CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: RD

Responsible Executive: CISER Secure Data Services Manager

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 5/11/15

Revised: 9/30/16

Sharing, Transmission and Distribution of Restricted Data

POLICY STATEMENT

This policy is to establish secure standards for the sharing, transmission and distribution of restricted data.

POLICY GUIDELINES

For the purpose of this document, restricted data relates to any nonpublic data that is protected by regulation, law or policy and/or is subject to contractual access restrictions as defined by a Data Use Agreement (DUA). Cornell Restricted Access Data Center (CRADC), as the Data Custodian of these data, along with the authorized research team (Researcher), are obligated to adhere to the conditions set forth by the Data Provider in a signed DUA and this policy.

Sharing:
The Researcher is authorized to access only the restricted data residing within the folders (and subfolders) on the CRADC computing system in accordance with their DUA to maintain the security and confidentiality of the encompassed data.

Providing anyone else with given credentials to access the restricted data or CRADC computing systems is strictly forbidden.

The Researcher is not to attempt to circumvent, or disable any of the security controls in place on the CRADC computing systems. If at any time the Researcher is aware of a potential security incident that may place the restricted data at risk of unauthorized access, it is the responsibility of the Researcher to contact CRADC's Security Liaison and abide by Cornell University Policy 5.4.2, Reporting Electronic Security Incidents.

Restricted data on the CRADC system may only be used for non-proprietary scientific research.

Transmission:
If permissible by the Data Provider, researchers may utilize either SFTP or HTTPS protocol to transmit restricted data. To secure access to use SFTP or HTTPS protocol, the Researcher must provide a pre-designated static IP address that is specific to a campus or industry location (no personal residences allowed). SFTP and HTTPS access is limited to the Researcher's personal project folder only.

Email or instant messaging should not be used to transmit restricted data. Nor should restricted data be placed on portable devices or media such as mobile phones, PDAs, USB drives, and CDs/DVDs unless allowable according to the DUA.

When required by the DUA, the CRADC Secure Data Services staff will disclosure proof any files uploaded to, or downloaded from, the CRADC computing system. Such files will be delivered by Cornell's Secure Dropbox service, SFTP or HTTPS to authorized IP addresses, or other methods considered appropriate by CRADC staff to insure compliance with the DUA.

Distribution:
Approved distribution methods for restricted data are Cornell's Secure Dropbox service, SFTP or HTTPS to an authorized IP address that is specific to a campus or industry location (no personal residences allowed), or methods vetted and considered appropriate by CRADC staff to insure compliance with the DUA.

Restricted data should only be distributed to known computing systems, with verified security measures in place prior to the transfer. Person(s) receiving the restricted data must have a current signed DUA that asserts an understanding of the required security protections, including the governed regulations, policies and laws, as appropriate.

ENFORCEMENT

Violations of this policy resulting in misuse of, unauthorized sharing of, unauthorized transmission of, or unauthorized disclosure or distribution of restricted data may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the University, or, in the case of students, suspension or expulsion from the University.

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

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

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.