement Telecommunications System (NLETS) and Criminal Justice Information System (CJIS) is to be used by law enforcement personnel and for law enforcement purposes only in accordance to established policies and procedures.

C. Police Records Management System (RMS) will be used by law enforcement personnel and for law enforcement purposes only.

D. When confidential or sensitive information has served its purpose, the information must be shredded or destroyed. This includes information obtained from resources listed in sections B and C, both printed or media recordings. This is also the procedure for police or fire worksheets that include telephone numbers of County employees, police information sheets, or any other documents that contain confidential or sensitive information including any notes taken in the performance of assigned duties.

E. At no time will a copy of CJIS information, in any form, be removed from ECC for private use or dissemination.

F. The taking of photos and filming will not be permitted in the ECC without prior approval from a Deputy Administrator or above. There is a potential of sensitive or confidential information from the Computer Aided Dispatch (CAD) and/or any computer with VCIN access being captured; therefore all taking of photos and filming must be closely monitored. ECC has stock photos that may be provided upon request.

G. When an employee with CJIS access terminates employment for any reason (retirement, termination, resignation, etc.) the employee must go through the checkout process with the TAC officer or designee. The TAC officer or designee assumes responsibility for notifying Virginia State Police to restrict access to CJIS.