SUBGRANTEE PROCEDURE

MONTANA BOARD OF CRIME CONTROL

EXAMPLE POLICY – REPORTING A BREACH OF PII

Subject: Example Policy – Reporting a Breach of PII	Page **1** of **2**
Effective Date: 05/07/2024	Revised:

I. Purpose

The purpose of this procedure is to outline the steps [your agency/organization] will take in the event of an actual or imminent breach of personally identifiable information (PII).

II. Definitions

Breach - 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.

Personally Identifiable Information (PII) - 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. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

III. Procedures

A. Reporting a Breach of PII

1. Per the MBCC Special Conditions, [your agency/organization] agrees to the following:

> Requirement to report actual or imminent breach of personally identifiable information (PII)
>
> The recipient (and any "subrecipient" at any tier) must have written procedures in place to respond in the event of an actual or imminent "breach" (OMB M-17-12) if it (or a subrecipient) – (1) creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of "Personally Identifiable Information (PII)" (2 CFR 200.1) within the scope of an OJP grant-funded program or activity, or (2) uses or operates a "Federal information system" (OMB Circular A-130). The recipient's breach procedures must include a requirement to report actual or imminent breach of PII to an OJP Program Manager no later than 24 hours after an occurrence of an actual breach, or the detection of an imminent breach.

Failure to comply with the above special condition may result in delay or suspension of funding.

2. [Your agency/organization] staff must report via email an actual or imminent breach of PII to their MBCC grant manager and the MBCC Director (nbowser@mt.gov) as soon as possible and no later than 24 hours after an occurrence of an actual breach, or the detection of an imminent breach. The report should include the following information:

    ☐ Date and time of the breach or detection of an imminent breach
    ☐ Description of actual or imminent breach
    ☐ Project number
    ☐ Project title
    ☐ Name of your agency/organization
    ☐ Contact information for your agency/organization

    Not sure who your MBCC grant manager is? See the Grant Programs and Contacts section on the MBCC Board Staff contact page: https://mbcc.mt.gov/About/Contacts

B. Remediation of Breach

[your agency/organization] will work with MBCC Staff to remedy the breach.

1. [your agency/organization] will document how another breach will be avoided and the policy or policies that have been created to protect another from another breach.

2. [your agency/organization] will provide remediation to MBCC and/or file the remediation file within the subgrantee file in AmpliFund.

3. MBCC Staff will ask to see a copy of [your agency/organization's] PII breach policy during the next scheduled monitoring visit or desk review. The policy should be tested and put into practice to ensure it is being followed.

4. If the breach is considered serious enough, the federal program manager may require MBCC to coordinate a monitoring visit or desk review sooner than the monitoring schedule determined by your subgrantee Risk Level. [Your agency/organization] will cooperate with MBCC to schedule the monitoring as soon as possible.

IV. Closing

Questions concerning this procedure should be directed to [title of individual responsible].

V. Attachments

Reporting a Breach of PII