



14.1.1 Rules of Behavior Procedure

Current Revision Effective Date:

03/06/2024

Original Effective Date:

02/01/2008

Contact:

OCISO@rti.org

Procedure Statement

Preserving access to Data and Resources is a community effort that requires each User to act responsibly and guard against abuses. Therefore, Users have an obligation to abide by the standards of acceptable and ethical use as laid out in this procedure.

RTI provides the tools to communicate, share, and process information which is essential to fulfill the mission of RTI. At the same time, RTI's systems and data must be kept secure in a manner that balances staff's needs for an open, creative environment with the realities of client requirements and the risk of losing information. As such, information security is the responsibility of all RTI staff. Failure to comply with the following Rules of Behavior and applicable RTI Policies and Procedures may result in disciplinary action up to and including dismissal.

Resources

Resources that are provided to Users are intended for the purpose of conducting business. Use of Resources and Data must be in compliance with applicable laws, regulations, and licensing agreements. All use of Resources and Data may be intercepted, monitored, recorded, copied, and inspected by GTS. Users should have no expectation of privacy in this regard. Users' right to privacy is superseded by RTI's requirement to protect the integrity of Resources. Occasional use of Resources for personal purposes is permitted if use does not negatively impact RTI business, does not compromise security, and is in full compliance with all other RTI policies and procedures. RTI IT systems should be used when conducting RTI business.

GTS will provide credential management (e.g., Username and Password) services for users. GTS uses credentials to manage access to IT resources and data, and to ensure individual accountability in the use of RTI IT resources.

User Accountability

Users may only use Resources for which they are authorized and must protect the access and integrity of Resources. **Users who have received elevated privileges are only allowed to access systems which they have been directed to access.** Passwords must not be shared with anyone. Passwords must not be revealed in written documents or electronic formats. Users must ensure that a backup exists of all Data and that security is maintained appropriately. Users are expected to use Resources in a productive manner and are responsible for Data that they transmit, store, or display. Users may not use Resources for private gain or any purpose that is illegal or against RTI policy or contrary to RTI's best interests. Examples include, but are not limited to, promoting personal political views, fund-raisers, or religious beliefs unless specifically approved by Corporate Communications.

Messaging

RTI messaging systems, such as e-mail accounts, are to be used for RTI business. Users will not use Resources to distribute fraudulent, harassing, or obscene materials. The use of personal "disclaimers" or signatures in electronic messages do not absolve the User from association with the content of messages; sent or received. Users may not engage in the transmission of unsolicited bulk e-mail ("spamming") or chain letters unless coordinated with GTS and for the purpose of conducting business. Users must not use personal messaging accounts for RTI business.

Data Security

All resources attached to RTI Networks must comply with applicable GTS security controls. Users will not attempt to circumvent security systems and may not store or execute programs, or engage in any activities designed to test or compromise system or network performance, without authorization from the Chief Information Officer (CIO). Users will not inspect, alter, delete, obtain copies of, publish, transmit, or otherwise tamper with Data for which they are not authorized. users must report any violation of these Rules of behavior or applicable policies to * [Help Desk \(GTS Security\)](#).