Connect@RIT Data Management Plan

This plan describes the approach the project team will take to define the type of data generated by the project, ensure integrity of the data and allow distribution of data in a way that conforms to university and NSF privacy and protection policies.

1. Types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project:

The data to be collected during the course of this project will be as follows: (a) survey results (including climate survey information past and future, feedback surveys, and the faculty characteristics and social network behavior surveys), (b) statistical indicators (faculty demographics, recruitment, retention and advancement statistics, and salaries), (c) qualitative responses (focus groups, exit interviews), and (d) progress counts (participation levels in events, number of policies changed, number of templates used, number of trainings completed, number of prospective hires who use provided services, etc.).

Data will also be created during the course of this project as follows: (e) any course, forms and/or outreach materials developed for the activities, (f) results of analyses of the collected data.

2. Standards to be used for data and metadata format and content (where existing standards are absent or deemed inadequate, this should be documented along with any proposed solutions or remedies):

The data will be recorded via typical practices used in the human resource/institutional research arena. Quantitative data is typically acquired and/or stored in excel format. Statistical analyses will be performed using Minitab, SAS, and Excel. Qualitative data will be recorded through audio and video recording, transcribed into word documents, and analyzed for common themes using the qualitative research package NVivo. All compiled data will be posted to the *Connect*@RIT website using HTML and commonly readable data formats. Climate survey results will be stored by the agency conducting the survey. The *Connect*@RIT team will consult with the agency to ensure that minimum confidentiality, privacy and security standards are met.

3. Policies for access and sharing including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements:

Data access will be shared by the *Connect*@RIT team (survey results, progress counts, and summaries of results from analysis of qualitative data) with the Human Resources and Institutional Research offices of RIT (statistical indicators). Due to the often-sensitive nature of qualitative data and the requirement to protect the identity of participants, interview recordings and transcriptions will be housed on an encrypted file server accessible only to the researchers who are analyzing the data. Summary reports describing key themes and results will be posted in files accessible to the full *Connect*@RIT team.

The *Connect*@RIT implementation team will share aggregate data in a compiled and analyzed form with organizations associated with the project such as the *Connect*@RIT executive team, the internal advisory board, the executive advisory committee, the external advisory board and internal and external evaluators. The team will share data to the broader external community through annual and project completion reports, submission of archival/refereed publications, presentations made at conferences, presentations made at any institution interested in the research and the public website. No fees will be charged for access to this publicly accessible data. To ensure the appropriate

*This material is based upon work supported by the National Science Foundation under Grant No. 1209115.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.*

protection of privacy and confidentiality, the team will abide by the RIT university policy C5.0, Policy for the Protection of Human Subjects in Research.

During the project, qualitative interview and survey response data, progress counts, and program data will be stored electronically on the RIT computers of the *Connect*@RIT office and the PI, Co-PIs and Senior Personnel. These machines will be managed according to the RIT "Security Standard: Institute Information Access and Protection" effective as of February 1, 2010. This standard, from the RIT Information Security Office (ISO), is provided to ensure a minimum set of criteria for data privacy, confidentiality and integrity. It requires that "private information in electronic form must be stored in secure ISO-approved servers, or, if authorized to be stored elsewhere, only in encrypted (not just password-protected) form." The RIT ISO Office provides assistance in setting up secure access to data. The standard also requires the use of secure file transfer and secure storage of printed materials. Additionally, statistical indicators will be stored within RIT's Office of Human Resources and Institutional Research, both of which are already required to be in compliance with the RIT security standard. Sharon Mason (Co-PI) from the Department of Information Sciences and Technology will interface with the ISO to oversee the provisions for data protection, confidentiality and security.

4. Policies and provisions for re-use, re-distribution, and the production of derivatives:

Restrictions will be placed on the raw data collected during the project to ensure protection of privacy and confidentiality. Although upper administration (Provost, deans, department chairs) may wish access to individual response sets, information will only be provided in aggregate, limiting access to groups of five or more. Re-use of the data in the future would be appropriate in the aggregate form, in order to complete linear analyses of the results.

5. Plans for archiving data, samples, and other research products, and for preservation of access to them:

Upon project completion, all digital data will be stored for a minimum of seven years. Physical notes will be retained by the team members for a minimum of five years post completion of the project. The RIT Information Security Office will be consulted in developing a plan for secure digital and physical data archival.

This material is based upon work supported by the National Science Foundation under Grant No. 1209115.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.