

CORNELL UNIVERSITY
Cornell Institute for Social and Economic
Research Policy

POLICY
Volume: GP

Responsible Executive: CISER
Director of Information
Technology

Responsible Office: Cornell
Institute for Social and
Economic Research
Originally Issued: 4/3/14
Revised: 5/8/18, 12/18/18

CISER Terms of Use

POLICY STATEMENT

The CISER Terms of Use policy outlines the expectations for the use of CISER resources, including but not limited to, CISER web site, CISER Research, CRADC, and Data Archive. In addition, each CISER service has distinctive policies specific to usage obligations.

A majority of the CISER services do not require any form of registration, allowing you to visit our web site and Data Archive without telling us who you are. However, some services may require you to provide us with Personal Data. In these situations, if you choose to withhold any Personal Data requested by us, it may not be possible for you to gain access to certain services and for us to respond to your query.

Archive:

1. Users agree to adhere to any and all licensing requirements as stipulated by the providers of datasets held in the CISER Data archive.
2. CISER Data Archive non-public use files which require Cornell University authentication may not be distributed to anyone, other than direct affiliates with Cornell University (i.e. current faculty, staff, and student), or used for private consulting or for non-academic research.

Web Site:

1. As a visitor of the CISER web site certain data elements are automatically and anonymously collected. CISER uses the information that is collected in a variety of ways in providing the service and operating our business.

- a. Operations
 - i. CISER utilizes the information collected from IIS web logs and Cookies to maintain, enhance and provide services and information that you request, to respond to questions and to provide support.
- b. Improvements
 - i. CISER utilizes the information collected from IIS web logs and Cookies to understand and analyze usage trends and preferences of our visitors and users, to improve our services, and to develop new products, services, features and functionality.
- c. Communications
 - i. CISER never shares the information collected from IIS web logs and Cookies. The use is strictly for administrative purposes.

Computing Resources:

1. Our statistical software may not be used for private consulting or for non-academic research. Users may not distribute licensed software from our systems to themselves or for any other persons.
2. The CISER file server may not be used for personal e-mail, personal multi-media (e.g. audio, images, photos, video files), nor backup of your personal computers or non-research files.

Computing Accounts:

1. CISER computing accounts and passwords may not be shared with any other person. Sharing passwords and/or account information is against CISER's policy, as well as Cornell's Abuse of Computer and Network Systems policy.
2. It is the responsibility of every CISER computing account holder to keep CISER apprised of any changes to the information provided in your account application, including change in affiliated faculty member, academic status, and your contact information.
3. CISER may collect personally identifiable information about you, such as your full name, phone number and email address when you register for an account. Personal Data is securely stored for the purposes of providing support services, analyzing computing usage statistics and maintenance communications.
4. Any files left on the CISER file server after an account has expired will be made available to the affiliated faculty advisor, if requested, within 60-days of account expiration. On day 61, the account will be closed and all data files will be deleted. CISER will not maintain a backup of any user data.

5. Users are responsible for complying with all applicable federal, state and local laws and must abide by Cornell University policies which are in line with generally accepted higher education policies. Any misuse of computing resources, proprietary software, or data violates the Cornell University Campus Code of Conduct and the Policy Regarding Abuse of Computers and Network Systems.
6. CISER reserves the right to disable a computing account immediately upon identification of possible misuse of any CISER services, or non-compliance with CISER or Cornell University policies. Account termination will occur if misuse is confirmed through proper authorities, and no reinstatement will be allowed.
7. By applying for an account and using CISER computing resources, you acknowledge all of the policies above and agree to adhere to them.

REASON FOR POLICY

To ensure that CISER clients understand their obligations in relation to use and misuse of data and associated services provided by CISER.

ENTITIES AFFECTED BY THIS POLICY

CISER Clientele

WHO SHOULD READ THIS POLICY

All clientele of CISER services, including but not limited to students, faculty, alumni, staff, and researchers at Cornell University, as well as external affiliates.

RELATED DOCUMENTS

Cornell University Policy Library

<https://www.dfa.cornell.edu/tools-library>

Cornell University Campus Code of Conduct

<https://www.dfa.cornell.edu/tools-library/policies/campus-code-conduct>

Cornell University Policy Regarding Abuse of Computers and Network Systems

<http://www.it.cornell.edu/policies/university/privacy/abuse/index.cfm>

CISER Policy Library

<https://ciser.cornell.edu/about-us/ciser-policies/>

CONTACTS

If you have questions about specific issues regarding this CISER Terms of Use Policy, call the following offices:

William Block	block@cornell.edu	CISER Director	607-255-4801
Janet Heslop	jheslop@cornell.edu	Director of Information Technology and Security Liaison	607-255-4801

RESPONSIBILITIES

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

Director of Information Technology	Oversee the implementation of operational, physical, and technical equipment and tools to facilitate compliance.
CISER Clientele	Responsible for understanding obligations and complying with this policy.

As determined by university administration, any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.