Security for Secondary Research-Data

The required security for secondary research-data depends on their sensitivity and identifiableness. Research-data with more sensitive information and greater potential identifiableness require extra security precautions. Each level adds another restriction layer. The levels are (0) Public-use (0.5) Private-use (1) Restricted-use 1 (2) Restricted-use 2 and (3) Restricted-use 3. Responsibility to protect respondent identities *and* their information

At level 0, public-use data do not require security.

At level 0.5, private-use data require encryption and approval.

At level 1, data must be encrypted at rest and in transmission. An additional security requirements is blocked Internet. The rooms that house the client and server must be lockable. *Data sent to researcher.*

At level 2, in addition to level 1 protections, nothing including output, data and data extracts can be removed from the computing system until vetted for disclosure risk by trained and authorized personnel. Furthermore, files cannot be added without security review. *Researcher comes to data virtually.*

At level 3, in addition to level 2 protections, processing must be monitored by trained personnel. Notes may not be taken. Moreover, all items such as backpacks and briefcases must be inspected for disallowed materials after a processing session ends. *Researcher comes to data in person.* This table summarizes the restrictions:

	Encryption	**Internet**	**Output**	**Processing**	**Access**	**Approval**
Public-use 0	Not encrypted	Allowed	Not vetted	Not monitored	Web	Terms of Use
Private-use 0.5	Encrypted	Allowed	Not vetted	Not monitored	Authorized download	Terms of Use with approval
Restricted-use 1 *Data sent to requestor*	Encrypted	Blocked	Self-vetted	Not monitored	Encrypted media or download	Data Use Agreement IRB approval
Restricted-use 2 *Requestor comes to data electronically*	Encrypted	Blocked	Vetted	Not monitored	Terminal Server with extra security	Data Use Agreement IRB approval
Restricted-use 3 *Requestor comes to data in person*	Encrypted	Blocked	Vetted	Monitored	Guarded "Cold" Room	Data Use Agreement IRB approval

Research-Data Security

Encryption

Encrypted. Data files, output files, temporary files and other project files must be encrypted *at rest* and *in transport*. Real-time or "on the fly" encryption must be used so that any files placed on the volume are automatically encrypted. Encryption software must be currently maintained. Encryption must meet AES standards.

Internet

Blocked. System must prevent all files from being copied to the Internet; data must be prevented from leaking out. Access to any systems with restricted-use files must not be directly accessible from the Internet. Access must be from designated locations only. Access through a VPN or private address space is acceptable; however, split tunneling is not allowed.

Output

Vetted. Results (tables, regressions, etc.) are checked for disclosure risk by authorized and trained personnel (not the researcher). Output includes data extracts. By requiring vetting, data cannot be copied. Inputs must all also be checked but this vetting is not as stringent.

Processing

Monitored: Data analysis can only occur in the presence of authorized and trained personnel.

Access

Web: Data are available on the ICPSR website

CD or download: An encrypted version of the data are sent on a CD or available for download

Terminal Server with extra security The ICPSR Virtual Data-Enclave (VDE) meets this requirement. After installing software and obtaining login credentials, a researcher may connect to the VDE to analyze data. Data and results cannot be downloaded.

Guarded "cold" room: The ICPSR Physical Data-Enclave meets this requirement. Researcher must come to the ICPSR (Perry) building to analyze data. Analysis times are restricted to ICPSR operating hours.

Approval

Terms of Use: Researcher must agree to terms of use before downloading data. Some data require approval.

Data Use Agreement. Researcher and researcher's institution must enter into a data use agreement with the University of Michigan/ICPSR.