CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: RD

Responsible Executive: CISER Secure Data Services Manager

Secure Standalone Desktop - CRADC Data Security Policy

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 11/10/17

Revised:

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 restricted-access data appropriately and effectively, secure standalone desktop 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 secure standalone desktop 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 secure standalone desktop.

    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 secure standalone desktop. Secure Standalone Desktop 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 Services staff may proceed with unique account creation. All temporary passwords, by group policy, must be changed upon initial login to the secure standalone desktop.

    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 Secure Standalone Desktop 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 Secure Standalone Desktop User Agreement.

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

    d. Idle Sessions: Idle sessions are suspended after 5-minutes of non-activity. If the Data Provider agreement establishes criteria requiring idle sessions be suspended after less than 5-minutes of non-activity, special requests will be accommodated.

    e. Authorization: Authenticated users have read and execute access to the restricted data provided under the Data Provider Data Use Agreement. Each user account has personal storage space and access to project-based 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 the Secure Data Services Support staff 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 the specific project folder on the hard drive of the secure standalone desktop secure. Authenticated users have read and execute access to the restricted data provided under the Data Provider Data Use Agreement. The user account has personal and project-based 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 being used on the secure standalone desktop. The local disk containing original restricted-use data files are not included in a routine backup.

    ii. Backups of Original Electronic Data Copies: 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 files (programs, output, log files and working datasets) housed on the secure standalone desktop are not included in a routine back up.

5. **De-provisioning of accounts**[1]
    a. Researcher Account De-provisioning: OSP communication initiates that an account should be de-provisioned. CISER Secure Data Services staff will contact the Principal Investigator (PI) and offer the PI the possibility to have the researcher's personal subfolder project files copied to the project's shared storage space. After 30-days, or sooner if the PI notifies CISER Secure Data Services staff 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 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.

    b. Destruction of Original Data Files on the Secure Standalone Desktop: The Secure Data Services staff will be responsible for the destruction of all original data on 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.

    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 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 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.

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 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.

7. Data Center Specifications

a. Managed Environment: The secure standalone desktop environment is based on specialized security-limited functionality, with security taking precedence over functionality. System integrity of hardware and software is verified quarterly. The system administrator receives notifications from Microsoft of any patches or service packs that need to be applied to the operating system. The secure standalone desktop has System Center Endpoint Protection (SCEP) 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 secure standalone desktop is monitored by the collection and review of security and system log files generated within the secure environment.

b. Maintenance: Monthly maintenance is accomplished quarterly, 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 secure standalone desktop will be located in Room 201H, 391 Pine Tree Road, at Cornell University, Ithaca, NY.

   ii. Access to room 201H is 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 are logged and monitored. A sign-in and sign-out sheet is also utilized for scheduling of the secure standalone desktop.

d. Networking and Firewall: The secure standalone desktop will have a Microsoft Windows Defender firewall with default deny applied.

ENTITIES AFFECTED BY THIS POLICY

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

Who Should Read this Policy

CISER Secure Data Services Manager, CRADC Secure Data Support Staff, CISER Information Technology staff, Secure Standalone Desktop 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	607-255-4801
Elena Goloborodko	cradc@cornell.edu	CISER Secure Data Services Manager	607-255-4801
Jonathan Bohan	cradc@cornell.edu	CRADC Secure Data 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.
CRADC Secure Data Services Support Staff	Responsible for knowing and assisting with tasks as related to this policy.
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.

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