


Granting Data Access Rights

 **DM-4442** - IAM process for granting data access rights DONE

This page proposes a draft process for granting of data access rights to LSST users according to the [Data Access White Paper](#) and recent discussions: [Data Access Rights](#) and [Data Access Rights and Policies](#) and [Notes on Assigning Data Rights for US Astronomers](#).

A [LSST Data Access Policy Working Group](#) has been formed and a [document drafted](#), LPM-261.

The goals for the process are:

- Minimize manual steps for LSST users and staff (e.g., grant data access rights automatically based on campus attributes when possible).
- (Something about balance between false positives and false negatives?)
- ...

People who have data rights:

- national "professional astronomical community" (US, Chile) (possibly France?)
 - when US community members submit a proposal to the Observatory Resource Allocation Committee for Level Elevation (ORACLE), do all proposal participants need to already have data rights or can the proposal process grant data rights?
- named individuals from international partners
- a limited number of designated additional individuals (post-docs, grad students) per named individual

Granting data rights based on campus attributes:

- National federations follow the eduPerson (<http://macedir.org/specs/eduperson/>) attribute standard
- <http://macedir.org/specs/eduperson/#eduPersonScopedAffiliation>
 - faculty, student, staff, alum, member, affiliate, employee, library-walk-in
 - member is faculty or staff or student or employee (not alum) i.e., "member in good standing of the university community"
- no "astronomer" attribute, departmental affiliation not well supported
- proposed: member@example.edu in national federations (InCommon, Chile COFRé) has data rights
- include post-docs/grad-students as members by default?

Granting data rights based on LSST review:

- For example, if user's home campus doesn't have an InCommon (Shibboleth) identity provider
- User clicks "apply for data access rights" button
- LSST review:
 - automated based on (verified) email address?
 - .edu TLD is "U.S.-accredited educational institutions" with some grandfathered exceptions
 - .cl TLD open to anyone
 - check campus directory info

Granting data rights based on named individuals:

- matching email addresses
 - email attribute from campus identity provider or verified by LSST sign-up process
- email-based invitation process
 - invite "named individuals" to create LSST account if they haven't already or add data rights to existing account

Granting data rights to designated additional individuals:

- anyone with data rights can add others? or only "named individuals"?
- email-based invitation process
- "people picker" - find individuals to grant data rights to
- limited number: who will control this policy

Maintaining data rights:

- Periodic (annual) re-validation of "designated additional individuals"
- de-provisioning of data rights?
 - "Once a scientist has data access, they don't lose it even if they change institutional affiliations."
 - faculty change of institution: leaving USA
 - what happens when student graduates?