



Personally Identifiable Information (PII) Incident Security Guidelines

The FBI has named Identity Theft as the fastest growing white collar crime with 27.3 million victims in the last five years.

The purpose of this document is to provide guidelines and expectations for collecting and securing PII data on incidents. These guidelines should be utilized by all levels of incident management. The intent is not to give specific direction, but to identify areas needing special attention and some guidelines for how to collect and secure PII data. Each incident is different and will require different considerations and levels of security.

Personally Identifiable Information (PII):

PII is generally defined as information about or associated with an individual. Some of this personal information is very sensitive, while some is not considered sensitive when viewed as a single attribute. However, combinations of the information may create a situation where the sensitivity of the aggregate information warrants restrictions on its use and disclosure.

It may be difficult to define the level of sensitivity of every combination of PII. Therefore, good judgment must be exercised when handling PII in order to prevent disclosure. Sensitive PII, such as name and social security number (SSN), must be safeguarded at all times.

What data is PII?

Any combination of two or more of the following items can be used to compromise a person's identity.

- Name
- DOB/Place of birth
- Home address/phone number/email address
- Social security number
- Financial data
- Employment history
- Mother's maiden name
- Driver's license number
- Vehicle license number
- Non public use photos
- Fingerprints, DNA, iris scans
- Health information
- Criminal history

Expectations and Responsibilities:

Each incident should identify areas where PII data is vulnerable and take appropriate actions to secure that data. Managers must ensure each incident is engaging in the identified actions, while still understanding each incident will have unique challenges.

Employees should also consider their responsibilities in providing PII data. Do not supply non-crucial information on incident.

Areas to consider:

I-SUITE

The rules and guidelines for ensuring the protection and security of the I-SUITE database are outlined in the Access Control and Account Management Plan located on the I-SUITE website. This document

outlines the Access Control Requirements and Enforcement procedures for ensuring secure and approved access to the I-SUITE database. The guidelines also cover the procedures and policies for the CTSP to follow while administering the I-SUITE database to ensure the security and protection of PII data stored within the database.

http://isuite.nwcg.gov/library/I-Suite_Access_Control_Plan_Jan_2009.pdf

For a user to be issued an I-SUITE user name and initial password they must sign an acceptable use agreement form and a Statement of Information Security Responsibilities form provided by the team CTSP. In addition all users must take an annual agency security awareness training course before they are allowed into I-SUITE or onto any team computers. For ADs this training can be provided at the incident in the form of a CD or paper based training course.

In accordance with I-SUITE standard operating procedures, the I-SUITE database is uploaded to the I-SUITE repository upon an Incident Management Team's (IMT) demobilization from an incident. If the incident database is not complete, then an interim copy of the database is uploaded to the repository and the master database is transferred to the necessary location. The database and all backups are then deleted from any team devices. This includes the database master computer and any storage devices containing backups of the I-SUITE database.

Purging PII data from the database administration module is necessary when you need to create reports that may include PII data. A copy of the database is made, SSN's are purged and then the necessary report can be run.

COMPUTER PHYSICAL SECURITY

Each incident shall ensure laptops and any other hardware containing PII data is secured at all times. This may be achieved by locking up laptops when not being utilized, having security personnel monitor the area, or other appropriate means.

INTERNET ACCESS WITHIN INCIDENT COMMAND POSTS

There are inherent risks with any internet connection brought in to support an incident command post including broadband cellular cards, DSL, Cable, satellite or any other Wide Area Network Connection. At the network level all teams are equipped with a firewall router that sits between the team's network and the public internet. This separates all local area network communication, filters internet traffic, tracks all internet usage and provides an extra layer of protection from unauthorized access to the ICP network. Access to the ICP network is limited to agency laptops. Before any user accesses the ICP network they are required to sign an acceptable use agreement as well as a request for a user name and password, both for windows and for ISUITE. These forms are sent to and retained by Tyler Hackney once signed. Once a user has access to the system their data access is limited to the data folders necessary for their role. The policy of R1 Fire IT has been to coordinate with the section chiefs to determine who needs internet access in their unit and who should have it restricted.

If more specifics are needed on the configuration and security policies of R1 Fire IT please contact Tyler Hackney at (406)-329-4935.

HARD COPY PII

Incidents should identify what PII data is absolutely necessary to obtain from employees. The more data collected, the more data compromised. Check in forms should only require information needed for incident use and incident personnel should advise resources what information to provide. Only authorized personnel should have access to documents.

Finance sections should rarely have SSN's and/or Tax ID numbers (TIN) written down on paper copies. I-SUITE does require this information; however SSN's/TINs should never be copied and kept in the Finance package.

Planning sections should be cautious in obtaining information from resources. Often the paper documents kept in Planning are not secured the same as Finance. Planning should only require work addresses rather than personal addresses. Work data is not considered PII as it is public knowledge. Emergency information further compromises the resources' friends and/or family. Planning should identify how they will gather this information, if at all. Dispatch and the resource's home unit will have emergency contact information.

AD's: All hiring paperwork for AD's should be done by the sponsoring unit and documented as complete on each Casual Hire form. If all appropriate paperwork was completed prior to dispatch, PII data collected at incident can be minimal.

For AD's not having a "work" address, personal addresses should be kept to a minimum. AD's may opt to use the hosting agency or dispatch address.

Payment for FS AD's are processed at incident and only official OF-288's should have SSN written on them. DOI AD's paperwork is processed at the home unit therefore SSN's can be documented there.

DISPATCH

Dispatch accesses PII data on a daily basis when managing resources. Dispatchers must ensure the same safe-guarding is being done with PII data as all other functions on an incident.

Arranging flights for resources now requires full legal name, gender, and date of birth. Dispatch and the incident must identify a secure process to share this information.

RENTAL COMPUTERS

To ensure no PII data is present on a rental laptop when returned to the vendor, it is the policy of R1 Fire IT that all rental laptops are wiped before they are returned. The use of rental laptops on Region 1 IMT's is limited as each team is equipped with 30 agency laptops. Region 1 has also reduced the need for rental laptops in the expanded dispatch environment with an agreement setup with the ISO to use previously replaced laptops. These laptops allow expanded dispatch to be setup on the Forest Service network with users utilizing generic system access accounts for access to DS.

Long Term Storage of Incident Documents

Incident packages must be stored in an appropriate secure facility. Only authorized personnel shall have access to the packages. Each unit shall ensure the packages are purged of all unnecessary data in accordance to NWCG Records Management policy.

Attachments

Updated Check-In form

Signature: */s/ Mike McMeekin*

MIKE MCMEEKIN

Chair, Northern Rockies Coordinating Group

Date: 4/15/2010

CHECK IN FORM

Red Card Checked Entered into I-suite
 Resource information received and complete
 Initiate shift ticket AOV/POV
Checked in by: _____ (initials)

Request # _____ Incident #: _____
(O, C, E, A)

Resource Name: _____ Resource Designator (if Equipment, Engine or Crew): _____ **Resource Position/Kind:** _____
(Last, First) (PNF 617, Anderson WT #1) (DIVS, HC1, ENG6)

Agency: _____ **Check-In Date:** _____/Time: _____ **Travel Began Date:** _____/Time: _____
(FS, BLM, BIA, Contractors are PVT)

Home Unit Name: _____ **5-Letter Designator (MT-LNF):** _____ **Demob City:** _____, **State:** _____

Leader/Operator Name: _____ **# of People:** _____ **Manifest:** YES NO

Plans Information

Method of Travel (circle one): AIR AOV POV BUS PAS A/R

If Air: Jetport/Airport Name: _____ Jetport Code: _____
(3 digit code e.g. MSO, GEG)

If AOV, POV, BUS: Vehicle Description: _____
(Dodge PU, Chevy SUV)

Vehicle ID: _____ Mileage: _____
(Govt Vehicle #, License #)

If Rented, where was it rented from: _____

Who is responsible for payment: _____ Assigned E#: _____
(Dispatch, Buying Team)

If Passenger, who did you ride with: Name: _____ Request #: _____

Other Qualifications: _____

Were you reassigned directly from another incident? YES NO

If Yes: Original Request #: _____ Name of Incident: _____

First day of first assignment for calculation of 14-day tour: _____

Crew Type: Hotshot Type I Type II (IA) Type II (Other) Camp Crew

Engine Type: I II III IV V VI VII

Foam Capability: YES NO **CAFS:** YES NO

Equipment Make/Model: _____

Is there a Lowboy? YES NO

Sawyers - Faller Qualifications: Class A Class B Class C Professional

Finance Information

Federal Resource Other (State Overhead)
 AD (Casual Federal Hire) EFF (Casual State Hire)
 Cooperator (City, County, Rural)
 Contractor
 Equipment Engine Crew
 Copy of Agreement/Contract/EERA
 Pre-Inspection completed and attached
 Copy of Resource Order

Position Held on Incident: _____

Home Unit Address: _____

Home Unit Phone #: _____

Home Unit Fax #: _____

Dispatch Center Name: _____

Dispatch Center 24-hr #: _____

AD Employees Only

Is this your first assignment for the calendar year? YES NO

AD Hire Form copy attached? YES NO

AD Classification: _____ AD Pay Rate: _____

Hiring Agency Name: _____

Point of Hire: _____

ID Badge Authorizations (authorized to receive cache/supply items)
ID Badge Restrictions (circle all that apply): Laundry Nomex

Circle One: ALL ONLY SUPERVISORS
Commissary Medical Other _____ None