Information Categorization and Access Policy

KB0014160

☆ ☆ ☆ ☆ ☆ 20 views

Information Categorization and Access

1. Purpose

This policy establishes information categories, the criteria for classifying information into one of these categories, and how information in each category must be accessed and protected.

2. Scope

This policy applies to all information stored on all Fermilab-managed systems and all systems connected to the Fermilab network, whether Fermilab-managed or not.

3. Applicability

This policy applies to Fermi Research Alliance, LLC (FRA) 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 May 14, 2010 and its update was effective on Nov. 1, 2021.

5. Policy

Fermilab uses four broad categories to regulate access to and determine other treatment of information. These are:

Level 1: Open Access information
Level 2: Limited Access information
Level 3: Restricted Access information
Level 4: Secure Access information

Level 1: Open Access Information

Information in this category is open to the public, and there are no specific access restrictions placed on this information.

Open access information does not require authentication, can only be served to the public from the public hosting zone (which could include various services such as public SharePoint, public DocDB, public Indico, or public web servers), and will undergo content review to ensure suitability and for public access. Regardless of the location of the data, the owner of open access information is responsible for ensuring that appropriate backup procedures are in place to allow for information recovery in the event of hardware, software, or human errors.

Any information in this category must meet the following requirements:

- There must be a statutory or regulatory requirement to make this information publicly available, or it must be important to the laboratory mission to make this information publicly available. Examples of the latter include but are not limited to profiles of laboratory community members, and information about the laboratory and laboratory environment, our science, and our research, projects, and experiments.
- The information must undergo a content review by the Information Manager or delegate to determine suitability for public distribution.
- The information must be scanned for presence of sensitive information, including but not limited to personally identifiable information (PII), controlled unclassified information (CUI), export-controlled information, intellectual property, and sensitive research technology information. Any such information must be redacted or suitably protected before public posting.
- An Fermilab employee (owner) must take responsibility for the content, and this responsibility must be renewed annually. Any information without an active owner will be removed from public access.

Open access information can only be served from the public hosting zone. Information intended to be shared with the public cannot be served from the internal (non-public) Fermilab network or from a server that contains any Level 2, 3, or 4 information.

Note that information in this category does not need to be available to anyone just by clicking. Access to some information may require the recipient to supply an email address or other information before the information is provided to them.

Level 2: Limited Access Information

This category includes information whose loss or disclosure could result in only limited harm, but whose owner still desires to limit access to certain classes of individuals. Examples of information in this category include but are not limited to budget, financial or property information, prepublication scientific results, information that could cause embarrassment if taken out of context, or training records.

Access to information in this category is limited, not to specific individuals, but rather to broad classes of individuals (for example all lab employees, all members of a particular experiment, or all members of a particular organizational unit). It is the responsibility of the owner to determine if some information in their responsibility falls into this category and, if so, to institute the necessary access restrictions.

Note that level 2 information requires authentication for access and cannot reside in the public access zone where information is available to the public without authentication.

Level 3: Restricted Access Information

This category includes information whose loss or improper disclosure could result in significant harm to the laboratory or to individuals. Examples of such information include but are not limited to proprietary vendor information, vendor bids, pre bid evaluations, performance appraisals, salaries, or security plans.

While the laboratory will offer guidelines and examples of types of information falling into this category, it is the responsibility of the owner to determine if certain information in their responsibility falls into this category.

Access to information in this category must be restricted to specific individuals with a specific business need for access, and at all times the owner will maintain a list of all such authorized individuals. A variety of technical means can be used to ensure that anyone not on this list will be unable to access the information. In addition, the information owner may impose additional protection mechanisms or procedures as appropriate, but the primary means of protection is expected to be tight access control. Those individuals granted access to information in this category will be trained on the proper handling of this information, in particular about disclosure of this information to unauthorized individuals.

Note that level 3 information requires authentication for access and cannot reside in the public access zone where information is available to the public without authentication.

Level 4: Secure Access Information
This category includes information which is specifically identified in statute or DOE order as requiring special protection. Examples of such information include but are not limited to High Risk Personally Identifiable Information (PII), Official Use Only information (OUO), and medical records governed by HIPPA statutes.

The standards for determining what information falls into this category are uniform across the laboratory (and in many cases are set by external regulations or orders). All types of information in this category have specific procedures in place maintained by the Information Manager describing what information falls into this category, how access to this information is controlled, and what practices must be followed in the use or transmission of this information. In all cases access is restricted to those individuals who have a specific business need to access this information, and all such individuals must receive specific training about handling such information, and in particular, about the standard lab wide procedures governing access and use of information in this category. In most cases there will be additional restrictions about where such information can reside, encryption, and reporting of any loss or compromise of such information.

Note that level 4 information requires authentication for access and cannot reside in the public access zone where information is available to the public without authentication.

Exceptions

Any exceptions or equivalencies from this policy must be approved by the Chief Information Officer.

6. Definitions

For the purpose of this document, Fermi National Accelerator Laboratory may be referred to as "Fermilab" or "laboratory." Additionally, to make the policy easily understandable, although Fermilab is a place and not a legal entity or an employer, Fermi Research Alliance, LLC (FRA) employees are referred to as Fermilab employees.

Controlled Unclassified Information (CUI): Information that law, regulation or government-wide policy requires to have safeguarding or disseminating controls excluding information that is classified.

Export-Controlled: Any item, material, software, or technology designated on the Commerce Control List (CCL) of the EAR, the U.S. Munitions List (USML) of the ITAR, or DOE policies, orders, and any other export control laws.

Level 1: Open Access Information: Information in this category is open to the public, and there are no specific access restrictions placed on this information.

Level 2: Limited Access Information: This category includes information whose loss or disclosure could result in only limited harm, but whose owner still desires to limit access to certain classes of individuals.

Level 3: Restricted Access Information: This category includes information whose loss or improper disclosure could result in significant harm to the laboratory or to individuals.

Level 4: Secure Access Information: This category includes information which is specifically identified in statute or DOE order as requiring special protection.

Official Use Only (OUO): Certain unclassified information that may be exempt from public release under the Freedom of Information Act and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities.

Personally Identifiable Information (PII): 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 is further defined and classified in the *Personally Identifiable Information (PII) Policy* (https://fermi.servicenowservices.com/kb_view.do?sysparm_article=KB0013870).

Public Hosting Zone: computing and network infrastructure provided by Computing which isolates publicly available Level 1 Open Access Information from Level 2, 3 and 4 information.

7. Responsibilities

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

FRA 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.

FRA 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.

Information Manager: The head of the Core Computing Division Information Resources Department is, ex officio, the Information Manager and is responsible for review and determination of suitability of distribution to the public of level 1 information before it is placed in the public access zone.

Owners of information are FRA Employees who are responsible for categorizing that information and applying information protections appropriate to the level of categorization.

FRA Employees, Fermilab Users and Affiliates, Visitors, Authorized Guests, Subcontractors, and Employees of DOE-FSO are responsible for adhering to this policy and supporting all processes associated with this policy.

8. Authorities

DOE O 205.1C, Department of Energy Cyber Security Program
DOE O 470.4B Chg 2 (MinChg), Safeguards and Security Program
DOE O 206.1 Chg1 (MinChg), Department of Energy Privacy Program
NIST Special Publication 800.53B Control Baselines for Information Systems and Organizations
Fermilab Policy on Computing
Fermilab Personally Identifiable Information (PII) Policy
Fermilab Web Governance Policy
Fermilab Policy on Export Control
Fermilab Policy on Official Use Only Documents

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.

Authored by Marcia Teckenbrock
Last modified 2021-11-01 11:55:54

Was this helpful?