# Personally Identifiable Information (PII)
# Incident Security Guidelines

**(Updated 2016)**

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:**

**E-ISUITE**

e-ISuite has a web-based version (Enterprise) and a standalone version (Site). For access to the Enterprise version, users are required to have an NESS Application Portal (NAP) profile. NAP profiles may be requested at https://nap.nwcg.gov/NAP/#. Users of the Site version must sign an acceptable use agreement form and a Statement of Information Security Responsibilities form provided by the team ITSS before the user can be issued an e-ISuite user name and initial password. In addition, all users must take an annual agency security awareness training course before they are allowed into e-ISuite or onto any team computers. For ADs this training can be provided at the incident.

In accordance with e-ISuite standard operating procedures, at the end of the incident, an e-ISuite Data Transfer file will be created and the incident transferred from Site to Enterprise. As a safeguard, a backup file (.bak) will also be uploaded to the e-ISuite Data 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 e-ISuite database.

**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 (ICP)**

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 secure ICP network is limited to agency owned computers and equipment. Before any user accesses the ICP network they are required to sign an acceptable use agreement. If they will be utilizing a team provided device, a request for a user name and password, both for windows and for e-ISuite, must be completed. Completed forms are sent to and retained by Patrick Murphy, Northern Rockies Fire IT Specialist. Once a user has access to the system, their data access is limited to the data folders necessary for their role. The policy of Northern Rockies 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 Northern Rockies Fire IT, please contact Patrick Murphy at (406) 829-6940.

**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 SSNs and/or Tax ID numbers (TIN) written down on paper copies. This information may be required by the host Incident Agency payment processing, however SSNs/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.

ADs: All hiring paperwork for ADs should be done by the sponsoring unit and documented as complete on each Single Resource Casual Hire form. If all appropriate paperwork was completed prior to dispatch, PII data collected at incident should be minimal. ADs are encouraged to use their hosting agency or dispatch address and not their personal address. Payment for FS ADs are processed at incident utilizing the AD's Employee Common Identifier (ECI) number on the official OF-288s and not their SSN. DOI AD's paperwork is processed at the home unit therefore SSNs 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, the Northern Rockies Fire IT policy is that all rental laptops are wiped before they are returned. The use of rental laptops on Northern Rockies IMTs is limited as each team is equipped with 30-40 agency owned devices. Rental laptops may be utilized in the event that cached laptops are unavailable, though this should be the exception and will require close coordination with Northern Rockies Fire IT. Generic System Access Accounts (GSAA) will be utilized to provide access to Forest Service Laptops for short term users that do not possess a Forest Service Active Directory account. Security policies for the use and management of GSAAs are determined by the Forest Service CIO organization.

## COPY MACHINES/COPY SERVICE

Most copy machines have an internal memory; any photocopied PII would be stored in the internal memory. Work with team ITSS or equipment vendor to have internal memory erased before returning to vendor.

## 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: Ken Schmid Date: 5-31-16

KEN SCHMID
NRCG BOD CHAIR

CREW MANIFEST: Hand Crews: HC1 HC2 Contract Other: Engine

| | | | | | | |
|---|---|---|---|---|---|---|
| Res No. | Person's Name | Position (KIND) | AD | FED | Other (State) | Agenc i.e. BL |

Red Card Checked Entered into e-ISuite
Resource information received and complete
Initiate shift ticket AOV/POV Checked in by: ______

**Request #** ____________
**(O, C, E, A)** **Incident #:** ________________________________

**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:** _________

**FOR CREWS:** **Leader/Operator Name:** ____________________________ **# of People:** ___________ **Manifest:** YES NO

## Plans Information

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

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

**If AOV, POV, Rental:** Vehicle Description (make/model/color): _________________________

Vehicle ID: ___________________________
(AOV #, License #)

**If Rented**, where was it rented from: _______________________

**Who is responsible for payment:** _______________________ Assigned E#:__________
( Dispatch, Buying Team, or Driver via agency travel program)

**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:** Type 1 Type 2 IA Type 2 (Other) Camp Crew

**Engine Type:** 1 2 3 4 5 6 7 **Foam Capability:** YES NO **CAFS:** YES NO

**Equipment Make/Model:** ______________________Water Handling Eqmt **Tank Cap:** _____gallons

**Is there a Lowboy?** YES NO **Is Lowboy staying at incident?** YES NO

**Lights for Night Operations?** YES NO **Four-wheel Drive?** YES NO

**Sawyers - Faller Qualifications:** FAL1 FAL2 FAL3

## Finance Information

Federal Resource [FED]
State and Local Government [OTHER]
AD/Casual Federal Hire [AD] **Enter AD Information below**
**Contractor**
Equipment Engine Crew #People [____]
Copy of Agreement/Contract/EERA/Manifest
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: ________________________________

Home Unit Timekeeper (email): ___________________________

### AD EMPLOYEE INFORMATION ONLY

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

AD ECI # ___________________

AD Hire Form copy attached? YES NO

AD Classification: ______________ **AD Pay Rate: $**__________

Hiring Agency Name: ___________________________________

Point of Hire: _________________ Per Diem/Mileage: Yes - No

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | i.e. FFT1 | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |