CRIME VICTIM AND SURVIVOR SERVICES DIVISION
NOTIFICATION PROCESS FOR
BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

All sub-recipients must have written procedures in place to respond in the event of an actual or imminent breach of personally identifiable information (PII) if the sub-recipient creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of personally identifiable information within the scope of the subaward activities.

The breach procedures **must include a requirement to report actual or imminent breach of PII to the sub-recipient's fund coordinator no later than 24 hours after an occurrence** of an actual breach, or the detection of an imminent breach.

To Report An Actual or Imminent Breach:

1. **Compose email to your Fund Coordinator notifying of breach**
2. **Copy Grant Unit Manager, Kim Larson (kim.larson@ doj.state.or.us)**
3. **Complete and attach the form in Appendix A to email**

CVSSD will then notify our federal fund coordinators of the breach.

For purposes of this requirement

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Breach[1] means: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other-than-authorized purpose.

> A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment.
> A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive the information.
> It may also include an authorized user accessing PII for an other-than-authorized purpose.

[1] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017), available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf .

OREGON DEPARTMENT OF JUSTICE, CRIME VICTIM AND SURVIVOR SERVICES DIVISION

BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT FORM

	Date CVSSD Reported to Federal Program Manager:

General Information

Date of Breach:	Date Breach Discovered:	Date Reported to CVSSD:
Program/Organization Name:		

Point of Contact Information

Name:	Email address:	Telephone Number:
Mailing Address:		

Description of Breach: (NOTE: **Do NOT include PII**)

Text is limited to 1000 characters. If you need additional space, please continue in the blank sections at the end of the form.

Actions Taken in Response to Breach or Imminent Breach: (NOTE: **Do NOT include PII**)

Text is limited to 1000 characters. If you need additional space, please continue in the blank sections at the end of the form.

Number of Individuals Affected (if known, or approximate if not known): _____

Personally Identifiable Information (PII) Involved in this Breach (mark all that apply**)**

- ☐ Names
- ☐ Social Security Numbers
- ☐ Dates of Birth
- ☐ Personal e-mail addresses
- ☐ Personal home addresses
- ☐ Protected Health Information
- ☐ Passwords
- ☐ Financial Information
- ☐ Other (*specify):*

Select All that Apply to this Breach:

☐ **Paper Documents/Records**
- ☐ Paper documents faxed
- ☐ Paper documents mailed
- ☐ Paper documents disposed of improperly
- ☐ Unauthorized disclosure of paper documents

☐ **Email**
- ☐ Email was encrypted
- ☐ Email was sent to commercial account

☐ **Information Dissemination**
- ☐ Information was posted to internet
- ☐ Information was posted to an intranet
- ☐ Information was accessible to others without need-to-know on a share drive
- ☐ Information was disclosed verbally

☐ **Equipment**
- ☐ Location of Equipment
- ☐ Equipment disposed of improperly
- ☐ Equipment owner
- ☐ Govt Equipment - encrypted
- ☐ Gov't Equipment -password protected
- ☐ Personal equipment password protected or commercially encrypted

If Equipment, specify what type of Equipment:

_____

_____

_____

Please use this space to continue narrative on the description of the breach and/or actions taken in response to the breach or imminent breach.