CITY OF SAN RAFAEL
POLICIES AND PROCEDURES

Policy No.	
Subject:	SRPD CLETS Access Network Computer Use and Security
Resolution No.	N/A
Issue Date:	October 1, 2014
Revision Date:	
Prepared By	Gus Bush, IT Manager
Approved By:	Diana Bishop, Chief of Police

SRPD CLETS Access Network Computer Use and Security

PURPOSE:

The purpose of this policy is to supplement the City of San Rafael's computer use and security policy. The Department of Justice (DOJ) has specific system security requirements that must be met by any systems with access to the Department of Justice's (DOJ's) California Law Enforcement Telecommunication System (CLETS) data. This policy does not replace the City of San Rafael's computer use and security policy, it should be viewed as supplemental to it. This policy has been developed to meet or exceed the security requirements as outlined by the DOJ in the Criminal Justice Information Services (CJIS) Security Policy v5.

Policy:

All employees and systems with access to DOJ CLETS data will adhere to the security policies as prescribed by the CJIS Security Policy v5.

RESPONSIBILITY:
All City Departments, Divisions, and City Officials

REFERENCES:
Computer Use and Security Policy

Overview

The San Rafael Police Department's (SRPD's) sworn and professional staff utilize DOJ CLETS data to effectively perform their duties. SRPD uses desktop computers directly connected to the Police Department part of the San Rafael computer network. Additionally, each patrol unit is equipped with a mobile data computer and a wireless modem to connect to the SRPD part of the San Rafael network. The San Rafael network environment that provides connectivity to

DOJ CLETS data will herein be referred to as the "SRPD CLETS Access Network". The SRPD CLETS Access Network also provides CLETS connectivity for the law enforcement agencies of the Central Marin Police Authority, Fairfax Police Department, Ross Police Department, Marin Community College District Police Department, and County of Marin District Attorney's Office.

Policy Details

1. Access Controls

Requests for new network accounts will be documented in writing and submitted to the Information Technology (IT) office for processing. Once a network account is established, requests for access to specific departmental systems (including SRPD CLETS Access Network) may be made directly to the assigned system manager.

Departments will notify IT as well as the Police Support Services Supervisor when accounts are no longer needed, before departure or as soon as feasible afterwards. Accounts will be disabled (or passwords changed) immediately upon departure (or notification afterwards). Departments will normally have 30 days to determine disposition of new/remaining files/messages prior to account deletion.

Two factor authentication (such as biometrics, electronic tokens, etc) will be employed for any systems used outside of physically secure locations whenever accessing DOJ CLETS data.

Systems will display logon banners that provide information about security and privacy policies.

2. Security Authentication Requirements

All employees accessing the SRPD CLETS Access Network must use strong password protocols as outlined in CJIS Security Policy v5.6.2.1.1.

All passwords must:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

3. SRPD CLETS Access Network Equipment Requirements

All equipment accessing the SRPD CLETS Access Network must be Police Department issued equipment. The current environment does not support CLETS access from employee owned equipment.
All Equipment accessing the SRPD CLETS Access Network must satisfy the following requirements (CJIS SP v5.5.7.3):

1. Desktop and Mobile Data Computers
    i. CJI is only transferred between CJI authorized applications and storage areas of the device.
    ii. Fully supported personal firewall enabled.
    iii. Updated virus protection software.
    iv. Updated Spyware protection software.
    v. Security updates for operating system applied in timely/automatic manner.
    vi. Screen Saver password with timing less than 30 min.
    vii. Bluetooth disabled.
    viii. Wi-Fi disabled.
    ix. Equipment may never be connected to a network not expressly authorized by the Chief of Police.
2. Mobile Devices (Smart Phones, Tablets)
    i. Cellular connection always on. (facilitates Mobile Device Management (MDM))
    ii. Folder or disk level encryption enforced.
    iii. Screen Saver password with timing less than 30 min.
    iv. MDM with centralized administration capable of at least:
        1. Remote locking of device.
        2. Remote wiping of device.
        3. Setting and locking device configuration.
        4. Detection of "rooted" and "jailbroken" devices (which are not allowed on network).

4. Mobile, Personal, and Other Devices

At this time, Mobile devices (such as tablets, smartphones, digital cameras, etc.) and portable media (such as optical disks, flash storage, portable hard drives, etc.) may NOT be used to access or store data from the SRPD CLETS Access Network.

Personally owned devices (computers, mobile devices, portable media, etc.) may NOT be used to access the SRPD Network.

No unauthorized wireless access points, routers, hotspots, voice over internet protocol (VOIP) devices, or similar devices will be installed on the SRPD Network.

5. Computer Software

All software used on city-owned computers is to be loaded by City IT staff, or with express permission from IT staff. No personal software is to be loaded on city-owned equipment. No software, except updates from official websites associated with approved virus protection software and updates for approved business software, is to be downloaded from the Internet or other electronic sources without express permission from City IT staff. Any copying or distribution of city-owned software for non-City use is strictly forbidden.

6. Internet Web Site Access Permissions

SRPD CLETS Access Network is restricted to pre-approved Internet web sites. A list of pre-approved Internet web sites are located on the intranet e-page located at

Https:\\intranet.cityofsanrafael.org/PD

Additional Internet web sites may be requested by filling out a request form and forwarding to the San Rafael Police Department's Police Support Services Supervisor. The form will be reviewed and responded to within 60 days. The request form is attached to this document for your convenience.

7. Employee Security Awareness Training

All Employees utilizing the SRPD CLETS Access Network shall complete end user training. Employees will renew training on a bi-annual basis. A record of employee participation in training will be kept by the San Rafael Police Department Police Support Services Supervisor. This training is required by CJIS Security Policy v5.

Employee training will include:

1. How to access the network (log-in procedures).
2. How to utilize the services provided.
3. A review of Policy and Procedures in regards to the SRPD CLETS Access Network.
4. Security issues inherent in a mobile communication network. (virus, worm, spyware, etc.)
5. Network Security Incident Response procedures.

The City of San Rafael's IT Manager will review training materials on an annual basis and ensure it is current and relevant.

8. Incident Response

Users will notify IT immediately of any potential security incidents involving the City's network and/or computer systems (including but not limited to compromised passwords, virus/malware activity, unauthorized access, or physical loss/damage to City systems). IT will respond and document its response to potential incidents, determinations made, and corrective actions taken (if any). IT may establish automated response capabilities for resetting passwords, reporting spam, and similar low-risk situations.

The San Rafael Police Department, Police Support Services Supervisor and the City of San Rafael IT Manager must be immediately notified of any security breach to any network or device that has access to the SRPD CLETS Access Network (such as the network used to update MDTs, or any computer on the SRPD network). This includes virus infection, unauthorized password disclosure, or a detected system intrusion.

Provide the following information:

a. Incident date and time.
b. Point-of-contact.
c. Systems affected.
d. Nature of incident.
e. Actions taken.

An Incident Response form is attached to this document for your convenience

9. Violations
Violations of any provision of this policy by any individual or entity may result in disciplinary action up to and including dismissal and/or civil or criminal prosecution.

APPROVED BY:

Nancy Mackle

Nancy Mackle, City Manager

9/12/14

Date

IT Security Incident Response Form

DATE OF REPORT: _____ (mm/dd/yyyy)
DATE OF INCIDENT: _____ (mm/dd/yyyy)
POINT(S) OF CONTACT: _____ PHONE/EXT/E-MAIL: _____
LOCATION(S) OF INCIDENT: _____
SYSTEM(S) AFFECTED: _____
_____
METHOD OF DETECTION: _____
_____
_____
TYPE OF INCIDENT: _____
_____
INCIDENT DESCRIPTION: _____
_____
_____
_____
ACTIONS TAKEN/RESOLUTION: _____
_____
_____

Copies To:

Gus Bush
City of San Rafael
IT Manager
1400 5th Ave.
San Rafael, CA 94901
(415) 458-5302
Gus.Bush@cityofsanrafael.org

Charles Taylor
San Rafael Police Department
Police Support Services Supervisor
1400 5th Ave.
San Rafael, CA 94901
(415) 485-3088
394@SRPD.org

Internet Web Site Access Request Form

Date of Request: _____ (mm/dd/yyyy)
Requestor's Organization: _____
Requestor's Name: _____email:_____
Name of Internet Web Site name or URL Address:

_____
_____

What service does or Internet Web Site provide?

_____
_____

Requestor's Supervisor Name and Signature:

_____
_____

Copies To:

Gus Bush
City of San Rafael
IT Manager
1400 5th Ave.
San Rafael, CA 94901
(415) 458-5302
Gus.Bush@cityofsanrafael.org

Charles Taylor
San Rafael Police Department
Police Support Services Supervisor
1400 5th Ave.
San Rafael, CA 94901
(415)485-3088
394@SRPD.org

Request Approved or Denied: _____Date:_____
Reason for Denial: _____

_____
_____