CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: RD

Responsible Executive: CISER Secure Data Services Manager

Secure Standalone Desktop - Data Destruction and Return of Restricted Data Policy

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 11/9/17

Revised:

POLICY STATEMENT

In order to comply with the terms set forth in the Data Use Agreement, Cornell Restricted Access Data Center (CRADC) staff must certify to the Data Provider that the associated data have been destroyed and/or returned to the Data Provider at the termination of the agreement.

This policy applies to all research data regardless of the storage medium (e.g., disk drive, electronic tape, CD, DVD, external drive, paper, fiche, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed within the Cornell Institute for Social and Economic Research (CISER) auspices.

PROCEDURES

To protect restricted-access data appropriately and effectively, CRADC researchers and staff must understand and carry out their responsibilities related to data security, as set forth by the Data Provider Agreement(s) (including referenced laws and regulations), Cornell University Institutional Review Board for Human Subjects, Cornell University Office of Sponsored Programs, and Cornell University Policy. This policy applies regardless of the source of funding for the research.

1. **Data Destruction**
    a. **Destruction of Physical media**: The Secure Data Services staff will be responsible for the return and destruction of all associated materials as determined by the Data Use Agreement. All physical media, whether originally supplied by the Data Provider or a CISER Secure Data Services created backup copy of electronic original data, will be destroyed and the Data Provider sent a Certificate of Data Destruction, unless the Data Provider requests the media returned within the Data Use Agreement. As stipulated by the Data Use Agreement, requested physical media will be returned to the Data Provider using a traceable method via FedEx, with requirement for a signature by the recipient.
        i. Physical destruction methods:
            1. CDs/DVDs are destroyed using a crosscut shredder.
            2. USB flash drives are first sanitized by utilizing Department of Defense shredding algorithm, using seven-rounds of overwriting and/or degaussing. After sanitation, the flash drives are turned over to Cornell University's R5 recycling unit whom then delivers the drives to a licensed company for physical destruction.
            3. Hard disk drives are first sanitized by utilizing Department of Defense shredding algorithm, using seven-rounds of overwriting and/or degaussing. After sanitation, the hard disk drives are turned over to Cornell University's R5 recycling unit whom then delivers the drives to a licensed company for physical destruction.
    b. **Destruction of Original Data Files on Secure Standalone Desktop**: The Secure Data Services staff will be responsible for the destruction of all original data on the Secure Standalone Desktop as determined by the Data Use Agreement. All original data will be destroyed and the Data Provider sent a Certificate of Data Destruction.
        i. Electronic destruction method: Electronic files on the Secure Standalone Desktop are disposed of utilizing Department of Defense shredding algorithm, using seven-rounds of overwriting.

    c. **Destruction of User-Created Electronic Files**: The Secure Data Services staff will be responsible for the destruction of user-created electronic files as determined by the Data Use Agreement. Electronic files on the secure standalone desktop are disposed of utilizing Department of Defense shredding algorithm, using seven-rounds of overwriting.
        i. Researcher Requested Copy of User-Created Electronic Files: If permitted by the Data Use Agreement, researchers may request a copy of their user-created, disclosure proofed, application code and log files, to be transferred to the researcher prior to the destruction of the project files.

    d. **Destruction of Paper Materials**: No paper materials or copies are produced or stored by CISER Secure Data Services, unless provided with the original media. The

Secure Data Services staff will be responsible for the destruction of all paper materials. If the Data Provider requests the return of any paper materials provided with the original media, the paper materials will be returned to the Data Provider using a traceable method via FedEx, with requirement for a signature by the recipient.

   i. Paper Destruction Method: Paper materials are destroyed using a crosscut shredder.

e. **Certificate of Destruction**: Upon completion of the disposal of all project related data, the Secure Data Services staff will certify that the secure data and user created project-based transitory files have been securely destroyed via a Secure Standalone Desktop Certificate of Destruction. The completed Secure Standalone Desktop Certificate of Destruction will be sent to the Data Provider either as a paper copy through FedEx or electronically via email, with a copy of the Secure Standalone Desktop Certificate of Destruction supplied to Office of Sponsored Programs.

   i. Requested Formats for the Secure Standalone Desktop Certificate of Destruction: In the case that the Data Provider requires the completion of a specific certificate of destruction, or certification of destruction format, for the conclusion of the Data Use Agreement, the requested certificate will be completed in replacement of the Secure Standalone Desktop Certificate of Destruction. Notarized affidavits may be requested as a section of a specific certificate of destruction, to be completed by the Secure Data Services staff as required.

Entities Affected by this Policy

CISER Secure Data Services staff, CRADC Secure Standalone Support Staff, CISER Information Technology staff, and CRADC Secure Standalone Desktop account holders.

Who Should Read this Policy

CISER Secure Data Services staff, CISER Information Technology staff, CRADC Secure Standalone Desktop account holders and affiliated CRADC Secure Standalone Support Staff.

Related Documents

Cornell University Policy 5.1, Responsible Use of Information Technology Resources
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/responsibleuse.cfm

Cornell University Policy 5.4.1, Security of Information Technology Resources
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/resources.cfm

Cornell University Policy 5.4.2, Reporting Electronic Security Incidents
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/incidents.cfm

Cornell University Policy 5.8, Authentication to Information Technology Resources
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/authentication.cfm

Cornell University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/itdata.cfm

Cornell University Policy 5.10, Information Security
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/infosecurity.cfm

Cornell University Policy 8.4 -- Management of Keys and Other Access Control Systems
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/riskandsafety/accesscontrol.cfm

NIST Special Publication (SP) 800-88 – Guidelines for Media Sanitation
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

CRADC Policies
http://www.ciser.cornell.edu/pub/policies/CISER_Policies.shtm

CONTACTS

If you have questions about specific issues regarding this Sharing, Transmission and Distribution of Restricted Data Policy, call the following offices:

William Block	block@cornell.edu	CISER Director	607-255-4801
Elena Goloborodko	cradc@cornell.edu	CISER Secure Data Services Manager	607-255-4801
Jonathan Bohan	cradc@cornell.edu	CISER Secure Data Services Support Staff	607-255-4801
Janet Heslop	jheslop@cornell.edu	CISER Director of Information Technology and Security Liaison	607-255-4801
Kim Burlingame	kb269@cornell.edu	CISER Sr. System Administrator	607-255-4801
Brandon Cruz	brc75@cornell.edu	CISER System Administrator	607-255-4801

Cornell University Security Office	security-services@cornell.edu		607-255-6664

RESPONSIBILITIES

The following are major responsibilities each party has in connection with this policy.

CISER Secure Data Services Manager	Interpret this policy, provide clarification and education, and implement operational and business processes to facilitate compliance.
CISER Director of Information Technology and Security Liaison	Implement operational, physical, and technical equipment and tools to facilitate compliance.
CISER System Administrators	Responsible for performing tasks in accordance with established policy guidelines.
CISER Secure Data Services Support Staff	Responsible for knowing and assisting with tasks as related to this policy.
CRADC Secure Standalone Desktop Researcher	Responsible for knowing and abiding by the Data Provider Agreement and this policy.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.