Protected Information

812.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Citrus Heights Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

812.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Citrus Heights Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

812.2 POLICY

Members of the Citrus Heights Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

812.3 RESPONSIBILITIES

The Chief of Police has selected the Support Services Supervisor to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS),Department of Motor Vehicle (DMV) records and California Law Enforcement Telecommunications System (CLETS).

(b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice’s current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

812.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Citrus Heights Police Department policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

812.4.1 PENALTIES FOR MISUSE OF RECORDS

It is a misdemeanor to furnish, buy, receive or possess Department of Justice criminal history information without authorization by law (Penal Code § 11143).

Authorized persons or agencies violating state regulations regarding the security of Criminal Offender Record Information (CORI) maintained by the California Department of Justice may lose direct access to CORI (11 CCR 702).

812.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to the Support Services Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Unit to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

812.5.1 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice (Penal Code § 11121).

Individuals shall be allowed to review their arrest or conviction record on file with the Department after complying with all legal requirements regarding authority and procedures in Penal Code § 11120 through Penal Code § 11127 (Penal Code § 13321).

812.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police has selected the Support Services Supervisor to oversee the security of protected information.

The responsibilities of this position include, but are not limited to:

(a) Developing and maintaining security practices, procedures and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.

(d) Tracking, documenting and reporting all breach of security incidents to the Chief of Police and appropriate authorities. See attachment: Protected Record Security Breach Response Plan - 2020.pdf

812.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

812.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination. This training shall be in the form of signing and acknowledging the confidential systems access forms that are disseminated annually in January.

812.8 CALIFORNIA RELIGIOUS FREEDOM ACT

Members shall not release personal information from any agency database for the purpose of investigation or enforcement of any program compiling data on individuals based on religious belief, practice, affiliation, national origin or ethnicity (Government Code § 8310.3).

Attachments

Protected Record Security Breach Response Plan - 2020.pdf

Protected Records Security Breach Response Plan

The Citrus Heights Police Department Protected Records Information Policy requires the tracking, documentation, and reporting of all breach of security incidents to the Chief of police and appropriate authorities (CHPD Policy 812.6(d)).

This protocol applies to a security breach any secured data base including, but not limited to National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records and California Law Enforcement Telecommunications System (CLETS).

1) Any department member or city employee who discovers the incident will immediately notify the Special Services Division Commander. If the Special Services Division Commander is unavailable, the on duty Watch Commander and Dispatch Supervisor should be notified.
2) The Special Services Division Commander, or their designee, will evaluate the incident and document:
    a) The name of the reporting department member.
    b) Time of the incident.
    c) The nature of the incident.
    d) What equipment or persons were involved?
    e) Location of equipment or persons involved.
    f) How the incident was detected.
    g) When the event was first noticed that supported the idea that the incident occurred.
3) The Special Services Division Commander, or designee, will assign an investigator(s) to evaluate the reported security breach and determine the following:
    a) Is the incident real or perceived?
    b) Is the incident still in progress?
    c) What data or property is threatened and how critical is it?
    d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    e) What system or systems are targeted, where are they located physically and on the network?
    f) Is the incident inside the trusted network?

g) Is the response urgent?

h) Can the incident be quickly contained?

i) Will the response alert the attacker and do we care?

j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

k) Is the equipment affected business critical?

l) What is the severity of the potential impact?

m) Name of system being targeted, along with operating system, IP address, and location.

n) IP address and any information about the origin of the attack.

4) The investigator(s) will work with Department Command Staff to determine a response strategy and response team as appropriate.

5) The incident and subsequent response shall be documented and forwarded to the Office of the Chief of Police. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.

b) Category two - A threat to sensitive data

c) Category three - A threat to computer systems

d) Category four - A disruption of services

6) The response team will establish and follow one of the following procedures basing their response on the incident assessment:

a) Worm response procedure

b) Virus response procedure

c) System failure procedure

d) Active intrusion response procedure - Is critical data at risk?

e) Inactive Intrusion response procedure

f) System abuse procedure

g) Property theft response procedure

h) Website denial of service response procedure

i) Database or file denial of service response procedure

j) Spyware response procedure.

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

7) They will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
8) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
9) Upon executive approval, the changes will be implemented.
10) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. (Preserve evidence before doing this).
    b) Make users change passwords if passwords may have been sniffed.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Be sure the system is fully patched.
    e) Be sure real time virus protection and intrusion detection is running.
    f) Be sure the system is logging the correct events and to the proper level.
11) Documentation—the following shall be documented:
    a) How the incident was discovered.
    b) The category of the incident.
    c) How the incident occurred, whether through email, firewall, etc.
    d) Where the attack came from, such as IP addresses and other related information about the attacker.
    e) What the response plan was.
    f) What was done in response?
    g) Whether the response was effective.
12) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
13) Criminal Investigation —complete a criminal investigation and notify appropriate external agencies if prosecution of the intruder is possible.
14) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
15) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
    a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

g) Have changes been made to prevent a new and similar infection?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?