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

**Attendees:** Steve Cramer, Peg Eusch, Peter Goff, Martha Kerner, Lee Konrad, Scot Owczarek, Tena Madison, March Walters, and Jason Fishbain. **Guest:** Kay Steiner and Stefan Wahe

**Data Stewardship Council Meeting Minutes**

**Tuesday, February 23, 2016**

**8:30-10:00 AM**

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

* The January 26, 2016 meeting minutes were motioned and approved by the committee.

1. **InfoAccess Usage (Jason Fishbain/Kay Steiner)**

* Kay is the manager of InfoAccess Team.
* InfoAccess Service is a Data Warehouse that stores student information mainly containing ISIS Data, which would include enrolled students, graduates, ect. It also stores housing information, budget for UW-System and a little historical HR information is stored in it.
* There is a broad spectrum of use of InfoAccess..
* Kay presented usage statistics to the Council. On average, there are between 140 & 175 distinct accounts that use InfoAccess each month.
* There is no policy today that governs the removal of users from InfoAccess
* Database ‘Hits’ are when someone runs a query. Each query counts as 1 ‘Hit.’
* Because of lack of policy and lack of resources (among other things), InfoAccess is not used solely as an analytical repository. It also supports operational reporting & is the source for some transactional systems across campus.
  + This could cause an issue:
    - The database was not created to be the source for transactional systems.
    - The proliferation of data from InfoAccess to other systems creates a more complicated environment in which to administer security and data policy.
* There is a need to distinguish between application use and analysis use. Having users distinguish what their business purpose would help to distinguish between the two.
  + There should be a repository available to supply the needs for academic operational reporting and InfoAccess seems to fulfill this need at the moment.
* Today InfoAccess allows service accounts to access the data. This practice should be revisited.

1. **Update On ORCID Talks (Lee Konrad/Jason Fishbain)**

* ORCID is a national used identifier for researchers.
  + Used to distinguish between on researcher from another.
  + It is a lifetime ID
  + Cost for UW-Madison to have an enterprise license is $5,000.
* Process of distributing ORCID.
  + Today, researchers obtain an ORCID on their own. The Libraries at UW-Madison facilitates this process but the onus is still on the researcher.
  + A group is looking at the option of automaticallygiving all researchers who have a NetID an ORCID assigned to them.
  + The possible option of using ORCID externally.
* Data Stewardship Council think IMLG should have the opportunity to weigh in on the technical procedures for capturing and storing ORCID.

1. **Update on UW-System Information Assurance Council – Security Update from UW-System (Jason Fishbain)**

* A news article came out around the LAB Audit for UW-System. UW-System was knocked for not having proper security controls around their data.
* UW-System is creating an Executive Committee of System Leaders to help in setting up mandatory security controls at a system level.

1. **Update on OBI Project (Jason Fishbain)**

* Moving from the Query Library to OBI.
* There is funding for the OBI project, but the particulars on how to use the funding are still being discussed
* There is a need to create both a project governance model for the project AND incorporate data governance around the information that will be delivered through OBI.
  + Getting governance in place early will help in distinguish between what information can be published around an institutional contact versus information being accessed by a small group of users.

1. **Criteria for accessing Restricted Data (Discussion/Decision)**

* Overall / Background discussion:
  + Possibly having criminal background checks done before someone is given access to restricted data like SSNs.
  + There should be a business purpose for someone to have access to SSNs.
    - HR, Business Services & Student Records (RO’s office) all have such a need
  + What could be the consequences for an individual if SSNs are not handled appropriately?
    - Human Resources is involved with incidents that occur with mishandling PHI.
    - Could something be established across the board for all employees?
    - Ultimately, the Data Stewardship Council would recommend any policy to be approved by the Data Governance Steering Team
* Criteria a user must meet to gain access to restricted data:
  + Their role should be responsible for reporting data to a federal agency OR
  + Their role maintains a business process that requires SSNs (i.e. financial transactions)
  + The user has received training dealing with responsible handling of restricted data
  + Department head / Risk Executive signs off on the request.
* Policy should also include the following:
  + Regular audit should be completed monitoring who has access
  + If a user has access but does not use it for a specified period of time, the access should be removed.
  + A user should not download restricted data to their local machines or to a system that does not have the appropriate security controls to store the data.
  + A user should not distribute restricted data to those who have not obtained permission to access restricted data.
* A draft version of a policy will be drafted and brought back to the Data Stewardship Council for review..