14.1 Network and Computing Services Policy

Current Revision Effective Date:	08/14/2023
Original Effective Date:	02/01/2008
Contact:	OCISO@rti.org

Policy Statement

It is the policy of RTI to provide to its staff and other Users the resources to electronically communicate, share information, and process data—an essential component of RTI's research and administrative operations. To this end, RTI staff require access to computing Resources both within and from outside RTI and access to computing resources external to RTI, including the Internet and the World Wide Web. At the same time, RTI's systems and Data must be kept secure in a manner that balances research staff's needs for an open, creative environment with the realities of client requirements and the vulnerabilities introduced by the use of information technology.

Data accessed, transmitted, or stored through the Network is a critical component of the daily functioning of RTI and as such is the property of RTI and/or RTI clients. Access to the Data and network is a privilege and must be so treated in accordance with RTI's Code of Conduct. Users must employ Resources in a responsible manner, respecting the trust through which the Resources have been provided, the integrity of facilities and controls, and all pertinent laws and RTI policies and standards.

Use of Resources is governed by this policy regardless of who owns the Data, location, or the User's employer.

Responsibility for Data Security

Office of the Chief Information Security Officer (OCISO) is responsible for establishing security standards for the RTI network and computing facilities. System administrators are responsible for maintaining the protection of data and resources following OCISO standards. In pursuing this goal, GTS will perform the following:

- Establish and enforce policies, procedures, and standards.
- Define acceptable use of Resources.
- Provide security awareness and training.
- Actively monitor for information security threats that would compromise the ability of RTI to fulfill its mission.

OCISO reserves the right to limit or restrict the use of Resources as deemed appropriate by the Chief Information Officer (CIO) or defined by GTS Information Security Policy (ISP). RTI will promptly investigate all reports or indications of policy violation as per the RTI 14.1.3 Acceptable Use Procedure.

GTS distributes Credentials to Users in order to facilitate access to Resources and Data. Users are accountable for all actions performed using assigned Credentials.

Training

- All Users must complete approved security awareness training no later than 30 days after being granted access to any resource.
- All Users must complete annual GTS security awareness training.
- All Users must report any suspected violation of policy and actively protect the information assets of RTI.

Persons Affected

All RTI International staff and contractors

Definitions

Credentials: A set of parameters that establishes the positive identity of the User.

Data: Data, or information assets, refers to any electronic information that can be stored or transmitted.

Network: A collection of both physical and logical assets that facilitate access to Data by Users.

Resources: Includes, but is not limited to, Data, Network, computing equipment, software, and telephones used to conduct business on behalf of RTI.

Users: A broad term used for anyone who interacts with RTI Resources. For purposes of this document, and subsequent GTS policy, Users includes all RTI employees and contractors, including vendors and agents, who provide services and resources to RTI or organizations and individuals accessing the Network. Users must understand and comply with RTI information security policies, standards, and procedures regarding the protection of RTI information system assets.