



14.1.3 Acceptable Use

Current Revision Effective Date: 06/18/2024
Original Effective Date: 05/29/2019
Contact: OCISO@rti.org

Procedure Statement

The purpose is to establish, define and communicate RTI's expectations for RTI Users when using or accessing RTI's information technology systems or services ("IT Resources" defined below), including connection of any device to any RTI network or information system. RTI Users will be asked to affirmatively agree to comply with this Acceptable Use Policy ("AUP") on an annual basis. Only Users in compliance with this AUP are authorized to use and/or access IT Resources.

IT Resources comprises equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term includes computers, mobile devices, ancillary equipment, software, services, including network and support services, and related resources at RTI. This Acceptable Use Policy ("AUP") sets forth the standards by which all Users may use IT Resources owned or managed by RTI.

IT Resources are provided to support RTI and its mission and vision. Any other uses, including uses that jeopardize the integrity of IT Resources, the privacy or safety of other Users, the privacy and confidentiality of Client data or that are otherwise illegal are prohibited. The use of IT Resources is a revocable privilege.

User Responsibilities

General requirements for acceptable use of IT Resources are based on the following principles:

1. Each User is expected to behave responsibly and, in a manner, consistent with RTI's Code of Conduct with respect to IT Resources and other Users at all times.
2. Each User is expected to respect the integrity and the security of IT Resources and data.
3. Each User is expected to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use IT Resources and show restraint in the consumption of shared resources.
4. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.
5. Each User is expected to cooperate with RTI when investigating potential unauthorized and/or illegal use of IT Resources.

Use Prohibitions

Without limiting the general guidelines listed above, unless expressly agreed to by the Chief Information Officer (CIO), the following activities are prohibited:

1. Users may not attempt to disguise their identity, the identity of their account, or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate RTI's name, network names, or network address spaces.
2. Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not engage in cyberstalking or infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.
3. Users may not use IT Resources in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any IT Resources, or any network that RTI connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by RTI, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others.
4. Users may not store, display, or disseminate unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography, or other illegal communications. This provision applies to any electronic communication distributed or sent within IT Resources or to other networks while using IT Resources.
5. Intentional access to or dissemination of pornography by any User is prohibited unless such use is specific to work-related functions and has been approved by the Office of Compliance or the Office of Corporate Counsel. This provision applies to any electronic communication residing on, distributed, or sent using IT Resources, including to other networks while using IT Resources.
6. Users may not attempt to bypass network security mechanisms, including those present on IT Resources. The unauthorized network scanning (e.g., vulnerabilities, port mapping, etc.) of IT Resources is also prohibited. To request network scans, users must contact GTS Security by sending a request to the GTS Helpdesk.
7. Users must not use IT Resources to violate copyright, patent, trademark, or other intellectual property rights. Examples of such violations would include engaging in the unauthorized copying, distributing, altering, or translating of copyrighted materials, software, music, or other media without the express permission of the copyright holder or as otherwise allowed by law. Note that Journals have differing rules regarding how they protect their copyright, and Users should carefully review the rules of a Journal before copying or re-using material.
8. Users may not extend or share the RTI network with the public or other Users beyond what has been configured accordingly by GTS. Users are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the RTI Network without advance notice to and approval by GTS.
9. Users may only connect personal devices to the RTI network for approved RTI business purposes.
10. Users must not copy RTI data to personally owned devices unless approved by the Office of Privacy and Data Protection. Removal of data from RTI systems or systems in the custody of RTI that violates RTI policies or procedures may result in disciplinary action up to and including termination. If you have questions regarding an acceptable use of RTI data or data in the custody of RTI, please contact the Office of Privacy and Data Protection before copying the data.
11. Users must not engage in activity that may degrade the performance of IT Resources, deprive an authorized User access to Resources, obtain extra Resources beyond those allocated, or circumvent information security measures.
12. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved by the RTI CIO.

13. IT Resources must not be used for personal benefit, political activity (see P&P 1.33 Political and Government Relations Activities), unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
14. Users must not allow family members or other non-employees to access IT Resources.
15. Users may only communicate or share RTI private IP addresses for RTI assets such as servers or computers to external parties via a secure transit mechanism (e.g., secure FTP, secure SharePoint site, secure client web portal), and in a form that is encrypted, and only after obtaining express permission of the Office of the Chief Information Security Officer. "External parties" includes but is not limited to, third party vendors, subcontractors, consultants, and clients. Assistance for responses to requests for this information should be directed to RTI's Chief Information Security Officer or RTI's Office of Privacy and Data Protection.
16. Users must not communicate or share RTI information security, data privacy or data protection policies or procedures about RTI assets or systems with external parties without the permission of RTI's Office of Privacy and Data Protection or RTI's Chief Information Security Officer. "External parties" includes but is not limited to, third party vendors, subcontractors, consultants, and clients. Requests for copies of policies or procedures should be directed to RTI's Office of Privacy and Data Protection or RTI's Chief Information Security Officer.

IT Security and Monitoring of IT Resources

RTI may review and/or monitor any use of IT Resources. Review or monitoring of use of IT Resources may occur in, but is not limited to, the following circumstances if deemed necessary by authorized personnel:

1. in accordance with generally accepted, network-administration practices
2. to prevent or investigate any actual or potential information security incidents and system misuse
3. to investigate reports of violation of RTI policy or local, state, or federal law
4. to comply with legal requests for information (such as subpoenas and public records requests), or
5. to retrieve information in emergency circumstances where there is a threat to health, safety, or RTI property involved in response to EVP's request

RTI, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter in its sole discretion.

Compliance

Penalties for violating this Policy may include restricted access or loss of access to IT Resources.

Failure to comply with this policy may put RTI information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Staff who fail to adhere to this policy may be referred to the Chief Information Officer. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with RTI.

Violation of this policy may also carry the risk of civil or criminal penalties.