SSRI Protected Research Data Network (PRDN) Policies
Updated: January 2018 (reviewed annually)

Scope
These policies apply to the PRDN and all components of the PRDN managed by SSRI, including servers, network equipment and storage devices.

Compliance
Any person who uses the PRDN consents to all SSRI (available at ssri.duke.edu), all OIT/ITSO policies (available at security.duke.edu/policies-standards-procedures), any pertinent University policies, and with all applicable state and federal laws and regulations. Faculty, staff, affiliates, and students have a responsibility to use these resources in an efficient, effective, ethical, and lawful manner. Violations of the policy may result in loss of usage privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Duke University disciplinary procedures, as well as personal civil and/or criminal liability.

These policies are subject to review and audit by Duke’s Office of Internal Audit.

Responsibility
SSRI is responsible for implementing the policies described in this document.

Authority
The SSRI PRDN operates under authority of the Director of SSRI and the Associate Director for Research Data Security in SSRI to satisfy the needs of SSRI, data providers, and university researchers.

Description
The Social Sciences Research Institute (SSRI), in partnership with OIT and the University IT Security Office (ITSO), offers our Protected Research Data Network (PRDN) to provide secure computation and storage for academic and research projects. SSRI also uses the PRDN to provide data hosting for data sets and manages access to those data sets. SSRI’s PRDN policies and procedures comply with OIT’s Protected Network policies and procedures and Duke’s Data Security Policy and Data Classification standard.

SSRI’s PRDN allows research data to be stored on a storage array and analyzed on a secure virtual machine (VM) on an isolated subnet within OIT’s Protected Network service. The PRDN is dedicated for the use of protected academic and research data (data classified as Sensitive or Restricted by Duke’s Data Classification standard) and is administered by SSRI IT staff.
SSRI IT Policies: posted on the SSRI website

SSRI policies specific to the PRDN

SSRI PRDN Access policy
Access to the PRDN is granted based on the needs of an academic or research project. Once technical resources are set up and administrative requirements are met, SSRI provides access authorization to project resources in the PRDN. SSRI staff and the Principal Investigator (PI) will determine who has been authorized to have access to project resources in the PRDN, and which level of access is appropriate for the user’s role on the project. In the event of project staffing changes, the PI amends their IRB and DUA as needed and notifies SSRI of the changes, and SSRI updates data access as appropriate. When a research project ends or an individual leaves a research team, SSRI staff will remove that user from the access groups within one business day of notification.

SSRI PRDN Log Review policy
SSRI coordinates with OIT and ITSO to develop log review reports for PRDN log reviews. Logs are reviewed weekly or more frequently as needed.

SSRI PRDN Security Training policy
SSRI is working with ITSO to make security training available to PRDN researchers and SSRI staff. Once implemented, security training will be required annually to access data and systems in the PRDN. SSRI’s Research Data Security team receive annual security training.

SSRI IT staff with administrative privileges participates in an annual review of Duke, OIT, SSRI, and PRDN policies and procedures.

SSRI PRDN Data Integrity policy
Original data sets are generally either received on physical media from data providers or transferred to the PRDN directly from the data provider by the PI or SSRI staff. Original physical media are secured in locked storage within locked SSRI offices, unless the researcher and the data provider have an alternative explicit agreement. Once uploaded to the PRDN, original data should only exist on PRDN resources or on the source media.

For PRDN research projects that receive data on physical media, SSRI will store and manage the physical media for the duration of the project and dispose of it according to the data provider policy and Duke policy. Alternative solutions can be approved by SSRI.
Data integrity is not monitored by SSRI. If researchers have questions about changes to data files, they can request an access log review by SSRI, and SSRI will work with OIT to review the appropriate logs.

**SSRI Application Patching policy**
SSRI monitors applications installed on PRDN VMs and mitigates vendor-announced vulnerabilities in our default application set in accordance with the ITSO Server Security standard. Researchers should notify SSRI of software updates (especially for unique applications) by sending requests for updates to SSRI Data staff [https://ssri.duke.edu/prdn-help](https://ssri.duke.edu/prdn-help).

**SSRI Data Retention policy**
Data in the PRDN will be backed up via encrypted backups unless explicitly prohibited by the data provider. Data providers’ original data on physical media and electronic copies of data providers' original data stored in the PRDN will be destroyed by SSRI staff in accordance with the data provider requirements, or 1 year after all data use agreements with the project’s data provider have ended or expired. OIT backups will be discontinued and will be deleted through OIT procedures, or in accordance with the data provider’s requirements.

When a PRDN research project ends, SSRI will coordinate with the PI to move any code or derived data out of the PRDN (if permitted by the data use agreement). If a project ends and the derived data are not removed, SSRI will retain the electronic copy of the data for 1 year, and no users except SSRI IT staff will have access to it.

SSRI can also assist researchers in moving their derived data to the Duke Library data archive, if permitted by the data use agreement.

Any applicable federal, state, university, or other legal requirements for data retention supersede this policy.

**SSRI PRDN Emergency Access policy**
SSRI depends on OIT’s infrastructure to provide the PRDN service; if some parts of the infrastructure are inoperable and delivery of the PRDN service is interrupted, it will not be available until OIT restores the service.

**SSRI PRDN Risk Management plan**
An annual process of risk identification, analysis, and planning occurs. The Duke Data Risk Assessment completed in 2013 was used as the starting point for this process, and it has been continued since. Identified risks are documented and
communicated to the director of SSRI, the University IT Security Office, OIT, OARC, Counsel, and the VPR as appropriate.

2015 risk assessment: January 2015
2016 risk assessment: December 2015
2017 risk assessment: January 2017
2018 risk assessment: January 2018