Information Security Policy

Effective: November 2020

Updated: July 2024

Governing Laws, Regulations, and Standards

Guidance	Section / Link
BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy	Binding Operational Directive (BOD) 20-01.
Cybersecurity Maturity Model Certification (CMMC) Domains	The current version of the CMMC framework consists of a matrix, composed of "Domains," "Capabilities," and "Practices and Processes." The model contains 18 different Domains of "key sets of capabilities for cybersecurity," 14 of which use the same terminology as the security requirement families in NIST Special Publication (SP) 800-171. Acquisition & Sustainment
HIPAA Security Rule	Health Insurance Portability and Accountability Act - NIST SP 800-66 HIPAA Security Rule|NIST
International Organization for Standardization (ISO) 27001	ISO - International Organization for Standardization ISO/IEC 27001 is an internationally recognized security standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain, and continually improve the ISMS.
National Institute of Standards and Technology (NIST) SP 800-53	NIST SP 800-53 database represents the controls defined in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53r 5 Control Families Crosswalks | NIST

Roles and Responsibilities

Roles	Responsibility
All RTI Staff and Contractors	Comply with requirements set forth in this policy; acknowledge read and understand training.
Chief Information Officer	The Chief Information Officer (CIO) is the company executive responsible for the management, implementation, and usability of information and computer technologies.
Chief Information Security	The Chief Information Security Officer (CISO) is the executive

Officer (CISO)	responsible for an organization's information and data security.
Global Technology Solutions (GTS)	Responsible for the governance of RTI's network, maintenance of the infrastructure, and functionality of corporate systems.
Office of the CISO	The Office of the Chief Information Security Officer (OCISO) staff serve in a segregated role and are responsible for keeping up to date on the latest IT compliance practices and regulatory requirements. The OCISO Managers and staff will assist to ensure that all network, digital and information technology related activities of RTI and its staff are conducted in agreement with RTI, the ISMS and IT Policies, Procedures and regulatory security compliance practices and standards. The team can be reached by emailing OCISO@rti.org.
RTI Vendors and Contractors	Comply with requirements set forth in this policy; acknowledge read and understand training.

Definitions

Term/Acronym	Definition
Document Management System (DMS)	A system used to retrieve, track, manage and store documents.
Information Security Management System (ISMS)	A set of policies concerned with information security management or IT related risks.
Vulnerability	a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." *-CISA*
Vulnerability Disclosure	"act of initially providing vulnerability information to a party that was not believed to be previously aware". *-CISA*

Introduction

This comprehensive Information Security Policy (ISP) provides information on the RTI | IT prescribed measures used to establish and mandate the IT security program for compliance to both internal and external data protection requirements. Information Security is everyone's responsibility and to ensure an effective security position is a team effort involving the participation and support of every RTI system user who interacts with data and information systems. Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and store this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats and vulnerabilities, as well as controls to ensure confidentiality, integrity, and availability of the data:

- **Confidentiality** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- **Integrity** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems.

Purpose

The purpose of this policy is to highlight the company and regulatory requirements under which RTI staff shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.
Implementing an Information Security Management System (ISMS) and consistent security controls within RTI helps the institute comply with obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of RTI and client data.

This policy summarizes the comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of RTI's data and related information systems.
- Protecting RTI, its employees, and its clients from unauthorized use of RTI owned and/or managed information systems and data.
- Ensuring the effectiveness of security controls over data and information systems owned and/or managed by RTI that support the Institute's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective management and oversight of Information Security risks.

Scope

This policy applies to all RTI employees, vendors, contractors, sub-contractors, as well as all RTI-owned or IT Administrator-managed data, information systems, activities, and assets owned, leased, controlled, or used by RTI. Any other systems, assets or activities not owned by RTI or maintained by RTI's IT Department, IT Administrator, are not included in this policy.

General Information Security Controls

The RTI security control policies align with the National Institute of Technology (NIST) framework, which is updated accordingly, and have been developed to define a minimum level of security and control across RTI. Any unauthorized exceptions to the ISMS and/or standards will not be permitted. These standards and the ISMS go into effect upon the initial publication of this document.

Business Units may provide more rigorous security and control solutions and standards beyond what has been required in the RTI 14.1 Network and Computing Security Policy and associated procedures.

All employees, contractors, and others who have access to RTI facilities and information assets must be made aware of the ISMS, Acceptable Use, and security policies within 30 days of hire (for employees) or prior to being given such access (for contractors) and at least annually thereafter. Security responsibilities are specified in job descriptions, through RTI policies, procedures, and contracts (as applicable), and compliance with RTI Information Security Awareness training is monitored and enforced by Office of the CISO in coordination with Enterprise Risk Management. For the purposes of this statement, Security Awareness refers to employee's awareness of the Information Security Management Systems (ISMS), Information Security policies, standards, and practices.
Some network activities shall be monitored and logged to ensure compliance with the rules established in this and other IT policies, standards, procedures, and guidelines.

External Regulations

Any systems connected to the RTI network or that store RTI or Client data will meet applicable requirements set forth by external regulations. Such regulations may include but are not limited to:

- EAR and Export-controlled data
- Federal Information Security Modernization Act of 2014 (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
- Validated (GxP) Systems
- Title 21 CFR Part 11 Electronic Signatures

If a client contractual requirement is more stringent than security baseline controls or regulatory mandates implemented at RTI, the contract will take precedence and IT Administrators must be notified of the requirements.

Information Security and Classification of Electronic Information

All client and enterprise information held by RTI, and information contracted by RTI to be held by third parties, are classified, and protected. The Office of the CISO creates and maintain standards regarding the use and disclosure of client and enterprise electronic information. RTI client and enterprise electronic information may only be used and disclosed for RTI business purposes. Information obtained from or on behalf of RTI's clients, vendors or other third parties may be used and disclosed only as permitted by the contracts with, and representations made to those third parties. Please refer to the RTI Policy 14.2 Information Security and Classification of Electronic Information and supporting procedures for the classification and handling of electronic data.

IT Operations Management Security

IT Administrators will create and maintain procedures that support this Policy and designate roles and responsibilities for the secure management and operation of all information processing facilities. This includes the development of appropriate operating instructions. IT Administrators will:

- Deploy code controls adequate to detect and prevent the introduction of malicious software.
- Deploy controls to adequately protect exchanges of information and software with third parties to ensure the security of the transaction as well as compliance with applicable laws.
- Enact standards to protect information and media in transit as defined in IT standards.
- Manage changes to the IT infrastructure to minimize the likelihood of outages and reduce the risk of negatively impacting RTI's IT security posture.

Data protection considerations are built into information systems and applications. This will include infrastructure, commercial products, and applications either developed internally or via outsourcing and client-facing applications hosted by both RTI and clients. All security requirements are identified and agreed to during the requirements -setting of a project and documented.

Appropriate controls and audit trails or activity logs must be designed into application systems including the validation, authorization, and authentication of access controls. Additional controls might be required for systems that process or have an impact on sensitive, valuable, or critical organizational assets.

IT Administrators will incorporate cryptographic controls, when applicable, to protect the confidentiality, integrity, and authenticity of information. In addition, IT Administrators will provide adequate protections for source code and incorporate technical security testing into development processes, lifecycles, and quality assurance.

IT Administrators will utilize change control, vulnerability scanning, security development, and testing processes to ensure the security of the system(s) and the operating environment(s) are not compromised. IT Administrators will implement and adhere to secure development practices and standards as specified by applicable regulations and law to their line of business.

Legacy RTI application products that have operationally survived longer than their capability to be sustained with relevant security patches and features to mitigate evolving threats are sunset or otherwise isolated from RTI's IT infrastructure.

Office of the CISO

The Office of the Chief Information Security Officer (OCISO) promotes a culture of shared responsibility to safeguard RTI by maturing the cybersecurity and resiliency of systems and information. The OCISO team's services are designed to assist the Institute by identifying, assessing, monitoring, and forecasting threats to information assets, advising on risk management and on contracts related to data security, providing Information Security Awareness training, consulting/advising on incident management, and developing and managing RTI policies related to information security. The Office of the CISO can be reached at OCISO@rti.org.

Compliance with legal and contractual requirements:

- All applicable compliance requirements are identified, documented, and well-maintained.
- Records are properly managed to avoid any destruction from natural disasters, unauthorized use, or loss.
- Personally Identifiable Information (PII) and Protected Health Information (PHI) are properly protected.
- Any cryptographic controls are used appropriately according to relevant compliance requirements.

Compliance with security policies and standards:

- At least annually, OCISO (or designated third party) will perform reviews or audits of users' and systems' compliance with the ISMS, security policies, standards, and procedures, and initiate corrective actions where necessary.
- Results from compliance reviews or audits shall be documented and reported by IT SLT.

Information system audit considerations:

- OCISO implements audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.
- IT information systems are enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

Policy Statements

IT Administrators shall design, implement, and maintain a coherent set of standards and

procedures to manage risks to data, in an effort to ensure an acceptable level of Information Security risk and alignment with the ISMS. Through these standards and procedures, RTI will protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its information systems and data, regardless of how it is created, distributed, or stored. Security controls are tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

a. Exceptions

While every exception to a policy or standard potentially weakens protection mechanisms for RTI information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in section Risk Acceptance Approval Process.

b. Updates

Updates to the Policy are announced to employees via management updates or email announcements. Changes are noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, and guidelines.

c. Monitoring

IT reserves the right to monitor RTI computer resources and/or Users at any time and for any reason (including compliance with this policy). Anyone using or accessing a RTI computer resource is deemed to have consented to such monitoring.

Policy: Access Controls (AC)

The purpose of this policy is to ensure users have the appropriate access levels specifically authorized to them to access information on systems and applications and that individuals understand the responsibility their access level provides them. This policy defines access control standards for system use notices, remote access, and definition and documentation of relationships for information systems. IT Administrators will create and maintain standards regarding information access controls. The minimum requirements for user credentials and the management of those credentials, as well as the Physical Access to RTI Data Center and Environmental Standards are defined in the supporting standard operating procedures.

Access privileges granted to an individual are for the sole use of that individual and are not to be shared. This includes, privileges granted via card key, username and passwords, keys, tokens, and access to RTI applications, systems, network assets, and resources. All granting of privileges must be controlled through proper approval processes and authentication mechanisms. Duties of individuals are separated to reduce the risk of malevolent activity without collusion.

a. Individual account permissions are not allowed on file shares.
b. Upon termination of employment, an employee's or external party's user access rights are revoked.
c. Asset owners must conduct regular reviews of users' access rights and use of accounts.
d. Unsuccessful logon attempts are limited.
e. Time and date of logons and account changes are appropriately recorded and monitored.

f. To prevent access/viewing of data after period of inactivity, session lock with pattern-hiding displays are used.
g. Password management systems are interactive and mandate strong passwords.
h. Remote access sessions are monitored and controlled.
i. Wireless access are protected using authentication and encryption.
j. Connections to and use of external information systems are verified, controlled, and limited.

Policy: Audit and Accountability (AU)

The purpose of the Audit and Accountability Policy is to ensure that major applications and general support systems are evaluated on a continual basis in accordance with OMB Circular A-130, FISMA and other applicable federal, state, and local guidelines. The quality and integrity of RTI's system monitoring and auditing is used to determine if inappropriate actions, either intentional or unintentional, have occurred within an information system. System monitoring is used to look for these inappropriate actions in real time while system auditing looks for them after the fact. Without system auditing and assigned accountability, it can be difficult, if not impossible, to determine when a failure of the information system security, or a breach of the information systems itself has occurred, the magnitude of the breach or failure, and the details of that breach or failure.

1. Event audit logs contain system generated audit records that contain information to establish what events occurred on the system, the source(s) of the events, and the outcome of the events.
2. Audited events are reviewed and updated.
3. IT Administrators create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
4. IT Administrators ensure that the actions of individual information system users can be uniquely traced to those users.
5. IT Administrators correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
6. Audit information and audit tools are protected from unauthorized access, modification, and deletion.

Policy: Assessment, Authorization and Monitoring (CA)

The quality and integrity of RTI's security assessment is focused on determining the degree to which information system security controls are correctly implemented, whether they are operating as intended, and whether they are producing the desired level of security. Vulnerability assessment is focused on determining the weaknesses inherent in the information systems that could be exploited, leading to an information system breach. Without security and vulnerability assessments, the potential exists that information systems may not be as secure as intended or desired.

- Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Information system security controls are monitored on an ongoing basis to ensure the continued effectiveness of the controls.

Policy: Awareness and Training (AT)

The quality and integrity of RTI's Information Security Awareness training ensures that the workforce members, including management of RTI's information systems, understand the ISMS as well as the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as social engineering).

The goal is to ensure users understand the risks of using information technology, how to defend against malicious threats, and how to react to information security events or incidents, whether at work or at home.

1. As per RTI Corporate Policy 14.1 Network and Computing Service, employees and contractors shall receive Information Security Awareness training upon hire and annually thereafter. This training explains RTI's ISMS and will also be reviewed annually.
    a. Exceptions: There may be circumstance where non RTI staff have limited access to the RTI network, thus Security awareness training completed by their employer is sufficient to meet RTI requirements.
2. Role-based training is required for all IT employees, contractors and consultants.
    a. RTI Managers of IT consultants and contractors are responsible for ensuring their contractors and consultants complete specific job-related training as fitting to their role to include review of appropriate RTI and GTS policies, Standard Operating Procedures (SOPs) and Work Instructions (WI).

Policy: Clean Desk

A Clean Desk Policy for workspaces is also required to ensure that all sensitive and confidential information, whether on paper, storage media, or hardware is properly secured and protected from unauthorized view.

- Users must ensure that all sensitive or confidential data in hardcopy is removed from their workspace and secured in a drawer when the desk is unoccupied at the end of the workday.
- File cabinets containing sensitive or confidential information must be kept closed and locked when not in use or when left unattended.
- Printouts containing sensitive or confidential information should be immediately removed from the printer. Sensitive or confidential documents must also be shredded upon disposal.
- Whiteboards containing sensitive or confidential data must be thoroughly erased.

Storage devices when not in use such as CD, DVD, hard drives, USB drives, etc. containing sensitive or confidential data must be secured in a drawer and data must be encrypted.

Policy: Configuration Management (CM)

The quality and integrity of RTI's standardized configuration settings allow information systems and information system components to be consistently deployed in an efficient and secure manner. Without standardized configuration settings, the potential exists that information systems may be deployed that fail to meet the security requirements of RTI, or

that compromise the security requirements of other information systems with which they interconnect.

- Configuration baselines and inventories are established and maintained of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development lifecycles.
- Establish and enforce security configuration settings for information technology products employed in organizational information systems.
- Track, review, approve/disapprove, and audit changes to RTI information systems.
- Analyze the security impact of changes prior to implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- IT Administrators will restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- User-installed software are controlled and monitored.
- Networks are configured to restrict information flow between information systems or components of information systems using access control lists.
- An asset inventory of information system components is maintained. The inventory is updated when a new information system or information system component is implemented or an old one is retired.

Change Management

Change Management ensures that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. All IT Administrators changes are executed in a documented and predictable manner so that Users can plan accordingly. All IT Administrator Divisions must follow the IT Change Management Standard Operating Procedure (SOP) which provides the change management process for all production systems and associated resources.

Policy: Contingency Planning (CP)

The purpose of this policy is to ensure that information security is properly addressed within the organization's Business Continuity Planning strategy. Business Continuity plans (BCP) and Disaster Recovery (DR) procedures shall be in place to ensure that effective compliance are maintained even in periods of business disruption. RTI's Resilience Programs maintain two distinct functions including Incident Management and Business Continuity. The Incident Response and Contingency Planning policies supports the implementation of and compliance with this policy.

GTS is required to develop, implement, test and maintain an IT Business Continuity Plan covering all IT staff and Contingency/Disaster Recovery Plans covering all supported networks that deliver or support core systems and services at RTI.

- Document a BCP that addresses documented recovery strategies designed to enable RTI to respond to potential disruptions.
- Contingency plans will go through testing to ensure comprehensiveness and effectiveness.

- These information security processes and controls are reviewed and validated regularly to ensure their continued effectiveness.
- Develop, maintain, and document data backup and storage procedures to ensure the recovery of electronic information in the event of failure.
- Identify and apply security requirements for protecting data backups based on the different types of data (e.g., sensitive, confidential, public) handled by the entity.

Policy: Documentation Management

In compliance with NIST SP 800-53, OCISO has developed this Policy and supporting Procedures that contains the following properties as identified in each NIST control family as XX-1 (e.g., Access Control).

It is required that each policy, standard, or procedure prescribed herein are reviewed and/or updated at least annually. The standards and requirements in this policy have been set forth by the Office of the CISO, in accordance with the National Institute of Standards and Technology framework and the Cybersecurity Maturity Model Certification (CMMC). Both Policies and Procedures require document owner, document reviewer (who is a subject matter expert), and document approver. Document changes are captured in the document history:

- Minor number (number to the right of the decimal, e.g., x.1) will capture changes made to the document.
- Major number (number to the left of the decimal, e.g., 1.0) when the document is moved to approval and publishing and training.

Only major numbers will require training. Minor changes that do not change the spirit of the policy (e.g., misspelling) are left as a minor number in the history and will not require training.

Changes to the ISMS, the policies or security standards must be authorized by OCISO. Depending on the nature of the policy or standards change and urgency, changes might be incorporated into the published policy and standards immediately upon approval or may wait for the next periodic release and update.

Supplemental and supporting materials including this policy, standards, procedures, and reference tools are developed and maintained in the IT Controlled Document System. This site will serve as the single, authoritative source for IT security policies and procedures as well as up to date supplemental security information.

Policy: Identification and Authentication (IA)

The purpose of this policy is to ensure IT Administrators have implemented controls within the information systems that uniquely identify and authenticate users and devices to ensure only those who have a need to know have access to RTI and/or client data.

<u>Basic Security Requirements</u>:

- Authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.
    - SaaS solutions managed by GTS will require Single Sign on (SSO) unless in conflict with legal, regulatory or framework control requirements which will take precedence.
- Derived Security Requirements:

    - Multifactor authentication is used for local and network access to privileged accounts and for network access to non-privileged accounts.
    - Replay-resistant authentication mechanisms are employed for network access to privileged and non-privileged accounts.
- Prevent reuse of identifiers.
- Disable identifiers after a defined period of inactivity.
- Implement a minimum password complexity and change of characters when new password creation is enforced.
- Prohibit password reuse for a specified number of generations.
- Temporary password use for system logons with an immediate change to a permanent password is required.
- Store and transmit only encrypted representation of passwords.
- Obscure feedback of authentication information.
- Create and maintain standards regarding the classification of client and enterprise information.
- Create and maintain standards regarding the secure disposal of client and enterprise information assets.
- Dispose of client and enterprise information in a secure fashion such that the information is not readable or recoverable after disposal and certificates of destruction are obtained and saved where required.

Policy: Incident Response (IR)

RTI has legal and contractual responsibilities to maintain and protect the confidentiality of all our customers' information. In this respect it is the company's obligation to ensure employees, contractors, consultants, and temporary employees are aware of and adequately trained regarding corporate security, privacy policies and standards.
The purpose of this policy is to ensure that RTI's incident response capabilities, used to monitor for security incidents have a maintained quality and integrity. The incident response capabilities determine the magnitude of the threat presented by these incidents, and how to respond to these incidents. Without an incident response capability, the potential exists that in the event that a security incident occurs, it will go unnoticed, and the magnitude of harm associated with the incident are significantly greater than if the incident were noted and corrected.

OCISO investigates and responds to any actual, threatened, suspected, or alleged security incident, including violation of RTI and IT security policies or a breach of information security safeguards (including any attempts to bypass, break through or override any information security safeguards). Incident reporting and notification is provided by OCISO to members of the incident response team, including the Privacy Office, Enterprise Risk Management, and others based on the nature of the event. Investigations are performed by OCISO or in collaboration with the Privacy Office, Enterprise Risk Management, and/or Corporate Counsel and representatives of certain business units if applicable.
An operational incident-handling capability is developed and implemented for all organizational information systems that house or access RTI controlled information. Incidents are tracked, documented, and reported to appropriate officials and/or authorities both internal and external to the organization in coordination with the Privacy Office, Enterprise Risk Management and Contracts Office.

Policy: Media Protection (MP)

The quality and integrity of RTI's media protection mechanisms allow information to be provided a greater level of security than can be achieved with system-based protection mechanisms alone. Without media protection mechanisms, the potential exists that RTI's information assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where that information is taken out of the information system. IT Administrators are responsible for the protection of media containing RTI corporate or client data and in ensuring that access is properly controlled during storage and transportation.

- All privileged information when stored out of system (via information media) are protected by media protection mechanisms to ensure the highest levels of security. Non-privileged information are protected to ensure the highest levels of integrity and availability.
- Where information is transferred to media, that media shall be stored securely within a controlled area and access to that controlled area shall be physically restricted to authorized personnel. Further, the mechanisms that enforce those access restrictions shall collect access information and shall include the ability to audit access attempts.
- Information system media are sanitized or destroyed before disposal or release for reuse.
- Cryptographic mechanisms shall be implemented to protect the confidentiality of data stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- Use of **non-IT managed** external devices (e.g., USB, **network based**) for workstations is not permitted. If an exception is granted, then the external device must be encrypted.

Policy: Personnel Security (PS)

The purpose of this policy is to ensure personnel, including contractors, are aware of and understand their responsibilities regarding information security. Additionally, security controls should be instituted to ensure that information and data security is considered throughout the employment process. This Personnel Security Policy applies to all business processes and data, information systems, as well as components, physical areas, and personnel of RTI.

Personnel include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by RTI.
- All contractors and third parties that work on behalf of and are paid directly by RTI.
- All contractors and third parties that work on behalf of RTI but are paid directly by an alternate employer.
- All employees of partners and clients of RTI that access RTI's non-public information systems.

Additionally,

- All candidates for employment, including contractors and third-party users, must undergo further background verification checks in accordance with the appropriate laws.

- Contractual agreements with all employees and contractors will clearly outline the responsibility of the individual/contractor to information security.
- All employees and contractors must undergo Information Security Awareness training and assessment based on their roles, as well as relevant updates in policies and procedures applicable to their jobs.
- There is a formal, communicated process to take action against employee(s) or contractor(s) when a failure to comply with security requirements occurs.

Policy: Physical and Environmental Security (PE)

The purpose of this policy is to ensure proper measures are in place to prevent unauthorized physical access or damage to the organization's information and facilities. IT Administrators will create and maintain physical security controls within established standards to prevent unauthorized access to, damage to, interference of, and unauthorized use of facilities and information. Controls, dependent upon established and Environmental Security Standards for specific Business Units, may include access control, alarm monitoring, video surveillance, and the deployment of security officers. The protection provided by physical security controls are commensurate with the classification and method of information stored, processes performed, and identified environmental and physical risks at each RTI location.

- RTI Global Security and GTS develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
- RTI Security and GTS will establish a process to review, approve, and issue credentials for facility access.
- RTI Security and GTS shall remove individuals from the facility access list when access is no longer required.
- Audit logs of physical access are maintained.
- RTI staff will escort visitors and monitor visitor activity.
- RTI Security and GTS will control and manage physical access devices.

Equipment shall be physically protected from security threats and environmental hazards. Equipment security requirements shall also address unauthorized access to and safeguarding supporting facilities/utilities, such as the electrical supply and cabling infrastructure. IT equipment must only be disposed of via secure, approved processes and vendors.

Policy: Planning (PL)

RTI has chosen to adopt the Security Planning principles established in NIST SP 800-53 "Security Planning," Control Family guidelines, as the official policy for our FIPS Low and Moderate enclaves. The FIPS Low and Moderate enclaves are bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related standards documented.

- Documents required for certification and accreditation of the IT FIPS enclaves are maintained.
- The documents are reviewed, updated, and approved on an annual basis and disseminated to project teams on an as needed basis.

Policy: Privacy & Data Protection (PT)

RTI has implemented an Office of Privacy and Data Protection to ensure compliance with regulatory and contractual requirements. See Privacy & Data Protection | Insider (rti.org) for policies and guidance on how to properly identify, manage and protect data in RTI's possession.

Policy: Program Management (PM)

RTI has developed and disseminated an organization-wide Information Security Program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and,
- Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations, organizational assets, individuals, and other organizations.

RTI manages 2 information system platforms that are subject to FISMA requirements:

- Information System Name: Low Network
  Owner: Vice President (VP), Infrastructure and Operations
  Authorizing Official: CIO
  Impact Level: Low

- Information System Name: Moderate Network (formerly ESN)
  Owner: Vice President (VP), Infrastructure and Operations
  Authorizing Official: CIO
  Impact Level: Moderate

IT has developed and maintains a system security plan (SSP) for the platforms that are reviewed annually. Additional project level system security plans exist for project system boundaries that are hosted on RTI's IT platforms.

Policy: Risk Assessment (RA)

The quality and integrity of RTI's risk assessments are used to determine the likelihood and magnitude of harm that could come to an information system, and ultimately, RTI itself in the event of a security breach. By determining the amount of risk that exists, RTI is in a better position to determine how much of that risk should be mitigated and what controls should be used to achieve that mitigation.

1. Risk assessments shall be performed upon initial acquisition of an information system (in the event that the information system is owned/operated by RTI) or prior to initial establishment of service agreements or in the event that the information system is owned/operated by a third party on behalf of RTI). Further, the risk assessment shall be reviewed and, where required, updated whenever a significant change is made to the information system, whichever comes first.

2. Periodic assessment must be conducted to identify the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data subject to HIPAA.
3. Prior to choosing a third party, a proper risk assessment must be conducted on the third party to ensure reputation, security practices, etc. are clearly made evident and work within RTI's risk tolerance.

Risk Acceptance Approval
Any significant exceptions or noncompliance with the ISMS, standards and policy must be approved in writing by a senior manager in the owning business unit, and then by the OCISO and must have an accompanying plan for remediation or mitigation per the Risk Acceptance Process. In evaluating exception requests, the OCISO shall be guided by strategic business objectives, sound risk management disciplines, and Policy and Compliance Statement. The Chief Information Security Officer may request input from the Enterprise Risk Management, Privacy Officer, Legal or others depending on the nature and extent of the request. Exception requests must be approved by the Chief Information Security Officer or their delegate.

Policy: Supply Chain Risk Management (SR)

The purpose of this policy is to ensure Vendors and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber risk assessment process.

- Protect against supply chain threats to information systems, system components, and information system services to categorize suppliers (e.g., strategic, tactical, commodity) and implement an automated security monitoring tool.
- Conduct supplier reviews prior to entering into a contractual agreement to acquire information systems, system components, or information system services.
- All vendors that access, process, store, or provide various IT components must agree with RTI's IT security requirements around suppliers' relationships with the assets.
- Security requirement agreements for suppliers include details on addressing risks surrounding the handling, processing, and communicating of assets or services
- Security requirement agreements for suppliers include details on addressing risks surrounding the handling, processing, and communicating of assets or services.

Policy: System and Communications Protection (SC)

The purpose of this policy is to ensure security is a key consideration in network management and in the transfer of information in and out of the organization. This System and Communications Protection Policy applies to all business processes and data, information systems and components, personnel, and physical areas of RTI.

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Implement limitation and controls of network ports, protocols, and services.
- Network connections associated with communications sessions are terminated at the end of the sessions or after a defined period of inactivity.
- Control and monitor the use of mobile code and Voice over Internet Protocol (VoIP) technologies.
- Protect the authenticity of communications sessions.

- Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
- Cryptographic mechanisms are implemented to prevent unauthorized disclosure of data during transmission unless otherwise protected by alternative physical safeguards.
- Establish and manage cryptographic keys for cryptography employed in the information system.

Policy: System and Information Integrity (SI)

The purpose of this policy is to ensure that the quality and integrity of RTI's information and systems are upheld across the organization. Ongoing system monitoring, scanning, and alerting is critical to ensuring that organization-wide security is upheld.

- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
    - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
    - Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Policy: System and Services Acquisition (SA)

An approved Systems Development Life Cycle (SDLC) must be followed for RTI developed and maintained systems.

- All software developed in-house, including low code/no code development, which runs on production systems must be developed per the SDLC procedures or Business Unit procedures consistent with SDLC governance framework.
- All development work shall exhibit a separation between production and test environments, and at a minimum have at least a defined separation between the development/test and production environments unless prohibited by licensing restrictions or an approved exception is made via the Risk Acceptance process. These separation distinctions allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.
- Documentation must be kept and updated during all phases of development from the initiation phase through implementation and ongoing maintenance phases. Additionally, security considerations should be noted and addressed through all phases.

A security evaluation must be performed on:

- products or services considered for purchase and installation on IT managed servers (hosting protected data or for use as RTI Corporate Systems as defined by RTI Policies & Procedures 14.4); and
- cloud-based services (as defined by RTI Policies and Procedures 14.5) being considered for use by RTI Staff regardless of whether the service is being used for a project or not, to ensure the product or service adequately protects RTI Data.

Policy: System Maintenance (MA)

The quality and integrity of RTI's information system maintenance is required to ensure that information systems are always operating optimally. Set maintenance processes are required to ensure that maintenance is conducted in the most secure manner possible. System Maintenance has become a crucial discipline for enterprises. It enables enterprises to properly maintain the systems they have come to rely on and ensure these systems continue to work and perform as expected. Without systems maintenance, the potential exists that information systems are unable to provide appropriate information security. Without maintenance processes, the potential exists that the act of performing systems maintenance could, either directly or indirectly, compromise information system security. IT Administrators are responsible for the maintenance of server/network resources.

- Perform maintenance on organizational information systems.
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- Only pre-authorized personnel are allowed to perform information system maintenance.
- Multifactor authentication is required to establish nonlocal maintenance sessions via external network connections; terminate such connections when nonlocal maintenance is complete.
- Remote maintenance must be authorized, actively monitored, and audited upon completion.
- A maintenance log shall be maintained for all information system maintenance.
- Maintenance activities of maintenance personnel without required access authorization are supervised.

Policy: Vulnerability Disclosure (VD)

RTI is committed to ensuring the security of its approved hosted environments and protecting their client's information. This policy is intended to give reporters and security researchers guidelines for submitting and/or conducting vulnerability discovery activities, as well as where to find updates for investigated vulnerabilities.
The Office of the CISO (OCISO) tracks and discloses vulnerabilities that impact the RTI hosted and managed infrastructure as needed. Updates on vulnerabilities are provided through the RTI CVE Dashboard. Reporters may also use this site to submit a request for research on a vulnerability not already listed.
OCISO Security researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Disclosure of any personally identifiable information to third party is prohibited.
- Only use exploits to the extend necessary to confirm a vulnerability's presence.
    - Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide a reasonable amount of time to resolve the issue before disclosing it publicly.
- Security researchers will not be subject to legal action for research activities that concludes represents a good faith effort to follow the policy, and deem that activity authorized.

Non-Compliance

Per RTI-14.1.3-Acceptable Use Policy, "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".

Training

Role based training will be documented by a 'Read and Understand' acknowledgement through the System of Record. This acknowledgement confirms your understanding of the Policy and that if you violate the rules explained herein, you may face disciplinary action according to the applicable company policy.