CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: SY

Responsible Executive: CISER Director of Information Technology

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 10/30/17

CISER Systems Use Policy

POLICY STATEMENT

CISER computing resources, including but not limited to, CISER Research or CRADC, are provided to support the evolving computational and data needs of Cornell social scientists and economists throughout the entire research process and data life cycle. The appropriate use and protection of all systems and associated resources is expected from all clients including faculty, students, employees, and visitors throughout the institution.

POLICY GUIDELINES

CISER computing resources (accounts, servers, software applications, file storage, data archive, etc.) are provided for research and academic needs only. Research and academic usage includes use associated with Cornell-approved research, class work for which you are currently enrolled, and staff work associated with supporting the mission of Cornell University.

CISER computing resources may not be used for any personal purposes, including but not limited to storage or backup of personal files (e.g. audio, images, photos, video files), personal email, use of social media, private consulting or business-related activities, watching streaming video or any other personal activities.

CISER related accounts and passwords may not be shared with any other person. Sharing passwords and/or account is against CISER's policy, as well as Cornell's Abuse of Computer and Network Systems policy.

CISER servers are a limited shared resource available to multiple clients at any time. Each client is expected to maintain an acceptable level of performance and must assure that excessive or inappropriate use of the resources does not degrade performance for others.

CISER provides multiple levels of secure computing environments. It is the client's responsibility to select the appropriate level of technical security to assert compliance with the terms and conditions, as well as laws and regulations, required for the type of data intended to use.

CISER reserves the right to disable access to any and all CISER services immediately upon identification of possible misuse. Access termination will occur if misuse is confirmed through proper authorities, and no reinstatement will be allowed.

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 Clients

Who Should Read this Policy

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

Related Documents

Cornell University Policy Library
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/index.cfm

Cornell University Campus Code of Conduct
http://www.policy.cornell.edu/Campus_Code_of_Conduct.cfm

Cornell University Policy Regarding Abuse of Computers and Network Systems
https://it.cornell.edu/policy/policy-50-abuse-computers-and-network-systems

CONTACTS

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

William Block	block@cornell.edu	CRADC Director	607-255-9026
Janet Heslop	jheslop@cornell.edu	Director of Information Technology	607-255-8531

RESPONSIBILITIES

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

CRADC Director of Information Technology	Implement operational, physical, and technical equipment and tools to facilitate compliance.
CISER Clients	Responsible for understanding obligations and complying with this policy.

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