



CRYSTAL POLICE DEPARTMENT

Department Policy Manual

TITLE: Criminal Justice Information (CJI)

NUMBER: 3.8

DATE: 07/06/2018

NO. PAGES: 3

PURPOSE

To formulate standard department policy and prescribe specific procedures to be followed in the handling of official criminal justice information (CJI) as defined and required by the Federal Bureau of Investigation and MN Bureau of Criminal Apprehension.

SCOPE

This policy will apply to all Crystal Police Department personnel and volunteers who have or may come into contact with criminal justice information.

DEFINITIONS

CJI DATA: the term used to refer to all data provided by the FBI criminal justice information systems, whether in digital or printed form. CJI data provided by the FBI can include, but are not limited to biometric data, identity history, biographic data, property data and case/incident history.

TERMINAL AGENCY COORDINATOR (TAC): serves as the point of contact at the local agency for matters relating to CJI access, and oversees the agency's compliance with CJIS system policies.

LOCAL AGENCY SECURITY OFFICERS (LASO): designated by the Chief of Police and is responsible for IT system access, security, incident reporting and documentation.

MANAGEMENT CONTROL AGREEMENTS (MCA): agreements with the Crystal Police Department and external government agencies that support, assist and/or possibly have unescorted to CJI data.

POLICY

PHYSICAL PROTECTION

Only Crystal Police Department employees and personnel covered by an active MCA will be allowed to have unescorted access to the Crystal Police Department. All others shall be escorted by authorized personnel at all times.

All access point to the Crystal Police Department will be secured, with electronic access controls and logging in place.

Information systems will be arranged in such a manner that they are not visible from non-secure areas.

MEDIA PROTECTION

Media containing CJI which needs to be protected can refer to digital media or physical media, and will be protected at all times until it is destroyed or disposed of in accordance with this policy. Access to CJI media shall be limited and controlled to allow only necessary and authorized individual's access.

Physical media shall be stored in a locked drawer, cabinet, officer or other designated securable storage area when not in use. Physical media being transported shall be protected from unauthorized viewing.

Digital media that contains CJI shall not be connected or accessed from non-agency owned and managed information systems equipment. Personally-owned digital media shall not be connected or accessed from Crystal PD's agency information systems if those agency systems contain CJI. Digital media shall be encrypted to NIST certified FIPS 140-2 standards when CJI is present if it is leaving a secure area.

Any loss or theft of CJI data shall be promptly reported to a supervisor and the LASO.

MEDIA DESTRUCTION & DISPOSAL

Digital media will be sanitized in accordance to NIST 800-88. Options for destruction/disposal including degaussing, shredding or physically destroying the media. A log of all digital media disposed of, and the disposal method, will be kept for at least one year.

Protected physical medial shall be destroyed by shredding when it is no longer required to be retained. Crystal PD personnel will escort any third-party agent who carries out document destruction until the disposal is complete.

INCIDENT RESPONSE

The Crystal Police Department will operate and respond to information systems incidents that potentially involve CJI data by following the City of Crystal Information Systems Incident Response Plan. The LASO will be primary point of contact between the Crystal Police Department and external agencies requiring notification in regards to any incidents that involve CJI data.

EVENT LOGGING

The Crystal Police Department information systems will maintain automatic logs of pertinent information system events as related to account and machine security. These logs will be maintained for a minimum of one year, and will be audited weekly for integrity.

AUTHENTICATION MANAGEMENT

The Crystal Police Department will follow all guidelines in the City of Crystal IT Policy in regards to password length, complexity and expiration.

User accounts will be disabled and/or removed immediately upon an employee's separation from the Crystal Police Department. The Crystal Police Department shall also conduct an annual review of all systems with CJI access, to ensure user accounts have been disabled or removed as necessary.

SECURITY ALERTS & PATCH MANAGEMENT

The LASO shall receive security alerts in regards to information system hardware and software. Using these alerts, the LASO shall patch systems and software after applicable testing has been conducted.

PERSONNEL SANCTIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment.