TALBOT COUNTY SHERIFF'S OFFICE

115 West Dover St.
Easton, Maryland 21601

Office
410-822-1020

Joseph J. Gamble
Sheriff

Fax
410-770-8110

February 4, 2016

GENERAL ORDER NO. 16-016

TO: All Talbot County Sheriff's Office Personnel

SUBJECT: Criminal Justice Information System (CJIS) Audits and Review

I. PURPOSE

To establish procedures for the review, accountability, and implementation of best practice measures to assure fully compliant results of any and all CJIS internal or external audits.

II. POLICY

All TSO personnel involved in the compilation of investigative reports, the review of any and all such reports, or who are involved in the entry, quality control, or periodic validation of items or data extracted and entered into CJIS from these reports will take all measures to assure that the information inserted or created as a record is accurate, complete, and that all data elements are supported by independent and verifiable documentation. All such entries and control of report data will be consistent with legal authority and guidelines. Only persons so authorized, trained, and granted approved access to CJIS will have control over the entry, update, audit, validation and removal of data that is entered into CJIS.

III. RESPONSIBILITIES

A. Only persons so authorized, trained, and granted CJIS access will be permitted to make, alter, remove or close CJIS entries. A Support Staff member will be designated and assigned primary responsibility for this task; consistent with this duty being a significant part of their assigned responsibilities. This assigned person will assume the role of liaison with authorized internal or external CJIS inquiries or audits.

B. An additional Support Staff or sworn member may be assigned as an alternate member for this task and obligation; meeting the same requirements that qualify the primary assigned member.

C. The Criminal Commander will have responsibility and oversight for the member so assigned with the task of CJIS entry, update, alteration, removal, or validation. The Criminal Commander will assume the role of alternate CJIS liaison and will work in conjunction with any and all issues that relate to CJIS audits, reviews, or changes and implementation of policy.

IV. PROCEDURE

A. Notice of CJIS audits, records requests, or file inquiries will be communicated immediately through the chain of command

B. Files and related supporting documents preliminarily requested for a CJIS audit will be collected, reviewed for completion, and will be verified for accuracy prior to the arrival of the audit team.

C. In addition to collecting the files requested for an impromptu or scheduled audit, an appropriate date, time, and place will be agreed upon that will enable the audit team access to the Office; enabling them to examine records and documents consistent with approved security measures that do not serve to disclose or reveal to unauthorized persons the confidential materials of such investigatory files.

D. Upon appearing for the audit review, members of the CJIS audit team will be requested to present valid, and legally issued photographic identification; attesting and verifying their identity as legitimate audit team members so authorized access to the Office and access to investigatory files.

E. Accommodations will be made for the needs of the audit team; to consist of personal acclimation, technology access, telephone, fax, technical support, identified parking, or other reasonably required measures to assure their personal comfort, security, and access to required areas in the Office.

F. Audit team members will be granted a private, limited access work area with freedom of movement within the office, restroom, and file areas. Team members will initially be introduced to other employees working in the immediate area, and may be asked to both wear and prominently display an Office visitor's badge, or to externally wear their agency approved identification card so that it may be viewed by Office personnel.

G. Issues that relate to audit team members will be immediately reported to the Command Staff for resolution.

V. AUDIT REVIEW AND RESULTS

A. Issues identified by the audit team will be immediately addressed during the course of the audit if they can be readily explained or supported by documentation or policy.

B. All contact with audit team members will be courteous, polite, professional, and in a constructive manner that serves to further the audit examination and findings.

C. Initial dispute or question of records, policy, legal guidelines, or other elements of records research will be discussed and reviewed in an impartial manner; with discussion leading to an evaluation of the elements discussed to reach a fair, unbiased, and impersonal conclusion that is consistent with the legal guidelines and requirements of the audit.

D. Upon conclusion of the audit, the Support Staff member with primary authority for this process will be present with their supervisor or member of the Command Staff for the out briefing of the audit team.

E. Upon note of formal discrepancies in the out briefing, records and entries requiring immediate attention will be corrected without delay; with a member of the Command Staff compelling action on the part of the member responsible for the corrective action.

F. Upon receipt of any such formal audit team report that notes discrepancies or issues of policy or practice, such correspondence will immediately be acted upon to take corrective measures to bring all records into immediate compliance. These corrective measures will be a priority task for the member assigned this task.

G. Upon taking corrective action consistent with the audit findings, a response letter to the audit team will be prepared addressing the measures taken to correct the record deficiencies. This letter and description of corrective measures will be prepared and mailed not later than 10 calendar days after receipt of the official report of audit findings.

H. All correspondence relating to the notice of audit and audit findings – to exclude the confidential or restricted content of those records identified in the audit – will be maintained in the appropriate administrative correspondence file.

VI. Corrective Measures

A. Discrepancies that relate to the collection and accuracy of investigative report information will be directed through the chain of command for follow up action or training/re-training.

B. Errors that relate to the input of data, the failure of quality control measures, or the timely conformance to record input and maintenance will be directed to the person identified as having primary responsibility for the program. Issues that involve system knowledge, changes in practice, policy, or law will be identified in a training/re-training process. Successive or repetitive failures that are singularly identified to a specific person may result in the loss of program/log on access.

C. Discrepancies that are directly attributed to specific employees will be jointly reviewed with the employee and their supervisor. Identified corrective measures may include: procedural issues, training/re-training issues, legal guidelines and constraints, and the implementation and review of best practice processes. Employees who are consistently identified for audit process failures will be subject to progressive administrative discipline, and/or the penalties of law – or both - if such violations constitute a violation of law.

VII. Security Concerns

A. Records that relate to CJIS inquiries, inputs, or validations are considered controlled records and are to be safeguarded consistent with the restrictive and legal provisions that govern their access, use, review, and distribution. Dissemination by view or print records will be recorded in accordance with policy guidance or law.

B. Criminal records will never be placed in an investigatory file, left unattended, or be kept in an unlocked or unsecure file or environment.

C. Certain criminal records that pertain to restricted access confidential information (informants, etc.) will be maintained under a double locked, secured confidential information file under the immediate control of the Criminal Commander. When the purpose or use of these files has been achieved, the controlled documents in these files will be removed and destroyed by shredding, with a single page document then inserted into the file indicating the formal destruction of the records.

D. The access and dissemination of controlled CJIS records will always be noted and recorded, whether the file was printed or merely viewed. When requested or printed, such records and their need for access will become the sole ownership and administrative responsibility of the person who requested, possessed, or used such record in an investigation. If the request/query is self-generated, the obligation and responsibility for record accountability is then placed upon the person who accessed it.

E. The query and viewing of controlled CJIS records on authorized terminals is restricted to persons who either have CJIS access, or who are authorized to request, view, or receive such records. Terminals with CJIS access will not be placed in areas or in a manner that permits persons or the public to view or see the materials on the screen. Printers that are used to print controlled materials will be co-located with the CJIS access terminal. Printed CJIS materials will be recovered immediately and will not be left unattended on the printer.

F. When records are viewed, printed, or disseminated to persons for use in an authorized investigation, when the use or purpose of those records has been served, such records will be destroyed by returning them to the originator of the query/access if the holder is not that

person, or the records will be destroyed by shredding. Controlled documents and records will not be merely torn into pieces or thrown away in internal or external trash containers.

G. Persons who have access to and/or use CJIS records, to include persons who may service, install, or maintain CJIS terminals or periphery components will be responsible for understanding and conforming to the policy, rules, guidelines, and legal mandates that regulate the installation and use of CJIS systems. Periodic, documented training that relates to security indoctrination and routine familiarization of security measures associated with CJIS will be conducted.

H. All hardware associated with CJIS terminals will be inspected by trained and authorized personnel so having access prior to installation and at the de-commission of any CJIS terminal. At the time of de-commission, the hard drive and all components will be scrubbed by authorized Sheriff's Office personnel using licensed military grade software. In addition, the Talbot County Information Technology (IT) Department will verify the cleaning of the terminal and may provide a second scrub of the device(s).

I. When persons with CJIS access are involved in substantive personal or criminal matters, their access and log on to CJIS files and programs will be suspended until such time that the matter is resolved. While their access is suspended, such persons will not solicit or permit others with access to conduct queries for them, or to print and permit them to possess controlled CJIS records.

J. The failure to follow the legal and policy guidelines concerning the access, possession, use of CJIS, and the handling of controlled documents and information can result in administrative and/or criminal sanctions that could lead to or result in the possible loss of employment.

VIII. GUIDANCE

A. State and federal law that governs the access, use, handling, and storage of controlled documents and information form the basis for this directive. Administrative rules, operational policies, and the secure handling of CJIS materials and controlled documents form a sub-set of instruction and guidance in office operations. 28CFR as it applies to the collection of intelligence/informant information will govern the collection, use, access, storage, and retention of controlled documents in those files.

IX. EFFECTIVE DATE

This order is effective immediately and supersedes General Order No. 12-004, and all orders and memoranda, in conflict therewith.

Joseph J. Gamble
Sheriff of Talbot County

JJG:tj