Restricted Access Data Remote Server (RADaRS) Action Plan

last updated June 6, 2016

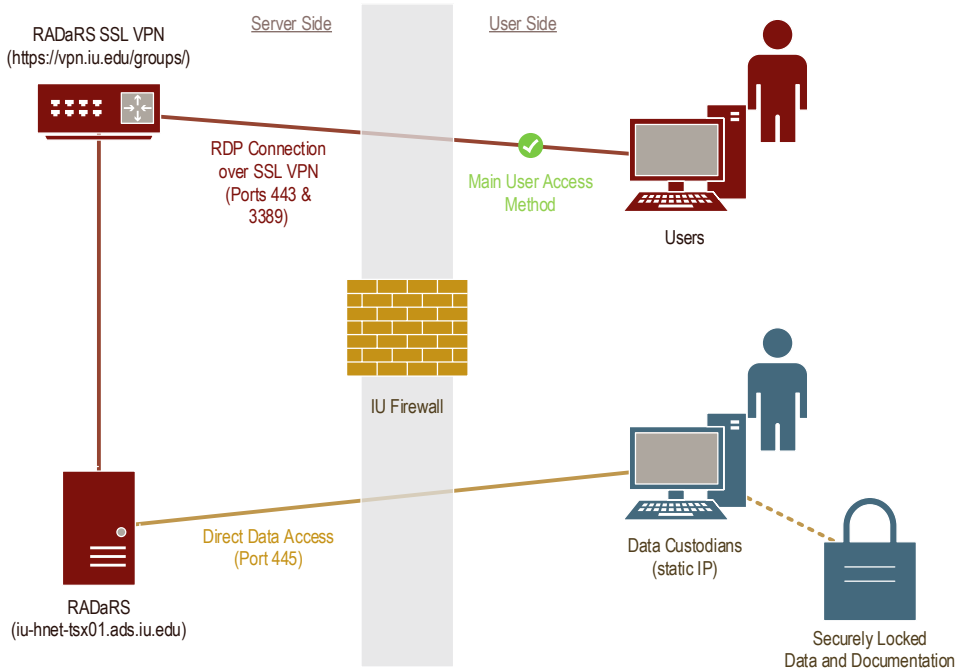
Introduction

IU UITS Research Technologies and the Social Science Research Commons maintains a Restricted Access Data Remote Server (RADaRS) for the purpose of allowing researchers to obtain, store, analyze and produce research related to datasets from a variety of providers that require the data be used only within an environment with added security protocols. The server was originally established and maintained by the School of Public and Environmental Affairs (SPEA) under the leadership of Dean David Reingold, Dr. Kosali Simon, and Chris England, Manager of Information Technology.

The server is part of a virtual server environment run by University Information Technology Services (UITS) called Intelligent Infrastructure which allows schools and departments to have a hosted server without needing to run any hardware. Further, the hardware behind the virtualized infrastructure is securely housed in a hardened data center with two-factor physical entry authentication, redundant power and network, and various natural disaster protections. More information can be found at the Intelligent Infrastructure and IU Datacenter websites at https://uits.iu.edu/ii and https://dcops.iu.edu/, respectively.

The server is intended to be a secure research hub for all areas of social sciences (and beyond), enabling a data custodian to upload secure datasets, while restricting researchers to do the analysis alone, remotely from their desktop workstations or laptops. Other restrictions are in place so that the researchers may not export/import other data, browse the Web, or otherwise get data in or out of the server without the cooperation of the data custodian.

RADaRS Infrastructure Diagram



Server Security

This server runs Microsoft Windows Server 2008 R2 64-bit edition, Microsoft ForeFront Client Security for anti-virus and anti-malware, various higher-end security protocols via group and local policy, and is protected by a local software firewall as well as the data center firewall service . The server and its software packages are updated from secure vendor sources on a monthly basis (unless otherwise deemed more critical via the vendor or IU's Security Office).

Researchers are only able to connect to the server via the Microsoft Remote Desktop Protocol (RDP). In order to do this, they must also connect to the IU SSL VPN service , which creates an encrypted tunnel from the researcher's computer to the secure server. They may NOT copy and paste from the server, map network drives to other servers, print to any printers, or access the Internet via the Web or any other protocol.

The only data transfers allowed out of or onto the server are via the data custodian, who will have access to upload the secure datasets received from data providers, and to release research output (e.g. tables for research papers) to the researchers. The data custodian may create project folders and assign permissions so that the permitted (and only the permitted) researchers may gain access to these files. Once the research is done, the data custodian may export any research output after ensuring there is no sensitive data in said output, delete the sensitive data and project files, and provide the output to the researchers.

Researchers may also request a secure folder on the server to which only they have access (no sharing with other members of the project team) in which they can store temporary files and additional research materials. The data custodian will also ensure these folders are cleared of sensitive data at the end of each project.

Backup

The server is backed up daily for disaster recovery purposes; this portion of the backup contains no sensitive data. The data folders are also backed up daily and stored in an encrypted tape archive in an off-site location from the virtual server. Folders may be excluded on a per-project basis as needed; if applicable, this information should be included in the User and Service Owner Agreements for the project.

All of these folders are controlled via NTFS access control lists so that only the appropriate users may access proper data.

External Security Factors

Hardware and Physical Security Several systems at IU play a large role in the functionality and security of this infrastructure. Most importantly are the aforementioned Intelligent Infrastructure and IU Datacenters. These are secure resources, with HIPAA-compliant measures in place to ensure the utmost security of data and processes. From a hardware and physical access point of view, the server is as secure as you will find at IU and across much of the world.

Authentication Another contributor to the project is the authentication mechanism, provided by an Active Directory domain from Microsoft, using Kerberos login authentication. This server utilizes this method of authentication in a secure fashion to ensure all users are unique and thoroughly identified via this login process. Login attempts (username, IP address, and datestamp) are logged in a secure logging server accessible only by the Active Directory systems administrators and the University Information Security Office personnel. Dual-factor authentication (e.g.: smart cards or one-time-password tokens) is being researched and may be implemented in the future.

Passphrases All IU users are now required to use a passphrase (a phrase of at least 4 words separated by spaces – special characters are optional, but encouraged) instead of a complex password. Any "grandfathered" user with an older complex password (requires numbers, special characters, and upper-case letters) is encouraged to move to a new passphrase for increased security.

Defense Department C2 Compliance By default, all Windows Server 2008 products are deemed C2 compliant.

HIPAA Compliance As stated above, the hardware and physical access of this server are HIPAA compliant. An exercise in the server's own HIPAA compliance (from a software standpoint) will be undertaken in the future.

RADaRS User Agreement RADaRS users are required to sign an Acceptable Use Agreement at IU adhering to appropriate use, misuse, and abuse IT policies . All users at Indiana University sign and acknowledge this agreement upon receipt of their IU network accounts.

Original Data Security

The original media from the data providers will be sent by secure courier delivery (e.g. FEDEX with signature) to the data custodian, and stored in a locked safe once it is copied to the secure server by the data custodian. Once the data set is no longer needed and is removed from the server, it can be disposed of as determined by the providing body (including degaussing, shredding, or returning to the provider).

The Social Science Research Commons' sensitive data safe is stored in Woodburn Hall Room 303, 1100 E. 7th St., Bloomington, IN 47405. The safe is water- and fire-proof, and only data custodians have keys to the safe. Additional information about the sensitive data safe is available upon request.

Additional Requirements

Before obtaining restricted-use data and beginning your research on RADaRS, you will also need to obtain documentation from the IU Institutional Review Board (IRB) and, if required, institutional signatures for your data use agreement. You will need to provide a copy of this documentation to the data custodian before commencing your project. You may send a copy of this document with both your IRB and data use agreement to describe the security protocols that will be used for the computing environment in which these data will be used.

Human Subjects Approval Often times, restricted access data involve data from human subjects. Please make sure that you are in contact with the IU Office of Research Compliance's (ORC) Institutional Review Board (IRB) procedures. Please ensure that you have received human subjects approval (or, if appropriate, documentation of an exemption or documentation of non-human subjects research), from the Human Subjects Office. You will not be able to begin your research on RADaRS until you have provided the data custodian with documentation of human subjects clearance from IU. You will also be responsible for making sure such documentation is up to date throughout the duration of your project. For instructions on how to retrieve your IRB approval letter in KC-IRB, please see http://researchcompliance.iu.edu/eo/guides/kcirb/retrieving_study_documents.pdf (p. 12).

Data Use Agreements and Signatures Obtaining your restricted access data often involves the signing of a data use agreement with the agency providing your data. Please make sure that you are in contact with the IU Office of Research Administration (ORA) Grant and Contract Services office for the appropriate signatures; if your data use agreement requires an institutional signature, please email the data use agreement to RUGS@indiana.edu (attention: Bethany Wuensch). Please make sure you also check with ORA before you sign any such data use agreement yourself.

RADaRS Key Parties and Contact Information

The key members or parties of this service are listed below along with contact information. For general inquiries on the service, users may contact ssrcdata@indiana.edu or call the Social Science Research Commons at 812-855-6664.

- Data Custodian: Emily Meanwell, SSRC Director, emeanwel@indiana.edu, 812-855-6661
- Project IT contact and backup data custodian: Esen Tuna, Manager and Technical Advisor, Research Data Services, UITS, metuna@iu.edu, 812-855-0984
- HELPnet services and systems administration providers: Carl Rhine and Allen Tucker, helpnet@iu.edu, 317-274-3087

RADaRS was originally established by the School of Public and Environmental Affairs under the leadership of Dean David Reingold, Dr. Kosali Simon (simonkos@indiana.edu, 812-856-3850), and Chris England, Manager of Information Technology for SPEA Bloomington (chenglan@indiana.edu, 812-855-4837).

Restricted Access Data Remote Server (RADaRS) User Agreement

User Agreement

The research user stated below agrees to adhere to the following practices and policies.

- The user has signed the "Acceptable Use Agreement" at IU: https://ams.iu.edu/useragreements/agreement.aspx/, and agreed to all pertinent IT Policies.
- The user has made a best effort to change to a "passphrase" for his/her IU user account: http://kb.iu.edu/data/acpu.html.
- The user has obtained and will maintain IRB clearance. Use of an account is contingent upon showing documentation of IRB clearance.
- The purpose of this service and the data herein is for research only and should not be used for academic or administrative work.
- The user agrees to work only in an environment in which no other persons are present in the room.
- The user acknowledges that this service is locked down to the best ability of the service owner and the user will not attempt to circumvent those security measures (e.g.: taking camera photos of the screen due to copy & paste being disabled).
- The work on this service will be limited to the user, folders, and sensitive data specified below.
- Misuse or abuse of this service may result in terminated access to the service and/or reporting to the University Information Policy Office.
- The user agrees to abide by any regulations and policies given by the data providing party and must adhere to any additional conditions set forth in the data user agreement from the data provider. These will be included as an appendix to this form.

If there are any questions or problems with the above statements, please contact the service owners in the action plan.

User and Project Information

User's name:_____ Project folder:_____

User's IU network username:_____ Project PI:_____

User's email:_____ Data information:

User's status:

☐ Faculty ☐ Graduate student ☐ Postdoc

☐ Personal folder requested:_____

User's signature:_____ Date:_____

Restricted Access Data Remote Server (RADaRS) Service Owner Agreement

Service Owner Agreement

The service owners, as signed below, agree to provide a secure environment for the users and the data via the following mechanisms:

- The systems administrators will ensure the highest degree of security, backups, and performance is being met for the users
- The data custodian will provide "gatekeeper" access for all incoming and outgoing data. The data custodian will place data on the server, and users will only have rights to login to the secured server via Remote Desktop protocol as described above, accessing their datasets locally on the server. Any changes to the folders and datasets must go through the data custodian.
- Support teams will not (and cannot) interfere with the integrity of the research or the security of the data.
- Similar to the User Agreement, all service owner and support parties involved have signed the "Acceptable Use Agreement" at IU (https://ams.iu.edu/useragreements/agreement.aspx/), adhering to various IT Policies, and have made a best effort to convert to a passphrase (http://kb.iu.edu/data/acpu.html) for their IU user accounts.

Project information

Project folder:_____

Project PI:_____

Data information:_____

Special requirements:

☐ Exclusion from backups:_____

☐ Other:_____

Emily Meanwell, Ph.D.
RADaRS data custodian
Director, Social Science Research Commons
emeanwel@indiana.edu

M. Esen Tuna
RADaRS IT Manager and backup data custodian
Manager & Technical Advisor, Research Data Services
metuna@iu.edu