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: 7/1/15

Revised: 9/30/16

CRADC Restricted Data Security Breach Reporting and Response Policy

POLICY STATEMENT

This policy establishes measures that must be taken to report and respond to a possible breach or compromise of restricted data, including the determination of the systems affected, whether any restricted data have in fact been compromised, what specific data were compromised and what actions are required for forensic investigation and legal compliance.

POLICY GUIDELINES

Cornell Restricted Access Data Center (CRADC) is committed to compliance of restricted data. 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). 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.

Reporting:
It is the responsibility of the Researcher to contact CRADC's Security Liaison in a timely manner, in accordance with Cornell University Policy 5.4.2, Reporting Electronic Security Incident, if the Researcher suspects or is aware of a compromise creating risk of unauthorized access to restricted data.

Response:

Upon receipt of such report, the CRADC Security Liaison, the CRADC Secure Data Services Manager, and the Sr. Systems Administrator will convene to review the report. Upon initial review, the Cornell University Security Office will be notified to assist, according to Cornell University Policy 5.4.2, Reporting Electronic Security Incident.

Process Steps:

1. Identify:
    a. Nature of incident to best of knowledge
    b. Identify data involved
    c. Establish Data Provider contact information
    d. Identify systems involved, remove from network if applicable
    e. Review applicable policies, regulations and/or laws involved
2. Recovery and Response:
    a. Contact Cornell University IT Security Office for assistance in forensics
    b. Secure the system and preserve it without change
    c. If deemed necessary, the Security Office will alert Cornell University Data-Loss Incident Response Team
    d. Resolve situation
3. Communicate:
    a. Contact Office of Sponsored Programs
    b. OSP will contact Data Provider to inform of current situation
    c. If required, notify individuals of data theft
4. Document:
    a. Create an incident report
    b. Document lessons learned
    c. Update necessary documentation

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
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.