**Members: Members:** Steve Cramer, Peg Eusch, Lee Konrad, Peter Goff, Jan Greenberg, Martha Kerner, John Lucas, Nancy Lynch, Jocelyn Milner, Tena Madison, Scott Owczarek, Umberto Tachinardi, Bob Tuner, Mark Walters, and Jason Fishbain

**Attendees:** Peter Goff, Lee Konrad, Nancy Lynch, Tena Madison, Jocelyn Milner, Scott Owczarek, Jan Greenberg, Mark Walters, and Jason Fishbain

**Data Stewardship Council Meeting Minutes**

**Tuesday, April 26, 2016**

**8:30 – 10:00 AM**

1. **Review/Approve Last Meeting Minutes (Jason Fishbain)**

* The March 22, 2016 meeting minutes were motioned and approved by the committee.

1. **Update from the Steering Team (Jason Fishbain)**

* The Vice Chancellor of Research and Graduate Education asked that someone represent the interests of Graduate Education & Research on the Data Stewardship Council.
  + Jan Greenberg has joined the Data Stewardship Council.
* Items proposed to the Steering Team:
  + Steering Team would like for ORCID ID Proposal to move forward in assigning ORCID IDs to the university’s research groups.
  + Steering Team suggest that the scope of the Access to Restricted Data Policy focus on Administrative Restricted Data. Steering Team is comfortable with the direction of the Policy and would like for it to move forward.

1. **Continue Discussion around Access to Restricted Data Policy (Jason Fishbain/Scott Owczarek)**

* The Board of Regents charged David Miller, David Stack and a team of Security SME’s to create a Security Program for UW-System. Included as part of that program is the creation of policies around securing systems and data.
  + If UW-Madison can adopt it’s own policy language ahead of UW-System, we can help guide the policy creation for the UW-System.
  + There are doubts that having generic UW-System policies will work/fit for all UW-System institutions.
* Purpose of the Access to Restricted Data Policy is to have a minimal standard regardless of the data domain (each of which may have additional standards that would be necessary to meet).
  + Users who request access to Restricted Data should have a job role need or a business purpose for that access A separate policy will be formed around Research-Restricted Data.
* Suggested changes to the Proposal for a UW-Madison Restricted Data Authorization Policy:
  + For number 1 section C of the proposal around Restricted Data, not using the term: “ on the behalf of UW-Madison”.
  + Investigate if the researcher is using data on the behalf of the UW-Madison or if the data is being used for institutional purpose.
    - To-Do. Nancy will help Jason with the rewording of C.
  + Stating “Restricted Administrative Data Policy” in the title.
  + Stating in policy that Research Restricted Data will be included as part of a separate policy. Distinguishing the difference between institutional Restricted Data and Research Restricted Data.
  + Stating that other policies will follow around restricted data domains of Institutionalized Data versus Research Data.
  + Also, making clear that researchers would need to take similar training to understand their responsibilities of using institutionalized data. FERPA allows researchers to use institutionalized data and states that the user needs to responsible of the data.
  + The scope is not to get into outlining on what users will use the data for, which is what the IRB’s function is (for researchers).
    - Eventually, procedures will need to be outlined.
  + A framework will need to be outlined on how users will get access to restricted data and how to audit who has access who no longer needs access to restricted data.
  + Policy Principle #6 speaks to exceptions to the process of gaining access to restricted data. The Data Stewardship Council said exceptions should be brought to them and system owners should not be in charge of making this decision. The Data Stewardship should be the ones to sign off on the exception cases.
    - Looking at expanding to have warranties/confidentiality agreement clause for general awareness.
  + Having the Data Stewardship handle granting access to restricted data and the Steering Team will be held accountable.
  + Making sure there is a business purpose for users to have access to full or partial SSNs.
  + The Data Stewardship has suggested that violators of these polices should a bare minimum should lose access to the restricted data.
  + The Data Stewardship will be responsible in implementing these policies and socializing them around campus.