CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: DA

Responsible Executive: CISER Data Librarian

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued:
Revised: 3/21/14

# CISER Data Archive Security Policy

## POLICY STATEMENT

The Data Security policy describes physical and information technology measures undertaken to protect CISER digital data collections from unauthorized access.

## POLICY GUIDELINES

All CISER file servers, which house the Data Archive, have Symantec Antivirus virus protection software installed, and data files are scanned for viruses prior to being added to the environment. Security on the CISER file servers is monitored by the collection and review of system log files generated on all the systems and the Cisco ASA.

**Data Center:** The CISER file servers are located in an environmentally controlled secure University data center, as part of CISER's commitment to take all necessary precautions to ensure the physical safety and security of the Data Archive. The data center maintains uninterrupted power supplies (UPS), fire prevention and protection system, physical intruder prevention and detection systems and environmental control systems.

Access to the data center 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 (Section 16.1 of this document) Entrance and exits to the data center are automatically logged and monitored by Cornell Information Technology staff (section 13.3.1. Cornell Information Technology Data Center Log Procedures) within the data center, the CISER file servers are housed in racks with locked doors, to which only authorized system administrators have keys.

**Authentication:**

**Public Access:** Authentication is not required for access to public-use datasets, if accessing via the CISER web catalog.

**Managed Access:** Where the Data Provider obligates, the user would be required to authenticate with CUWebAuth (Cornell NetID required) via the CISER web catalog or through a CISER computing account. The Microsoft Windows domain controller for the CISER computing research environment employs user-based authentication. A user's access is authenticated by Kerberos using an encrypted project- based unique username and password.

A strict password complexity policy is enforced as follows:

- Enforces password history to 24 passwords remembered;
- The password cannot be changed unless it is a minimum of 1-day old;
- Complexity requirements are enabled; and
- Storage of passwords using reversible encryption is disabled.

Passwords must be at least eight characters long and may not contain the user's first or last name and changed every 42 days.

Idle sessions are suspended after 15-minutes of non-activity.

**Terms of Use:** Terms of Use for the CISER Data Archive are maintained on the CISER web site

**Authorization**: Access to the Data Archive digital collection is preserved through Microsoft Windows NTFS permissions.

**Receipt of original media:** CISER will employ the highest standard of ingest processing to ensure the quality, integrity, and secure storage of datasets. Refer to the CISER Data Archive Data Collection Policy for ingest details.

**Storage of original Media and electronic copies:** Any original media/electronic data that is retained, will be stored in compliance with the CISER Data Archive Preservation and Storage Policy.

**Disposal/Decommissioning of data:** CISER reserves the right to decommission data and/or dispose of physical media. The data will be decommissioned/disposed of in line with the directives of the Data Provider.

**Backup:** Data is backed up by Cornell Information Technology EZ-Backup service.

**Security Incidents:** Reporting security incidents is mandated by Cornell University Policy 5.4.2, Reporting Electronic Security Incidents.

## Entities Affected by this Policy

CRADC Director, CRADC Data Custodian, CRADC Information Technology staff, and CRADC Users.

## Who Should Read this Policy

CRADC Director, CRADC Data Custodian, CRADC Information Technology Director, System Administrator, and all affiliated CRADC staff

## Related Documents

CISER Terms of Use:
http://ciser.cornell.edu/pub/policies/CISER_Terms_of_Use.pdf

CISER Data Archive Data Collection Policy
http://ciser.cornell.edu/pub/policies/CISER_Data_Collection_Policy.pdf

CISER Data Archive Preservation and Storage Policy
http://ciser.cornell.edu/pub/policies/CISER_Data_Preservation_and_Storage_Policy.pdf

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

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

## Contacts

If you have questions about specific issues regarding this Data Security Policy, call the following offices:

| | | | |
|---|---|---|---|
| William Block | block@cornell.edu | CISER Director | 607-255-4081 |
| Data Librarian | ciser@cornell.edu | CISER Data Librarian | 607-255-4081 |

## RESPONSIBILITIES

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

| | |
|---|---|
| CISER Data Librarian | Interpret this policy and provide clarification and education and implement operational and business processes to facilitate compliance. |
| CISER Director of Information Technology | Implement operational, physical, and technical equipment and tools to facilitate compliance. |
| CISER System Administrator | Responsible for performing tasks in accordance with established policy guidelines. |
| CISER Affiliated Staff | Responsible for knowing and assisting with tasks as needed related to this policy. |

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