RADaRS Action Plan

SPEA Bloomington Restricted Access Data Remote Server (RADaRS)
Faculty: Kosali Simon, IT: Chris England, Data Custodians: Emily Meanwell and Kevin Wilhite
Last Updated: 10/9/2013

Introduction

The School of Public and Environmental Affairs (SPEA) at Indiana University, in conjunction with other units including the Social Science Research Center (SSRC) and the Department of Political Science in the College of Arts and Sciences, has created and 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 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.

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.

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).

http://ssrc.indiana.edu/home/
http://ii.uits.iu.edu/ resources/expectations.shtml
http://www.dcops.iu.edu/policies.html
http://kb.iu.edu/data/azwj.html
Researchers are only able to connect to the server via the “Remote Desktop” protocol from Microsoft. In order to do this, they must also connect to the IU SSL VPN service\(^6\), 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 (Tables for research papers) to the researchers out of the server. The data custodian may create project folders and assign permissions so that the correct (and only the correct) researchers may gain access to these files. Once the research is done, the data custodian may export any reports/findings after ensuring there is no sensitive data in said reports/findings, delete the sensitive data and project files, and provide the reports/findings to the researchers.

Researchers also have a secure folder on the server to which only they have access (no sharing with others) 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.

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

**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. The researcher signs (annually) agreements to abide by the rules of conducting research on the secure server. 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 location of this safe-locked data is: **Woodburn Hall Room 303, 1100 E. 7th St., Bloomington, IN, 47405.**

**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 Administration (ORA)’s Institutional Review Board (IRB) procedures. Please ensure that you have received human subjects approval or exemption as appropriate, if your research involves human subjects. You will not be able to commence your research on RADaRS until you have provided the data custodian with documentation of human subjects clearance from IU\(^7\). You will also be responsible for making sure such documentation is up to date.

---

\(^6\) [http://kb.iu.edu/data/aygt.html](http://kb.iu.edu/data/aygt.html)
\(^7\) [http://researchadmin.iu.edu/HumanSubjects/](http://researchadmin.iu.edu/HumanSubjects/)
For example, if you believe that your research meets the criteria for exempt research, please fill out the exempt research checklist and follow all instructions.8

Complete the 4 forms under “Exempt Research Studies” and email them to irb@iu.edu to start the process. Once you have completed the process, please provide the data custodian a copy of the approval.

**Data Use Agreements**

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, and please provide a copy of the agreement to the data custodian prior to commencing your project. Please email the data use agreement that needs institutional signatures to RUGS@indiana.edu (attention: Bethany Wuensch). Please make sure you also check with ORA before you sign any such data use agreement yourself.

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.

**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 (include info in User Agreement below).

**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 Windows 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. Dual-factor authentication (e.g.: smart cards or one-time-password tokens) is being researched. 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.

---

8 [http://researchadmin.iu.edu/HumanSubjects/exempt_review.html](http://researchadmin.iu.edu/HumanSubjects/exempt_review.html)
**RADaRS User Agreement**
RADaRS users are required to sign an Acceptable Use Agreement⁹ at IU adhering to appropriate use, misuse, and abuse IT policies¹⁰. All users at Indiana University sign and acknowledge this agreement upon receipt of their IU network accounts.

**Passphrases**
All IU users are now required to use a passphrase¹¹ (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.

**Key Parties**
The key members or parties of this service are listed below along with contact information. For general inquiries on the service, users may contact **SPEA Bloomington IT Services** at speabits@indiana.edu or 812-855-6544.

- Dr. Kosali Simon, Faculty, SPEA and project manager: simonkos@indiana.edu, 812-856-3850
- Chris England, Manager of Information Technology, SPEA Bloomington and project IT contact: chenglan@indiana.edu, 812-855-4837
- Carl Rhine and Allen Tucker, HELPnet services and systems administration providers: helpnet@iu.edu, 317-274-3087
- Data Custodians: Emily Meanwell, SSRC Associate Director and Kevin Wilhite, Data Services Coordinator and Data Steward: ssrdata@indiana.edu, 812-855-6664

---

⁹ [http://protect.iu.edu/acceptableuseagreement](http://protect.iu.edu/acceptableuseagreement)
¹⁰ [http://protect.iu.edu/cybersecurity/policies/IT01](http://protect.iu.edu/cybersecurity/policies/IT01) and [http://protect.iu.edu/cybersecurity/policies/IT02](http://protect.iu.edu/cybersecurity/policies/IT02)
¹¹ [http://kb.iu.edu/data/acpu.html](http://kb.iu.edu/data/acpu.html)
User Agreement
The research user stated below agrees to adhere to the following practices and policies.

- The user agrees to abide by any regulations and policies given by the data providing party. These will be included as an appendix to this form.
- The user has signed the “Acceptable Use Agreement” at IU: [https://ams.iu.edu/useragreements/agreement.aspx/](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](http://kb.iu.edu/data/acpu.html).
- The user has obtained IRB clearance, and will continue to do so. Use of an account is contingent upon showing 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 must adhere to any additional conditions set forth in the data user agreement from the data set provider.

**Signature:** __________________________________________

**User’s Name:** ________________________________

**User’s Email:** ________________________________

**Date:** _______________________________________

**User’s Project Folder:** ________________________________

**User’s Personal Folder:** ________________________________ *(if applicable)*

**Confidential Data Information:** ________________________________

____________________________________________________________________________________

____________________________________________________________________________________

If there are any questions or problems with the above statements, please contact the service owners in the action plan.
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 data incoming and outgoing. Users will only have rights to login to the secured server via Remote Desktop protocol as described above, accessing their data sets “locally” on the server that have been placed there by the data custodian. Any changes to the folders and data sets 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 account.

______________________________
Name:
Data Custodian

______________________________
Chris England
SPEA Bloomington IT Director
Appendix A: RADaRS Diagram

Secure Server Infrastructure Diagram

Current RADaRS & RSR Infrastructure

- RADaRS
  - (non-sensitive, iu-hnet-srv4003.adasiu.edu)
  - (sensitive, iu-hnet-txs01.adasiu.edu)
- RSR
  - (non-sensitive, iu-hnet-srv4003.adasiu.edu)
- RADaRS SSL VPN
  - (https://vpn.iu.edu/groups/)
- Direct Data Access
  - (Port 445)
- RDP Connection over SSL VPN
  - (Ports 443 & 3389)
- IU Firewall
- Users
  - Main User Access Methods
  - RDP Connection (Port 3389)
- Data Custodians
  - (static IP)
- Securely Locked
  - Data and Documentation