CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: RD

Responsible Executive: CRADC Secure Data Services Manager

CRADC Data Security Policy

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 7/13/15

Revised: 9/30/16

POLICY STATEMENT

The fundamental obligation of the Cornell Restricted Access Data Center (CRADC) is to protect restricted-access research data that are confidential due to applicable laws and regulations, by means of contract or agreement, and University policies.

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.

POLICY GUIDELINES AND PROCEDURES

To protect research-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. **Identify and Assess Security Risks**
    a. Review Data Provider's Data Use Agreement, or Cornell University agreement for internal data, to determine if CISER Secure Data Services is an appropriate location for the research project

    b. Evaluate applicable laws and regulations, by means of Data Provider's Data Use Agreement, or Cornell University agreement for internal data

    c. Ensure appropriate University units are involved:
        i. Institutional Review Board (IRB): Unless determined otherwise by Cornell Institutional Review Board for Human Participants (IRB), all researchers allowed on the CRADC servers are required to complete the CITI training course on Social & Behavioral Research Basic, Stage 1 satisfactorily. CRADC relies on the confirmation from the Office of Sponsored Programs (OSP) that approved researchers have satisfactorily passed the CITI training course on Social & Behavioral Research Basic, Stage 1, in addition to their Conflict of Interest (COI) statement.

            In instances where the Cornell's IRB states that an IRB review is not necessary for a project, such as with proprietary business data, which contains no human identifying characteristics, researchers will not be expected to complete the CITI training course on Social & Behavioral Research Basic, Stage 1. CRADC relies on the confirmation from the Office of Sponsored Programs (OSP) that these data continue to be exempt from IRB review for Cornell's processing approval.

        ii. Office of Sponsored Programs (OSP): CRADC accepts projects and provisions unique user accounts for faculty/staff/students once final approval from the Office of Sponsored Programs has been attained from the Data Provider, on behalf of Cornell University. Data internal to Cornell University is exempted from the need for OSP approval to be housed on the CRADC servers.

    d. Confirm that the CRADC User Agreement has been signed
        i. In addition to the final approval from the OSP, which includes the IRB review as necessary, each researcher is required to complete a user agreement with CRADC covering the usage of the CRADC servers. CRADC User Agreements are only sent to a researcher for signature once CRADC has final approval from OSP, or internal agreement from Cornell University for Cornell data.

2. **Provision Access and Security on a Project by Project Basis**[1]
    a. Account Creation: Upon receiving a signed CRADC User Agreement, the Secure Data Specialist may proceed with unique account creation. All temporary passwords, by Active Directory Group Policy, must be changed upon initial login to any CRADC server.

    b. Account Expiration: User account access remains dependent on the existing project requirements, as stipulated within the Data Provider's Data Use Agreement and approved by OSP, IRB, and the CRADC User Agreement. Any project with an internal agreement from Cornell University for Cornell data is exempt from approval by OSP, but must retain approval of IRB and the CRADC User Agreement.

    c. Password Requirements: The CRADC server environment requires researchers to change their passwords every 90-days. Password complexity is enabled, and a strict password complexity policy is enforced.

    d. Dual-Factor Authentication: The CRADC researcher must activate DUO prior to logging on to a CRADC server for the first time. Subsequent logins require DUO authentication after entering the researcher's unique user account password.

    e. Idle Sessions: Idle sessions are suspended after 15-minutes of non-activity. If the Data Provider agreement establishes criteria requiring idle sessions be suspended after less than 15-minutes of non-activity, special requests will be accommodated.

    f. Authorization: Authenticated users have read and execute access to the restricted data provided under the Data Provider Data Use Agreement. The user account has project-based transitory storage space to store application program files and interim datasets. Authorization is based upon Microsoft Windows NTFS permissions.

3. **Restricted-access Research Data Storage**[2]
    a. Storage of Original Media:
        i. The physical media on which the data were received from Data Providers (e.g., CDs, DVDs, USB drives) are stored in a locked fire-protected safe in CRADC office Room 201A, CISER building, 391 Pine Tree Road. Only the CISER Secure Data Services Manager and CISER Secure Data Support Specialist have keys to access the Sentry Media Safe.

        ii. Original electronic data may be copied to physical media as a backup when permitted by the Data Provider's Data Use Agreement, and stored in the Sentry Media Safe.

        iii. Storage of Included Documents: No documents are produced or stored by CISER Secure Data Services, unless provided with the original media.

Documents provided with original media are stored in the safe in the project folder, alongside the physical media.

b. Data for Analysis:
    i. Restricted data are copied to secure CRADC network attached storage. Authenticated users have read and execute access to the restricted data provided under the Data Provider Data Use Agreement. The user account has project-based transitory storage space to store application program files and interim datasets. Authorization is based upon Microsoft Windows NTFS permissions.

c. Researcher Responsibility:
    i. Data Security of Researcher Copies: The Principal Investigator and others authorized by the Data Provider to have an external copy of their non-restricted user created working files are responsible for the creation and storing of such documents in strict accordance with the Data Use Agreement they have signed with the Data Provider. It is the responsibility of the researcher to properly manage and destroy user created working files as required by the Data Use Agreement.

    ii. Researcher Publication of Data: It is the responsibility of the researcher to request approval from the Data Provider prior to publishing study findings that include statistics, beneficiary, or facility level data. Any questions the researcher may have pertaining to publication and Data Provider publication policies must be directed to the Office of Sponsored Programs.

    iii. Researcher Modification of Temporary Analysis Files: When specified within a Data Provider's Data Use Agreement, it is the responsibility of the Principal Investigator to ensure that all stipulated temporary analysis files for the project, within all project user accounts, are deleted at the specified Agreement dates each year.

4. Restricted-access Research Data Backup[3]

a. Original Media Backups:
    i. Data Security of Original Media Backups: The original physical media stored in the Room 201A safe serves as the only backup of the restricted data stored at CRADC. The disk array containing original restricted-use data files are not included in the routine backup.

    ii. Backups of Original Electronic Data Copies: Electronic data copies of the restricted data reside on the CRADC network attached storage and are excluded from backup routines. When permitted by the Data Provider's Data

Use Agreement, original electronic data may be copied to physical media as a backup and stored in the safe as noted above.

b. Backups of User Created Files (Unless Prohibited by Data Use Agreement): The user created transitory files (programs, output, log files and working datasets) housed on the CRADC network attached storage are backed up via disk-to-disk and are never commingled with any other backups.

5. De-provisioning of accounts[1]

a. Researcher Account De-provisioning: OSP communication initiates that an account should be de-provisioned. CRADC will contact the Principal Investigator (PI) and offer the PI the possibility to have the researcher's personal project subfolder files copied to the project's transitory storage space. After 30-days, or sooner if the PI notifies CRADC to destroy the files, the researcher's personal project files will be destroyed utilizing the disposal of electronic files method.

b. CISER Secure Data Services Staff De-provisioning: Changes in the CISER Secure Data Services staff will be communicated via email to the Data Provider through OSP. The staff account will be disabled on the last day of employment within CISER Secure Data Services and terminated shortly thereafter.

6. Data Destruction and Certification[4]

a. Destruction of Physical media: The Secure Data Services Manager or Data Support Specialist will be the person 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 CRADC 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.

b. Destruction of Original Data Files on CRADC Servers: The Secure Data Services Manager or Data Support Specialist will be the person responsible for the destruction of all original data on CRADC servers as determined by the Data Use Agreement. All original data will be destroyed and the Data Provider sent a certificate of data destruction.

c. Destruction of User-Created Electronic Files: The Secure Data Services Manager or Data Support Specialist will be the person responsible for the destruction of user-created electronic files as determined by the Data Use Agreement. Electronic files on the CRADC servers are disposed of utilizing the Department of Defense shredding algorithm.

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 Manager or Data Support Specialist will be the person 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.

e. Certificate of Destruction: Upon completion of the disposal of all project related data, the Secure Data Services Manager or Data Support Specialist will certify that the secure data and user created project-based transitory files have been securely destroyed via a CRADC Certificate of Destruction. The completed 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 Certificate of Destruction supplied to Office of Sponsored Programs.

7. Data Center Specifications

a. Managed Environment: The CRADC servers managed environment is based on specialized security-limited functionality, with security taking precedence over functionality. System integrity of hardware and software is verified daily on the CRADC servers. The system administrator receives notifications from Microsoft of any patches or service packs that need to be applied to the operating system. All CRADC servers have Symantec Endpoint Protection software installed, and data files are scanned for viruses prior to being added to the environment. Real-time (automatic) file scanning is enabled and will quarantine or delete the file immediately. Security on the CRADC servers is monitored by the collection and review of system log files generated on all the systems and the Cisco ASA within the secure environment through a Security Information and Event Management (SIEM) application.

b. Maintenance: Monthly maintenance is accomplished the second Thursday of each month, based on hardware, operating system and applications requiring updates (i.e. BIOS, firmware, Microsoft security patches, service packs, and application revisions).

c. Physical Location:
    i. The CRADC servers and network attached storage (NAS) will be located in an environmentally controlled secure Data Center at Cornell University, Ithaca, NY.

    ii. Access to the Data Center will be granted by an authorized proximity card (Cornell University ID card) issued only to Cornell staff with the required credentials according to Cornell University Policy 8.4 -- Management of Keys and Other Access Control Systems. Entrance and exits to the Data Center will

be logged and monitored. The CRADC servers will be housed in racks with locked doors within the Data Center, to which only authorized administrators have keys.

d. Networking and Firewall: The CRADC servers will be installed behind a firewall with default deny applied and FIPS 140-2 security levels implemented.

Entities Affected by this Policy

CRADC Secure Data Services Manager, CRADC Secure Data Specialist, CISER Information Technology staff, and CRADC account holders.

Who Should Read this Policy

CRADC Secure Data Services Manager, CRADC Secure Data Specialist, CISER Information Technology staff, CRADC account holders and affiliated CRADC 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) 800-53
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

FIPS Publication 199
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS Publication 200
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.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	607-255-4081
Stephanie Jacobs	cradc@cornell.edu	CRADC Secure Data Services Manager	607-255-4081
Michelle Edwards	cradc@cornell.edu	CRADC Secure Data Specialist	607-255-4081
Janet Heslop	jheslop@cornell.edu	CISER Director of Information Technology and Security Liaison	607-255-4081
Kim Burlingame	Kb269@cornell.edu	CISER Sr. System Administrator	607-255-4081
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.

CRADC 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 Sr. System Administrator	Responsible for performing tasks in accordance with established policy guidelines.
CRADC Affiliated Staff	Responsible for knowing and assisting with tasks as related to this policy.
CRADC 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.

1 Refer to CRADC Account Provisioning and De-Provisioning Policy
2 Refer to CRADC Receipt, Storage and Possession of Restricted Data Policy
3 Refer to CRADC Restricted Data Backup Policy
4 Refer to CRADC Data Destruction and Certification Policy