Computer and Mobile Device Equipment Security Brief

May 29, 2008

Presented by: Kevin G. Sutton, Chief, Information Technology Unit

About Confidential, Personal, and Sensitive Information

- CDPH considers all information about individuals private and confidential, unless the information is determined to be of public record.

- Examples of information that should not be disclosed include, but are not limited to:
  - Social Security Number (SSN)
  - Address
  - Phone Number
  - Driver's license number or State-issued identification card number
  - Account number, credit or debit card number
  - Medical information
  - Health insurance information

Mobile Device Equipment Security

Mobile device equipment presents a unique set of security concerns due to their portability. These devices include, but are not limited to:

- **Laptops**
- **Portable computers**
- **Personal Digital Assistants (PDA)**
- **Compact Discs (CD)**
- **Digital Video Devices (DVD)**
- **Flash drives**

Mobile Device Equipment Security

Contractors must consider the physical security of these devices and the protection of the confidential and/or sensitive information that is often stored on them.

Mobile Device Equipment Security

As a reminder, Contractors are responsible for:

- **The security of their assigned mobile device equipment and any confidential, sensitive, or personal information (data) that it may contain.**
- **Any subcontractors and consultants under Contractor's charge that utilize mobile device equipment purchased with *Network* funds and any confidential, sensitive, or personal information (data) that it may contain.**

Mobile Device Equipment Security (continued)

- Prior to being reimbursed for the purchase of mobile device equipment, Contractors will have to sign and return the “Contractor Mobile Device Policy, Procedures, and Guidelines” Agreement.
  - This document can be found in the Fiscal Section of the Guidelines Manual (Appendix).

Mobile Device Equipment Guidelines

The following guidelines are intended to help improve the protection of mobile device equipment.

Physical Security of Mobile Devices
Do's and Don'ts

- **Don't store your password with your mobile device.**
  - You should secure your mobile device with a strong password, but don't keep the password in the carrying case or on a piece of paper attached to the equipment.
- **Don't leave your mobile device in your car.**
  - Don't leave your mobile device on the seat or even locked in the trunk. Locked cars are often the target of thieves.
- **Don't store your mobile in checked luggage.**
  - Never store your mobile device in checked luggage. Always carry it with you.
- **Don't carry mobile devices in easily identifiable carrying cases.**
  - Particularly when traveling through airports, mobile devices should be kept in briefcases, backpacks, or other carrying cases that are not obvious.

Physical Security of Mobile Devices
Do's and Don'ts (continued)

- **Do secure your mobile device when unattended.**
  - Attach the mobile device with a security cable to something immovable or to a heavy piece of furniture when it is unattended (e.g. laptop).
- **Do keep track of your mobile device when you go through airport screening.**
  - Hold onto your mobile device until the person in front of you has gone through the metal detector. Watch for your device to emerge from the screening equipment.
- **Do record identifying information and mark your equipment.**
  - Record the make, model, and serial number of the equipment and keep it in a separate location. Consider having the outside of the equipment case labeled with your agency's contact information.
- **Do backup your files.**
  - Make a backup of your files before every trip. In the event that your mobile device is lost or stolen, you will still have a copy of your data.

Data Security on Mobile Devices

- If your mobile device contains confidential and/or sensitive information, do consider using a product that will encrypt the entire hard disk of your device, so that the device can not be accessed by anyone without a password.
- Insure that all files that reside on your mobile device are:
  - Regularly backed up to a secure server or other media (e.g. CD or flash drive)
  - Stored in a secure location
  - Encrypted
- Any mobile device that is lost, stolen, or damaged must immediately be reported to your assigned Contract Manager.
- Do use good judgment about the amount of confidential and/or sensitive data that you store on your mobile device. Only store data that will be needed while traveling.

About Encryption

What is encryption?

- Encryption is the coding of data so that it cannot be read by anyone who does not know the password that decodes it.
- Encryption garbles your data by using irreversible mathematical functions in order to make it nearly impossible to retrieve.

About Encryption (continued)

Why do I need encryption?

- **Data on nearly mobile device is vulnerable to accessibility, theft, loss, or damage. Protecting personal, confidential, and sensitive information is paramount and can easily be done through encryption. Even if your mobile device is stolen or accessed without your knowledge or permission, the encrypted information is useless to an outside user.**

Encryption Requirements

- **Contractors are required to install a virus protection application and a 128 bit hard drive encryption application on all laptops or tablet PCs.**
- **Contractors may use *Network* funds to pay for these applications, but costs must be prorated according to *Network* full-time equivalent (FTE) percentages.**

Reporting Mobile Device Theft, Loss, or Damage

The following is a step-by-step process in the event that your mobile device is stolen, lost, or damaged:

- **Immediately contact your assigned Contract Manager and the appropriate law enforcement agency.**
  - **Relay any information from law enforcement agencies, including police report number, to your Contract Manager. This information will be required for documentation of the incident.**
- **Your Contract Manager and other *Network* staff will notify appropriate State agencies about the incident and complete necessary reporting.**
- **Please make yourself available should your Contract Manager or other State staff need to contact you for more information.**

Closing

- **Thank you for reviewing this security brief and for proactively securing the mobile device equipment and confidential, sensitive, or personal information in your care.**
- **For additional questions, please contact your assigned Contract Manager.**