Protected Research Data Network (PRDN) Policies

Updated: January 2020 (reviewed annually)

Scope

These policies apply to the PRDN and all components of the PRDN managed by the Research Data Security (RDS) team.

Compliance

Any person who uses the PRDN consents to all pertinent University policies, including:

- Research Data Security (RDS) policies (available at prdn.duke.edu)
- other Duke departmental IT policies (e.g. it.duke.edu/about-duke-it/policies-guidelines-and-practices)
- University IT Security Office policies (available at security.duke.edu/policies-standards-procedures)
- 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 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.

Responsibility

The RDS team is responsible for implementing the policies described in this document.

Authority

The RDS team operates under authority of the Office of Research, the Office of the Provost and the Associate Director for Research Data Security to satisfy the needs of the University, data providers, and university researchers and academic programs, and to protect research participants in compliance with Duke and other requirements.

Description

The Research Data Security team supports the evolving computational and data needs of Duke faculty, staff and students using protected data (as defined by the University) in their research or academic capstone projects.

We assist researchers across the institution in developing project documentation and obtaining research approvals, and to verify that the administrative and technical requirements of both the university and data providers are met.

The team also manages and supports the technical environment (the Protected Research Data Network, or PRDN) to ensure that the security controls in place are sufficient, appropriate, and consistent, and to monitor for unauthorized activity. The administrative and technical security controls are based on Duke's Data Classification and University IT Security Office standards. We regularly consult and coordinate with the Duke entities that are involved in research governance and institutional approvals to provide up-to-date guidance to those we support. Research Data Security staff will participate in internal, funder, data provider, and third party audit processes and penetration tests as agreed to by the University in specific data use agreements, subject to suitable arrangements between the parties.

PRDN Access policy

Access to the PRDN is granted based on data classification, data provider requirements, and the needs of the project. Once technical resources are set up and administrative requirements are met (and remain current), RDS staff provide access authorization to project resources in the PRDN. RDS staff and the Principal Investigator (PI) will determine who has been authorized to have access to project resources in the PRDN.

In the event of project staffing changes, the PI amends their IRB and DUA as needed and notifies RDS of the changes, and RDS updates data access as appropriate. When a project ends or an individual leaves a project team or the University, RDS staff will remove that user from the project's resource access groups within one business day of notification.

PRDN Log Review policy

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

PRDN Security Training policy

All individuals with PRDN access must complete IT security training. PRDN users and RDS staff will complete training managed by RDS. Other University employees with PRDN access due to their job responsibilities (e.g. OIT staff) will complete IT security training as coordinated by their department.

PRDN Data Integrity policy

Original data sets are generally either received on physical media from data providers or transferred to the PRDN directly from a data provider by RDS staff. Original physical media are secured in locked storage within locked offices, unless the researcher and the data provider have an alternative explicit agreement. Once uploaded to the PRDN, original data should only exist in location(s) permitted by the project documentation.

For PRDN projects that receive data on physical media, RDS 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 ORS and the data provider.

Data integrity is not monitored by RDS. When RDS receives questions about changes to data files they will work with OIT to review the appropriate logs.

Application Patching policy

RDS 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 RDS of software updates (especially for unique applications) by sending requests for updates to RDS staff (https://ssri.duke.edu/prdn-help).

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 RDS 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 project in the PRDN ends, RDS will coordinate with the PI to move any code or derived data out of the PRDN (as permitted by the data use agreement). If a project ends and the derived data are not removed, RDS will retain a copy of the data for 1 year, and only RDS staff will have access to it.

RDS 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.

PRDN Emergency Access policy

RDS 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.

PRDN Risk Management plan

An annual process of risk identification, analysis, and planning occurs. Identified risks are documented and communicated to the director of SSRI, the University IT Security Office, OIT, OARC, Counsel, and the OVPR as appropriate.

2015 risk assessment: January 2015
2016 risk assessment: December 2015
2017 risk assessment: January 2017
2018 risk assessment: January 2018
2019 risk assessment: February 2019
2020 risk assessment: January 2020