Personally Identifiable Information Policy (PII)

KB0013870 - Latest Version

☆ ☆ ☆ ☆ ☆ 10 views

Personally Identifiable Information (PII) Policy

1. Purpose

The purpose of this policy is to establish guidance, definitions, and classes for the protection of personally identifiable information (PII) at the Fermi National Accelerator Laboratory (Fermilab).

2. Scope

This policy applies to all information stored on all systems managed by Fermi Research Alliance, LLC (FRA) and all systems connected to the Fermilab network, whether FRA-managed or not.

3. Applicability

This policy applies to Fermi Research Alliance, LLC and all its employees, Fermilab users and affiliates, authorized guests, and subcontractors and their employees.

4. Effective Date and Date Reviewed/Updated

This policy went into effect on April 26, 2007, and its update was effective on April 19, 2022.

5. Policy

All PII must be handled and protected appropriately. The sensitivity of PII increases when combinations of elements increase the ability to identify or target a specific individual.

All electronic copies of High Risk PII (as defined in Section 6) will reside within an accreditation boundary protected at least at the NIST SP 800-53 moderate level. High Risk 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.

If there is an operational or business need to store High Risk PII outside the accreditation boundary (in particular on laptops and mobile devices) a waiver must 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.

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

High Risk PII must be given greater protection and consideration because of the increased risk of harm to an individual if it is misused or compromised. A suspected or confirmed breach of High Risk PII must be immediately reported to the Fermilab Cyber Incident Response Team following the procedures under “Incident Reporting” in the Fermilab Policy on Computing (https://cd-docdb.fnal.gov/cgi-bin/sso/ShowDocument?docid=1186). The Incident Response Team will handle such reports as a “Class A” incident under the Cyber Incident Response Procedures (https://cd-docdb.fnal.gov/cgi-bin/sso/ShowDocument?docid=1162).

Procedures for handling and storage of High Risk and Non-High Risk PII are found in the document Procedures Implementing the PII Policy (https://cd-docdb.fnal.gov/cgi-bin/sso/RetrieveFile?docid=2134&filename=PII%20Procedures-final.pdf).

6. Definitions

Personally Identifiable Information (PII): PII, as defined in DOE Order 2016.1 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII can include unique individual identifiers or combinations of identifiers, such as an individual’s name, Social Security number, date and place of birth, mother’s maiden name, biometric data, etc.

Non-High Risk PII: One of two types of PII identified by the lab. Publicly available or Non-High Risk PII may include 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 Non-High Risk PII and must be protected with at least NIST SP 800 -53 low-level controls.

High Risk PII: One of two types of PII identified by the lab. PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples include, Social Security Numbers (SSNs), biometric records (e.g., fingerprints, DNA, etc.), health and medical information, financial information (e.g., credit card numbers, credit reports, bank account numbers, etc.), and security information (e.g., security clearance information).

Breach or Data Breach: An incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

a. A person other than an authorized user accesses or potentially accesses PII; or
b. An authorized user accesses or potentially accesses PII for other than the authorized purpose.

Breaches do not require evidence of harm to an individual, or of unauthorized modification, deletion, exfiltration, or access to information. PII can be breached in any format, including physical (paper), electronic, and verbal/oral.

Accreditation Boundary: All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3. (NIST SP 800-18r1). Also known at Fermilab as the "major application boundary."

Designated Approval Authority (DAA): Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (NIST SP 800-18r1)

Fermi Research Alliance, LLC is the operator and manager of the Fermi National Accelerator Laboratory under Department of Energy Prime Contract No. DE-AC02-07CH11359 and is the principal employer of personnel working at Fermilab.

For the purpose of this document, Fermi National Accelerator Laboratory may be referred to as "Fermilab" or "laboratory."

7. Responsibilities

The Fermilab Director is responsible for all programs related to this policy.

The Chief Information Officer is responsible for ensuring that this policy is current and that there is effective and consistent implementation and adherence to the requirements highlighted in this policy across Fermilab.

Chiefs, Division, and Section Heads and Project Directors are responsible for ensuring that all requirements highlighted in this policy are effectively and consistently implemented and communicated with full adherence within their organizations.

FRA Employees, Fermilab Users, Visitors, Authorized Guests, Subcontractors, and their Employees are responsible for adhering to this policy and supporting all processes associated with this policy.

8. Authorities

DOE O 206.1 Chg1 (MinChg), Department of Energy Privacy Program (https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg)
Fermilab Policy on Computing (https://cd-docdb.fnal.gov/cgi-bin/sso/ShowDocument?docid=1186)
Policy on Information Classification and Access (https://fermi.servicenowservices.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3Dda00edbd1bef70100a91eb5ce54bcb3c)
Cyber Incident Response Procedures (https://cd-docdb.fnal.gov/cgi-bin/sso/ShowDocument?docid=1162)
NIST SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems (https://doi.org/10.6028/NIST.SP.800-18r1)
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-53r5)
FIPS 140-3 Security Requirements for Cryptographic Modules (https://csrc.nist.gov/publications/detail/fips/140/3/final)
DOE CIO CS-38

9. Owner

The Chief Information Officer is the owner of this policy.

10. Review Cycle

This policy shall be reviewed every 2 years.

11. Communication Plan

The requirements of this policy shall be communicated by the Chief Information Officer to all employees, users, and affiliates. This policy shall be available in the Fermilab Policy Database.

Revised by Marcia Teckenbrock
Last modified 2022-04-20 15:11:32

Was this helpful?