ECONOMIC ROUNDTABLE
CONFIDENTIAL DATA MANAGEMENT POLICY

The following guidelines approved by the Board of Directors on September 17, 1999 and revised on January 10, 2007, apply to all confidential data files to which the Economic Roundtable is granted access. Confidential data includes records with individual identifiers such as name, taxpayer identification number, client identification number, address, telephone number, or date of birth. The purpose of this policy to protect the privacy of individuals and entities whose records are studied by the Economic Roundtable, uphold the Economic Roundtable's policy on the protection of human subjects, and ensure compliance with data security requirements set forth by the organizations that provide confidential data.

1. **Compliance with Terms for Obtaining Data**: Any data security provisions required as a condition for obtaining and using specific confidential data sets that are not specified in this policy shall be followed in addition to these provisions whenever using those confidential data sets with additional security requirements.

2. **Security Oversight**: A data manager, appointed by the President of the Economic Roundtable, is responsible for maintaining compliance with confidential data agreements. Members of the Board of Directors and of its Institutional Review Board may visit the Economic Roundtable office on any business day, unannounced, to review storage and security of data. Responsibilities of the data manager shall include:
    a. Ensuring that all staff and collaborating researchers receive a copy of the Economic Roundtable's confidential data management policy.
    b. Maintaining a log that identifies all accesses to confidential data files, including source/location of access, beginning and ending dates, user, activity performed, and any record and field modified.
    c. Carrying out a risk analysis with sufficient regularity to identify and assess vulnerabilities associated with all information assets owned, maintained, or used by the Economic Roundtable that are used to process or store confidential information, and identifying cost-effective approaches to managing such risks. Specific risks that shall be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of employees and outsiders; fire, flooding, and electrical disturbances; and loss of data communications capabilities.
    d. Ensuring that security patches and upgrades released by the respective manufacturers of the components of the information assets used to process confidential data are promptly applied to the components. Patches and upgrades downloaded from public networks shall be applied only if digitally-signed by the source and only after the data manager has reviewed the integrity of the patch or upgrade.
    e. Implementing security measures to physically protect data, systems and workstations from unauthorized access and malicious activity.

f. Establishing and implementing contingency plans for the Economic Roundtable's information assets containing confidential data to ensure that operations can be back to normal in minimum time after natural or man-made disasters, unintentional accidents, or intentional acts such as sabotage. These plans shall include, but not be limited to the regular backup of automated files and databases, secure storage, recovery, and restarting procedures.

g. Maintaining a current list of personnel authorized to access each confidential data set, and ensuring that former employees and individuals no longer involved in the research projects associated with each data set are removed from the list.

h. Restricting access to each confidential data set to those individuals currently authorized to work with the data.

i. Carrying out ongoing monitoring of the use of confidential data to ensure compliance with the provisions set forth in this policy and confidentiality agreements with each organization providing confidential data.

j. Restricting the removal of confidential data from the authorized work location.

k. Reviewing all data outputs prior to removal from secured work areas to ensure that they are in an aggregated and non-confidential form. Personal identifiers must be removed or recoded with random identifiers.

l. Preventing unauthorized access to or viewing of confidential records by unauthorized persons, whether in work areas, in transit, or in storage.

3. **Physical Security**: The following procedures will be followed to ensure the physical security of confidential data:

    a. Computer media used to store confidential data (diskette, CD-ROM, tape back-up) are to be kept secure in a locked cabinet in the Economic Roundtable office, accessible only by the President and the data manager.

    b. The Economic Roundtable office in which secure data is stored shall be located in a building with 24-hour security.

4. **Access to Data**: Only authorized employees and collaborating researchers shall be allowed access to confidential data.

    a. Only individuals carrying out approved research that requires them to use confidential data shall be considered for authorization to have access to confidential data.

    b. As part of the authorization process, individuals who are candidates for working with confidential data shall be instructed regarding the constraints for handling confidential data:

        i. The confidential nature of the information, and

        ii. The sanctions against unauthorized use or disclosures found in the law as well as Economic Roundtable policies.

    c. To become authorized to use confidential data staff members must be approved by a corporate officer of the Economic Roundtable as well as by the agency

providing the data (if required by that agency), and must sign all confidentiality agreements required for the project for which the data was obtained.

5. **Limitations in the Use and Disclosure of Data**: Confidential data shall be used only for authorized purposes.
    a. Confidential information shall not be disclosed to any other person or entity without prior written approval from the organization providing the data.
    b. In publishing information, no individual or business entity whose identity was obtained through confidential sources shall be identified.
    c. Geographic identities may be specified only in areas that include five or more individuals in order to protect confidentiality.
    d. All work products containing any material derived from confidential data must be reviewed to ensure that they comply fully with these policies as well as the terms of the applicable confidentiality agreement(s) prior to distribution or public release.

6. **Security of Electronic Data**: Information in electronic format, such as computer memory or electronic memory media, must be stored and processed in such a way that unauthorized persons cannot retrieve the information by computer, computer network, remote terminal, physical removal of storage media, or other means. The following procedures shall be followed to ensure the security of confidential data in electronic format:
    a. Computers that store confidential data must be password protected by alpha-numeric passwords that are unique to each computer and known only by the assigned, authorized computer user and the data manager.
    b. If non-approved staff members are to work on a computer that has stored confidential data, all confidential files must be removed from the hard drive prior to use of that computer by the non-approved staff member
    c. Confidential data shall not be used or stored on wireless devices. This prohibition includes notebook computers and Personal Digital Assistants (PDAs) equipped for 802.11x wireless networking.
    d. Individual identifiers shall be removed from confidential data, substituted by unique random identifiers, as soon as possible after receipt of confidential data.
    e. Confidential data shall be encrypted when transmitted or stored. Non-proprietary, secure, generally-available encryption software such as FineCrypt version 9.1 or equivalent shall be used. Data encryption shall meet the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES).

7. **Security of Printed Data**: Confidential data shall not be printed unless there is a compelling need to do so. Any printed material containing confidential data shall be stored in stored in a locked file cabinet. Access to the key shall be highly restricted.

8. **Transmission of Data**: Procedures for ensuring the security of confidential data transmissions shall include:
    a. All confidential data that is transferred on tapes, cartridges or CDs shall be encrypted and placed in separate files with identifiers and a crosswalk on one file, the crosswalk and remaining data on another file, with the files transported separately. Additionally, the tapes, cartridges and CDs shall be delivered using a bonded accountable mail service.
    b. Confidential data shall not be transferred via File Transfer Protocol (FTP) or as an e-mail attachment even if the file is encrypted.
    c. Confidential data shall not be transferred via fax.
    d. Paper copies of confidential data shall be mailed using double envelopes and shall be delivered using a bonded accountable mail service.

9. **Dissemination of Security Policy:** Copies of this policy shall be provided to all staff and collaborating researchers.