

Fermilab Policies on Information Categorization and Access

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

- Level 4: Secure Access data
- Level 3: Restricted Access data
- Level 2: Limited Access data
- Level 1: Open Access data

This document describes how data is determined to fall into one of these categories, and how data in each category must be treated.

Secure Access Data

This category includes data which is specifically identified in statute or DOE order as requiring special protection. The standards for determining what data falls into this category will be uniform across the laboratory (and in many cases are set by external regulations or orders). All types of data in this category will have specific procedures in place describing what data falls into this category, how access to this data is controlled, and what practices must be followed in the use or transmission of this data. In all cases access will be restricted to those individuals who have a specific business need to access this data, and all such individuals will receive specific training about handling such data, and in particular, about the standard lab wide procedures governing access and use of data in this category. In most cases there will be additional restrictions about where such data can reside, encryption, and reporting of any loss or compromise of such data. Examples of such data are Protected Personally Identifiable Information (Protected PII), Official Use Only information (OUO), and medical records governed by HIPPA statutes.

Restricted Access Data

This category includes data whose loss or improper disclosure could result in significant harm to the laboratory or to individuals. While the laboratory will offer guidelines and examples of types of data falling into this category, it is the responsibility of the data custodian to determine if certain data in their responsibility falls into this category. Access to data in this category must be restricted to specific individuals with a specific business need for access, and at all times the data custodian 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 data. In addition, the data custodian 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 data in this category will again be trained on the proper handling of this data, in particular about disclosure of this data to unauthorized individuals. Examples of such data include proprietary vendor information, vendor bids, pre bid evaluations, performance appraisals, salaries, security plans, etc.

Limited Access Data

This category includes data whose loss or disclosure could result in only limited harm, but whose data custodian still desires to limit access to certain classes of individuals. Access to data 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 data custodian to determine if some data in their responsibility falls into this category and, if so, to institute the necessary access restrictions. Examples of data in this category include budget, financial or property information, pre publication scientific results, information that could cause embarrassment if taken out of context, training records, etc.

Open Access Data

Data in this category is open to the public, and there are no specific access restrictions placed on this data. As for all other levels of data, the data custodian is still responsible for ensuring that appropriate backup procedures are in place to allow for data recovery in the event of hardware, software, or human errors.