American University Restricted Use Data Guidance Document

This guidance document addresses the use of **restricted use data sets** (hereinafter "RUDS") at American University, whether funded by external sponsored research sources or not. This guidance document is a companion document to the American University Policy on Academic Requests for Restricted Use Datasets for Research[1].

Definition of Restricted Use Data Sets

Administratively, as the aforementioned AU Policy defines them, RUDS are "Data from third parties which can only be obtained by committing American University to comply with predetermined restrictions." This compliance emphasis reflects that the use of RUDS not only binds the researcher(s) to certain conditions, imposed by data providers and legal regulations, but also binds the university as an organization. Therefore, "All requests for access to restricted use datasets must be coordinated and approved by the Vice Provost for Graduate Studies and Research."

RUDS are different than "public use" data files (PUDFs), which typically almost anyone can access/download and analyze, with or without payment to a data provider. By contrast, the potential disclosure of information that can be gleaned from RUDS – which may be about human groups or individuals, nesting sites of endangered species, corporations, or any other entity – represents a substantial risk related to confidentiality, privacy, safety, security, or similar concerns. The RUDS provider therefore requires the researcher(s), their collaborator(s), and the researcher's employing organization, to provide certain security assurances, and enter into a legal agreement to assure the safety of the data and manage the disclosure risk of information derived from the data. An example of RUDS access and use requirements is provided by the National Center for Education Statistics[2].

Technically, RUDS can come in a variety of file formats or packages – such as statistical analysis software data files, databases, collections of text documents, audio or video files … or a combination thereof.

What AU faculty should know about obtaining and using RUDS

The overall responsibility for managing a research project that involves the use of RUDS rests with the AU faculty member acting as Principal Investigator (PI). The aforementioned Policy outlines the elements of the review and approval process for obtaining RUDS, which may involve different campus units depending on:

- where and how the RUDS will be stored and analyzed
- what requirements the data provider imposes
- what computing and physical environment resources for the use of the RUDS are and will need to be available to the PI (and any research collaborators)

[1] See: http://www.american.edu/loader.cfm?csModule=security/getfile&pageid=2915125
[2] See: https://nces.ed.gov/statprog/instruct_access_faq.asp

The steps for obtaining and using RUDS are typically:

1. The PI obtains information on the requirements for using a RUDS from the potential data provider. These requirements may include training or certification.
2. The PI contacts the office of the Vice Provost for Graduate Studies and Research regarding the intent of using the RUDS for their research project, includes the RUDS requirements, and describes the applicable physical space and computing resources (that the RUDS provider requires) already available to them. This may include secure office space only accessible to individuals to be named on the RUDS agreement with the provider, computing equipment that is not connected to a network and not visible from outside the office space, and safe storage for media (such as optical discs, magnetic tapes or drives, or flash memory) on which the RUDS is delivered by the provider. The particulars will always depend on the specific requirements for the use of *that* RUDS, at *that* time, by *that* data provider.
3. The office of the Vice Provost for Graduate Studies and Research[3] evaluates the feasibility of executing the RUDS agreement given current infrastructure (computing and space) capabilities, or resources that may be provisioned[4] to meet the requirements, in coordination with other campus units as needed (such as OIT[5], incl. Chief Information Security Officer; IRB[6]; University Library[7]; PI's department's IT unit). Based on this analysis, the Vice Provost for Graduate Studies and Research either approves and executes the RUDS agreement, or not. If approved:
4. The secure space and computing environment (sometime also called "data enclave") is set up and maintained by the appropriate campus unit(s), and access is granted to the approved RUDS users, per the RUDS agreement. This setup may be temporary (only for the duration of this RUDS research project) or permanent (in any restricted-use data facility set up on AU's campus, but used by different projects over time).
5. The PI, and any collaborators, conduct their research project with the RUDS as governed by the agreement, and report on progress to the RUDS provider and the office of the Vice Provost for Graduate Studies and Research as required by the agreement and AU policies.
6. At the end of the research project, in coordination with requisite campus units specified in the agreement, the PI oversees either
   6.1. return of the RUDS to the provider, or
   6.2. wiping/destruction (on/of computer/delivery media) of the RUDS, as required by the agreement.
7. The PI verifies the closure of the project in compliance with the RUDS agreement to the office of the Vice Provost for Graduate Studies and Research.

[3] Including Office of Research Integrity (ORI) and Office of Sponsored Programs (OSP)
[4] Such as through secured external research funding for the project
[5] http://www.american.edu/oit/
[6] http://www.american.edu/irb/
[7] http://www.american.edu/library/