California Exposition and State Fair Police Department
PHONE (916) 263- 3050 ★ 1600 Exposition Boulevard, Sacramento, CA 95815

DEPARTMENTAL GENERAL ORDER **ORDER № 3500.000**
July 2019 (New)

DATA BREACH INCIDENT RESPONSE PLAN
COMPUTER SOFTWARE SECURITY: PATCHING AND UPDATES
COMPUTER SECURITY AND PROTECTED INFORMATION
CLETS MEDIA HANDLING POLICY

3500.001 DATA BREACH INCIDENT RESPONSE PLAN

Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will define staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be made available to personnel whose duties involve data privacy and security protection.

The purpose of this document is to focus attention on data security and data security breaches and how the California Exposition & State Fair Police Department should respond to such activity. The California Exposition & State Fair Police Department is committed to protecting employees, partners and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly.

Background

This policy states that any individual who suspects that a theft, breach or exposure of California Exposition & State Fair Police Department Protected data or California Exposition & State Fair Police Department Sensitive data has occurred, must immediately provide a description of what occurred via e-mail to Helpdesk@CalExpo.com, or by calling 916-236-3083. This e-mail address and phone number are monitored by the California Exposition & State Fair's IT (Information Technology) Department. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the IT Department will follow the appropriate procedure.

Scope

This policy applies to all staff, employees, and contractors who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information from CLETS/DOJ/FBI resources, or any Protected Health Information (PHI) of California Exposition & State Fair members. Any agreements with vendors will contain similar language.

Confirmed theft, data breach or exposure of California Exposition & State Fair Protected or Sensitive Data

As soon as a theft, data breach, or exposure containing California Exposition & State Fair Protected data or Sensitive data has been identified and confirmed, the response will vary based on the facts of the incident.

Response

The IT Department, based on the nature and severity of the problem, will initiate a response to handle the breach or exposure.

Other Departments who may be informed or asked to assist are:

- Law Enforcement
- Human Resources
- Accounting
- Operations

Containment

- Removing personnel involved in the breach.
- Securing areas in which the breach took place
- Isolating the compromised or infected area and/or devices.

Remediation

- Remove malicious code or threat.
- Secure any unauthorized areas that were accessed as part of the breach.

Recovery

- Restore from backups if necessary.
- Ensure users change passwords, if appropriate.
- Ensure that the system is fully patched.
- Ensure real time virus protection and intrusion detection is running.

Communications

If necessary, work with California Exposition & State Fair (Cal Expo) Administration, the Chief of Police, and/or the Human Resources Department to determine the best method of disseminating information on the breach to:

- Cal Expo Management
- Cal Expo Employees
- Those directly affected.
- The public.

Documentation

The type and amount of documentation can vary greatly depending on the nature and severity of the incident. For moderate to severe breaches, a detailed report containing the following documentation will be compiled and shared with the appropriate Cal Expo departments:

- Description of what happened including how the breach was discovered.
- What was done to contain the problem.
- Steps taken to prevent future occurrences.
- Recommendations for updates to procedures or upgrades to equipment. to prevent future occurrences.

3500.002 COMPUTER SOFTWARE SECURITY: PATCHING AND UPDATES

CAL EXPO PATCHING

The purpose of this document is to provide supporting documentation regarding patching life cycle at California Exposition and State Fair, including the Cal Expo Police Department. This document will identify current patching policies.

SUMMARY OF CAL EXPO PATCHING

All professional licensed desktops/servers in N-Central receive operating system critical and security patches automatically. The scheduled maintenance window for Cal Expo is the third (3rd) Saturday of the month. Cal Expo does not have site wide third-party patching deployed at this time.

Cal Expo does not have a test or development network to test patches prior to installation. The Infiniti Team delays regularly scheduled patches up to five (5) days after an initial patch release for the Infiniti team to closely monitor regularly scheduled patches, and to be prepared to provide on-demand patching for critical vulnerabilities.

PATCH ADMINISTRATION

PATCH ON DEMAND

Patch on demand is a way to install patches on a device outside the scheduled patching maintenance windows. It provides the ability to schedule a one-time, non-recurring patch installation of outstanding approved patches to update outlying systems that are not reliably available, or for new devices added to the network. This enables Cal Expo / Infiniti Consulting Group to update a new device so that it meets system requirements for compatibility and security on a customer's network, without waiting for the next patch maintenance window.

Solarwinds N-central prompts devices to initiate patching at the scheduled time. If the device is unavailable, Solarwinds N-central continues to prompt the device until the maintenance window duration expires after 24 hours.

PATCH MANAGEMENT REPORTING

Solarwinds N-central reports provide summary and overview information on the status of patching for our customers. With the information from the reports, Cal Expo / Infiniti IT Staff can get a complete picture of the patching status for Cal Expo and identifies where deficiencies are occurring.

PATCH ROLLBACK PROCEDURES

If Infiniti Administrators determine that an approved patch should not be installed, the patch can be deleted from the Pending Patch Approvals list. This changes the patch to a state of *No Approval*. When deleting an automated patch approval rule, Solarwinds N-central provides an option to purge patches that are currently pending approval. Cal Expo / Infiniti can choose to delete these patches or keep them. Keeping patches that are pending approval means these approvals will execute once the configured delay time, at the time of deletion, has expired. Patches can also be rolled back manually on local machines.

PATCHING THIRD-PARTY SOFTWARE

The Windows agent communicates with the probe to determine what third-party applications can be updated. The agent obtains a list of applications from the probe and compares it to the software installed on a device. The agent determines which applications on a device need to be updated and sends the list of available software updates needed on the device to Solarwinds N-central to be approved by the Infiniti administrator.

The agent communicates with the probe to request the updates approved by the Infiniti administrator. The probe downloads the updates and patches from the third-party software vendor’s website and stores them on a local server on the network. Storing updates locally saves on speed and Internet bandwidth. At the configured time, the agent copies and installs the software updates from the network location.

SOLARWINDS MSP WINDOWS AND THIRD-PARTY PATCHING PROCESSES
WINDOWS UPDATES

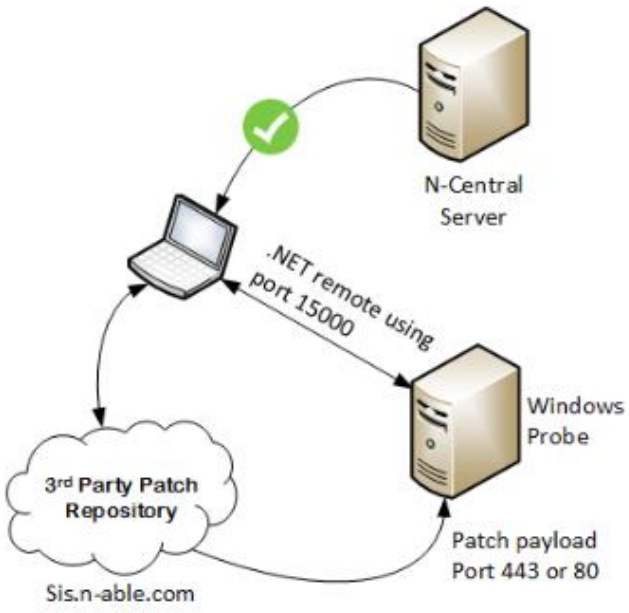
The Windows update workflow for downloading and installing the updates is:

- The agent communicates with the Windows Update server and requests a list of available updates.
- The agent sends the list of updates to the Solarwinds N-central server.
- The Infiniti administrator reviews the list of updates and sets the approvals for the list of possible updates. Solarwinds N-central notifies the agent which updates it can apply.
- The agent communicates with the probe to request the approved updates, or downloads them directly depending on the profile settings.
- The probe downloads the updates.
- The agent downloads the updates from the probe and applies the patches determined by the schedules defined by the Infiniti administrator.

THIRD PARTY UPDATES

The workflow to patch a device with third party updates is as follows:

- The agent retrieves a list of updates from sis.n-able.com and compares available third-party updates to the list of applications installed on the device.
- The agent sends a list of third party applications that need updating to Solarwinds N-central, where the Infiniti administrator has configured the approvals for the list of possible updates and notifies the agent which updates it can apply.
- The agent communicates with the probe and requests the approved software patches or downloads them directly from the source based on the profile settings.
- The agent downloads the updates from the probe and applies the patches determined by the rules defined by the Infiniti administrator.



35000.003 COMPUTER SECURITY AND PROTECTED INFORMATION

PURPOSE

This policy's purpose is to establish the security of the premises where computers (that contain confidential, restricted or protected information) are located; and to serve as a guideline for access, use and release of confidential, restricted or protected information for members of the California Exposition & State Fair Police Department. This policy does not cover information subject to the Public Records Act. Covered in this policy is any information which 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.

DEFINITIONS

Criminal Offender Record Information (CORI) is defined in 11075 Penal Code. CORI is a collection of arrest information stored in summary format. Included in CORI are the following:

- California Department of Justice RAP sheets.
- Automated criminal history information received from California DOJ via CLETS.
- Department of Justice computerized Criminal History System printouts (CHS).
- FBI and other states' rap sheets.
-

Note: Individual arrest, incident, and crime reports are not considered CORI, but their release is covered by the Public Records Act (Government Code §§ 6250-6260).

Right to Know: "Right to know" is the legal authority granted by statute or court order for a person or agency to access CORI. Those persons and agencies are described in Penal Code §§ 11105 and 13300, and listed in the Department of Justice Authorized Agencies List.

Need to Know: "Need to know" is defined as the official purpose for which information may be requested and used. "Need to know" is described in the Department of Justice Authorized List. Note: The "Right to Know" and the "Need to Know" must exist at the same time to justify access to CORI.

Administrative Assistant. An individual designated by the Chief of Police who is responsible for:

- 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).
- 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.
- 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.

- Developing procedures to ensure training and certification requirements are met.
- Resolving specific questions that arise regarding authorized recipients of protected information.
- Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.
- Reviewing/analyzing the computer system (including hardware, software, system users and data) audit records for indications of inappropriate or unusual activity; and investigating suspicious activity or suspected violations of policy.

POLICY

Members of the California Exposition and State Fair Police will abide by this policy as well as by all orders, laws, regulations, and user agreements related to access and use of CJI and confidential protected information. It is the responsibility of all employees to ensure the security of this information and comply with training standards. This includes but not limited to all information from:

- Department of Motor Vehicles (DMV).
- Criminal Justice Information System (CJIS).
- National Law Enforcement Telecommunications System (NLETS).
- California Law Enforcement Telecommunications System (CLETS).

COMPUTER SECURITY AND PROTECTION OF CJI AND CONFIDENTIAL PROTECTED INFORMATION

The California Exposition & State Fair Police Department has a responsibility to secure all CJI and confidential and protected information, and the computer(s) that are used to access that information. This includes maintaining security practices, training, and compliance with state and federal CJIS security policy and Criminal History systems.
The following security measures are in place to protect computer(s) used to access CJI:

a. CJI connected computer(s) shall be housed within a secure office within the secured Police Facilities Building on the grounds of the California Exposition & State Fair property.
b. The California Exposition & State Fair property is, in and of itself, a secure premises surrounded by gates, fencing, and access restrictions.
c. Within that property, the California Exposition & State Fair Police Department building is a separately secured, locked building with restricted key or security code access.
d. Keys and security code access are strictly controlled, and only authorized persons are issued keys or codes and allowed access to the building. The Chief of Police is the ultimate authority in the issuance of keys or access codes to the secured police building.
e. Within the secured police building and the secured Cal Expo property, the computer(s) with access to CJI is/are secured within a locked office on the upper floor of the police facilities building, adjacent to the office of the Chief of Police and the Records/Administrative offices.
f. When these offices are open during the day for public access, the facility is staffed by personnel that have been cleared for access to CJI.

g. This staff prohibits any unauthorized entry into the secure areas of the police facility, or escorts any person, employee or staff member who requires access to the policy facility (e.g. Maintenance staff, computer I.T. staff, mail room staff, and janitorial staff, visitors, etc.).
h. Within the locked office and the secured police building, within the secured Cal Expo property, computer(s) with access to CJI are further protected by:
i. Computer(s) are positioned in such a way as to prevent unauthorized individuals from accessing or viewing CJI.
j. Computer(s) are protected by password access to the physical desktop.
k. Passwords to computer(s) that can access CJI are only issued to those police department personnel who need access for the performance of their official duties.
l. Passwords expire every 60 days and must be renewed on a regular basis, and past passwords cannot be re-used.
m. Computer(s) time out, locking a user out of the session after a 30 minute period of inactivity.

Those authorized personnel who are allowed access to the computer(s) that can access CJI, are further issued an additional user ID and password in order to gain access to the Sacramento County Frontline Web Query system that provides access to the Sacramento County Justice Communication Hub which is linked to CLETS and other law enforcement databases. This final access to CJI is further protected by the following measures:

A welcome/warning screen notifying the user of the following:

"All system activity is monitored and all such activity is searchable and retrievable within the system. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. The mere use of the system constitutes consent to such monitoring for information retrieval for Law Enforcement and other purposes. All users shall have no expectation of privacy as to any communication on or information stored within the system. This includes information stored on the network, local computer or hard drive, or any other type of recordable media."

Passwords authenticate an individual's unique ID and meet the following requirements:
Minimum length of eight (8) characters that must include:

1. Capital letter(s).
2. Lower case letter(s).
3. Number(s).
4. Special character (!@#$%&*).

ii. Not a dictionary word or proper name.
iii. Not the same as the User ID.
iv. Expires within 90 days.
v. Cannot be identical to the previous ten (10) passwords.
vi. Not transmitted in the clear outside the secure location.
vii. Not displayed when entered.

ACCESSING CJI, CONFIDENTIAL AND PROTECTED INFORMATION

No CJI shall be accessed in violation of policy, law, regulations, user agreement or training. All employees must meet the following minimum standards prior to being allowed access to CJI:

Complete certified training contained with the Sacramento County Sheriff's Department's User Compliance website. This security awareness training shall be completed on a biennial basis and completion of the training will be documented via the User Compliance website.

Read, agree to, and sign an Employee/Volunteer Statement or a Sacramento Justice Portal User Agreement Form to document their understanding of the laws, restrictions, and responsibilities related to the access, use or misuse or restricted CJI. These documents will be scanned and stored within the User Compliance website.

Employees who access CJI via computer terminals shall complete, within the first six months of employment/assignment, a Full Access or Less Than Full Access Operator's Exam via the User Compliance website. Test completion results and scores shall be documented within the User Compliance website. CLETS testing will be conducted and completed on a biennial basis for all employees who continue to access CJI.

All employees who access restricted CJI shall be approved for access by the Chief of Police.

All employees must establish the "Right to Know" and the "Need to Know" for work related purposes prior to accessing CJI.

MISUSE OF RECORDS

Accessing CJI or confidential protected information without a legitimate work related purpose is a violation of this policy and may result in administrative and/or criminal prosecution. It is a misdemeanor to provide, possess, or sell any confidential protected information provided by the Department of justice Criminal Justice Information System without authorization per California Code 11143.

Each suspected incident of unauthorized or improper use of CLETS equipment or CJI, or of a failure to take physical security measures to protect CLETS equipment or CJI, may be investigated as a possible criminal violation and assigned for a detailed follow-up and investigation by administrative personnel as assigned by the Chief of Police.

Process for handling suspected misuse/abuse:

1. The Chief of Police shall assign a Lieutenant or Sergeant, or other command individual as a primary internal investigator.
2. This assigned Investigator shall have access to the resources of the Department's Administrative Assistant who is responsible for CLETS compliance. The Administrative Assistant shall provide data and information from criminal justice databases including journal processes to locate and document any and all computer access suspected to be in violation of this policy.
3. The assigned Investigator shall gather all pertinent information, interview any pertinent witnesses, and gather information from the suspected violator. When dealing with sworn Peace

Officers, the Investigator shall respect and follow all provisions of the Peace Officer's Bill of Rights in regards to conducting their investigation.

4. At the completion of the investigation, the assigned Investigator shall compile a detailed report containing all information gathered, and submit the package to the Chief of Police along with a recommendation for disciplinary action if appropriate.

5. Violations of this policy will result in disciplinary action consistent with established internal affairs investigations. Disciplinary action may include:

- The employee's loss of use or limitations on use of computer equipment.
- Removal from position, demotion, suspension, loss of rank or privileges.
- Criminal prosecution for any violation of criminal law or statute.
- Financial liability for the cost of any suit brought for improper use or violation of this policy.

3500.004 CLETS MEDIA HANDLING POLICY

All CLETS materials shall be handled, stored, and disposed of in compliance with the following procedure. All CLETS information received from the CLETS terminal (including criminal justice information from County, State, and FBI resources) shall be considered CONFIDENTIAL materials and will be handled with the utmost care to insure that only those individuals that have a "need to know AND the right to know" will access, handle, view, or dispose of these materials.

Only California Exposition & State Fair staff that have been fingerprinted and subjected to a background check are allowed to access, view, print, handle, store, destroy or otherwise be in contact with confidential CLETS materials.

PRINTED MATERIALS

Whenever possible, information from the CLETS terminal shall NOT be printed unless there is a valid law enforcement need for the printed document. Printed CLETS materials shall only be handled as follows:

- Printed CLETS materials shall only be stored in secure filing cabinets within the secure Police Facility building.
- If CLETS materials must be transported outside of the Police Facility (e.g. to court or to the District Attorney's Office), they shall only be handled, transported and possessed only by police personnel who have been fingerprinted, background checked, and approved for access by the Chief of Police.
- Printed CLETS materials shall be immediately destroyed once the documents are no longer needed, or no longer meet the "need to know AND right to know" criteria.
- All printed CLETS materials shall be destroyed via the cross cut shredder on the upper level of the Police Facility. NO OTHER shredders shall be used for the destruction of CLETS materials unless they meet the definition of cross cut or "confetti" shredders. "Strip cut" shredders are not to be used for the destruction of CLETS or other CONFIDENTIAL materials.
- Staff assigned to police administrative functions will be responsible for shredding CLETS materials on a regular basis, or at a minimum, weekly as necessary.
- Once CLETS materials have been destroyed and made un-readable via the cross cut shredder in the Police Facility, the subsequent shredded material may be disposed of via regular trash collection and disposal procedures.

ELECTRONIC MEDIA

Confidential CLETS data shall not be stored on any portable electronic media, including CD, DVD, flash drive, thumb drive or other media storage device. If any of these portable media devices are used to temporarily contain any CLETS materials, they shall be immediately destroyed by physically breaking the device, or where possible, CD's or DVD's will be destroyed via the cross cut shredder located on the upper level of the Police Facility.

Confidential CLETS data shall not be stored on any servers, hard drives or other electronic devices other than those developed and maintained by Cal Expo I.T. staff. In the event that servers or hard drives need to be replaced, they shall be securely erased using DOD approved methods, or the hard drive shall be physically destroyed by breaking or drilling the device to render it useless.