

1.0 Title

No. 38.000 Rev. 0

Personally Identifiable Information

2.0 Effective Date

4/26/2007

3.0 Scope

This document establishes Policy guidance, Definitions, and Classes for the protection of Personally Identifiable Information (PII) at the Fermi National Accelerator Laboratory.

4.0 Applicability -

All Fermilab Employees

5.0 Policy-

General

All electronic copies of Protected PII will reside within an accreditation boundary protected at least at the moderate level. Protected PII is not to be downloaded to mobile devices (such as laptops, personal digital assistants or removable media) or to systems outside the protection of the accreditation boundary.

Waiver

If there is an operational or business need to store Protected PII outside the accreditation boundary (in particular on laptops and mobile devices) a waiver may be granted by the Designated Approval Authority (DAA). In instances where a waiver has been granted, the controls as specified by DOE CIO CS – 38 will be applied. In particular, encryption (FIPS140 – 2 compliant) will be used to protect PII and a 90-day review policy will be enforced.

Remote Access

If there is an operational need to access Protected PII data from outside the accreditation boundary an automatic disconnect after 30 minutes of inactivity will be enforced. In addition, 2-factor authentication will be required to access Protected PII.

Incident Reporting

Within 45 minutes after discovery of a real or suspected loss of Protected PII

data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

6.0 Definitions

PII is any information concerning an individual maintained by the laboratory, including but not limited to, education, financial transactions, medical history, and criminal or employment history that can be used to distinguish or trace an individual's identity. This may include information such as Social Security Number (SSN), date and place of birth, mother's maiden name, biometric records, as well as any other personal information that is or could be linked to an individual.

Classes of PII

The Lab has identified two types of PII as follows:

1) Public PII

Publicly available or *Public PII* is PII already available in public sources such as telephone books, public websites, business cards, university listings, etc. This PII includes, for instance, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. This category of PII will be referred to as Public PII and must be protected with at least NIST SP 800 -53 low-level controls.

2) Protected PII

Protected PII requires enhanced protection. This typically includes information that, if compromised by being left unprotected and/ or made available in any public manner, can cause serious or severe harm to an individual through Identity Theft or other unauthorized use/misuse of this information.

An individual's first initial and last name in combination with any one or more of the following data elements types of information including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts, requires enhanced protection.