Information Security Policy

Effective: November 2020

Updated: May 2026

Purpose

The purpose of this Information Security Policy is to demonstrate RTI's commitment to safeguarding the confidentiality, integrity, and availability of its information systems and data through a structured, risk-based approach that ensures effective information security management and compliance with relevant standards and regulations.

Scope

This policy is applicable to RTI managed information systems classified as low or moderate impact, including cloud-based platforms, applications, infrastructure, and related services that handle, store, or transmit sensitive organizational or protected health information, as warranted. It applies to all personnel and authorized users who engage with RTI's information assets, irrespective of their role, location, or device. The scope encompasses all organizational information assets, including those requiring enhanced security measures due to regulatory or contractual requirements.

Cybersecurity and IT Roles and Responsibilities

Role	Responsibilities
Vice President, Information Security and Chief Information Security Officer (CISO) and Office	Responsible for RTI's information and data security. Office of the Chief Information Security Officer (OCISO) and staff ensure that all network, digital, and IT activities comply with RTI's ISMS, IT Policies, Procedure/s and regulatory security standards.
OCISO-Security Operations (Security Ops) Team	Responsible for monitoring, detecting, and responding to cybersecurity threats and incidents across the organization. Their duties include operating and tuning security monitoring tools, conducting threat assessments, coordinating incident response activities, maintaining security event records, and supporting vulnerability management and remediation efforts in alignment with RTI's security policies and regulatory requirements.
OCISO-Cybersecurity Compliance Team	Ensures RTI adherence to cybersecurity regulations and standards, conducts compliance assessments, supports audit activities, and coordinates remediation efforts to address identified gaps.
OCISO Information Security Officer (ISO)	Responsible for ensuring effective implementation of security controls for RTI's information systems. The ISSO works closely with system owners, engineers, and cybersecurity leadership to implement,

	maintain security controls in compliance with organizational policies.
Project Information System Security Officer (ISSO)	Responsible for implementing and maintaining security measures for project information systems, ensuring compliance with relevant regulations and standards as per contractual requirements. The ISSO conducts risk assessments, monitors systems for security incidents, assists with audits, and supports remediation of identified vulnerabilities.
IT Department	Implements technical controls, monitors systems, supports risk management activities, and ensures compliance.
System Owners	Responsible for the security of information systems under their control, including risk management activities and compliance.
Users	Required to comply with security policies, report incidents, and participate in training.

Introduction

All users are required to familiarize themselves with and adhere to these security measures, which have been implemented to protect the confidentiality, integrity, and availability of data. This policy specifies controls to prevent unauthorized access, modification, disclosure, or destruction of information, and underscores that data protection is a collective responsibility throughout RTI.

General Information Security Controls

RTI security control policies set a standard level of security across the organization. Unauthorized changes to the ISMS or standards are not allowed. These guidelines take effect upon this document's release. If a project information system requires extra controls due to project contracts, it must establish project-level procedures to comply with those requirements. Those controls shall be in addition to, or in adherence to RTI's security policies.

External Regulations

Data stored and managed on RTI's network must adhere to a range of external regulatory frameworks. The regulations listed below represent key standards we comply with; however, this list is not exhaustive, and additional requirements may apply based on specific project contract requirements.

Regulation/Standard	Description/Title
CMMC	Cybersecurity Maturity Model Certification is the U.S. Department of Defense cybersecurity framework contractors must meet to protect sensitive government information, especially Controlled Unclassified Information (CUI).
FISMA	Federal Information Security Modernization Act of 2014
GDPR	General Data Protection Regulation is a European Union law that governs how organizations collect, process, store, and protect the personal data of individuals in the EU, giving individuals stronger rights and control over their personal information.

HIPAA	Health Insurance Portability and Accountability Act, including the HIPAA Security Rule, which establishes national standards for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI).
HITECH	Health Information Technology for Economic and Clinical Health
ISO/IEC 27001:2022	International Organization for Standardization and International Electrotechnical Commission
ITAR	International Traffic in Arms Regulations
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Office of the CISO

RTI's Office of the Chief Information Security Officer (OCISO) strengthens cybersecurity and boosts system resilience by encouraging everyone across the organization to share responsibility. The OCISO offers services such as threat assessments, IT risk management, security training, incident response consulting, and IT event record-keeping. The Cybersecurity Compliance team creates policies to meet legal and security requirements, performs audits or reviews to check compliance, and oversees corrective actions with minimal disruption. For questions or assistance, you can contact the Office of the CISO at OCISO@rti.org.

IT Operations Management

IT Operations Management develops and maintains procedures that uphold security policies, assigns roles, manages information facilities, and ensures secure data handling and infrastructure changes. Continuous monitoring and vulnerability assessments are performed to maintain a secure environment. IT Administrators set standards to manage data risks and align practices with RTI's Information Security Management System, ensuring confidentiality, integrity, and legal compliance. Exception request procedures are in place, and RTI may monitor resources to enforce policy compliance.

Policies

Access Controls

Access controls will be enforced to ensure information, including sensitive information, may only be accessed by authorized individuals. Access privileges are for individual use only and must not be shared. Procedures will cover secure information management, effective account management (activation, changes, review, and deactivation), enforcement of access and authentication restrictions, controls on information flow, separation of duties, and the least privilege principle to limit access to only what is needed.

Audit and Accountability

Requirements are set to improve transparency, accuracy, and compliance through thorough audit log management and system monitoring. The organization must securely handle information, identify and record audit events with full details, allocate storage, regularly review logs, generate reports, apply time stamps, and safeguard audit data from unauthorized changes. These steps aid in detecting and investigating security incidents and uphold organizational integrity.

Assessment, Authorization and Monitoring

Audit and accountability controls are required for all information systems, ensuring that records of security-relevant events are generated, safeguarded, and retained. These measures facilitate the detection and investigation of unauthorized activities, support compliance with applicable legal, regulatory, and industry security requirements, and ensure alignment with relevant internal control standards. Audit logging, monitoring, review, and retention practices are adjusted based on system impact and regulatory needs. Low impact systems must log key events, protect audit records, perform periodic reviews, and maintain accurate time synchronization. Moderate impact systems require advanced logging, centralized record storage, automated alerts, regular reviews, and extended retention. Roles are clearly assigned; compliance is mandatory, and any exceptions must be documented, assessed, and approved.

Awareness and Training

All personnel who access RTI assets are required to complete Information Security Awareness training, ensuring they understand their security obligations. This program lowers risks by educating participants about IT threats, defense strategies, and how to respond to incidents. The Office of the Chief Information Security Officer (OCISO) is responsible for developing security procedures, delivering both basic and role-specific training upon hiring and annually, maintaining records of completed training, conducting monthly phishing simulations, and providing additional instruction when necessary.

Clean Desk

All personnel must keep desks clear of sensitive information to protect confidential information both in the office and when working remotely. Secure documents in locked drawers, keep file cabinets closed and locked when unattended, retrieve and shred sensitive printouts promptly, erase whiteboards with confidential data, and encrypt and store electronic devices securely.

Configuration Management

Configuration management requirements will be established and documented to enforce standardized configuration settings for all information systems and components. Management procedures will be developed and distributed to relevant stakeholders; baseline configurations will be maintained and regularly reviewed, and formal change control processes will be consistently applied. All proposed changes will undergo thorough security impact analysis, and only authorized personnel will be permitted to implement modifications. Restrictive settings will be adopted to minimize risk, essential system functionalities will be enabled, and an up-to-date inventory of all system components will be maintained. These measures collectively ensure system integrity and security are preserved throughout the operational lifecycle.

Contingency Planning

A robust Contingency Disaster Recovery Plan will be implemented that provides staff with clear training on their designated roles, conducting regular tests of response plans to verify effectiveness, establishing alternative locations and backup services to ensure continuity of operations, and continuously enhancing procedures based on lessons learned from past events. These systematic practices are implemented to ensure the organization is prepared to respond effectively to unexpected disruptions and maintain essential services without interruption.

Documentation Management

Office of the Chief Information Security Officer (OCSIO) will maintain a comprehensive information security management system that governs the lifecycle of IT procedures, ensuring annual review, proper ownership, authorization of amendments, accurate recordkeeping, role based training acknowledgements and secure management within the designated system of record. This policy is subject to review every 3 years, unless circumstances necessitate an earlier review.

Identification and Authentication

Users and devices will be distinctly identified and authenticated prior to accessing information systems, utilizing secure mechanisms such as passwords, tokens, or biometric verification. Comprehensive procedures will be established to govern the management of user and device identifiers, ensure robust authenticator controls, safeguard authentication feedback, and facilitate the secure disposal of sensitive data. These protocols are implemented to restrict system access to authorized personnel, reduce the likelihood of unauthorized entry, and uphold the security of information assets.

Incident Response

Incident Response prioritizes the protection of customer information through the enforcement of a robust Incident Response Plan. The Office of the CISO (OCISO) leads the investigation and management of security incidents and collaborates with relevant departments as necessary. RTI strives to minimize operational impact and enhance security via its comprehensive incident-handling capabilities. Additionally, staff responsible for managing incidents receive role-based training encompassing preparation, detection, analysis, containment, eradication, and recovery. Security event reporting is managed through our ticketing system, ensuring events are closely monitored, promptly escalated to appropriate teams and stakeholders, and that incident response support is provided to users as needed.

Media Protection

Safeguards are established to prevent unauthorized access, disclosure, modification, or destruction of sensitive physical and digital media. These controls include the implementation of secure management procedures, restriction of non-IT managed device usage unless expressly authorized and encrypted, application of appropriate classification markings, enforcement of secure storage and transport measures, and comprehensive sanitization prior to disposal or reuse. Such measures are intended to protect information assets and maintain organizational security. The use of USB drives for media protection purposes is strictly prohibited unless an approved exemption is granted.

Personnel Security

Ensuring staff who are in sensitive positions are trustworthy and reliable, RTI manages personnel security by assigning risk designations (see Position Risk Designation section below) and screening criteria for all roles. This includes conducting initial background checks, implementing secure processes for termination and transfers—which involve revoking access and recovering security-related property—and requiring documented access agreements before granting system access. External providers must also meet RTI IT's personnel security requirements to maintain the protection of information systems and uphold organizational standards.

Position Risk Designation

RTI IT assigns risk levels to positions based on an assessment of duties and potential impacts on organizational security, conducted by the Chief Information Security Officer (CISO). The sensitivity of a position determines screening requirements, ongoing training, and the authorization for access to information systems. Staff, contractors, vendors, and interns are screened and receive initial and annual security awareness training, with additional training provided as needed for roles with higher access privileges to ensure alignment with their responsibilities.

IT Position Responsibilities

Position	Logical Access	Physical Access to Datacenter	Risk Designation Level
AWS Cloud Engineer (Deployment, maintenance, and monitoring of AWS services and infrastructure)	Yes	No	3
AWS Database Administrator (Administration and maintenance of AWS RDS, DynamoDB, and other cloud databases)	Yes	No	4
AWS DevOps Engineer (Automation of deployments, CI/CD pipelines, and infrastructure management on AWS)	Yes	No	3
AWS Security Specialist (Management of AWS security configurations, monitoring, and compliance)	Yes	No	4
AWS Solutions Architect (Design and implementation of AWS cloud solutions)	Yes	No	4
Backup Administrator (Maintenance of systems used for data backup and data restores)	Yes	Escorted	4
Data Center Operations (Facility and overall maintenance of primary and backup data centers)	Yes	Yes	3
Database Administrator (Maintenance and monitoring of SQL and Oracle-based databases at RTI)	Yes	Escorted	4
Domain Administrator (Management of domain settings and GPO at RTI)	Yes	Escorted	5

Firewall Administrator (Maintenance and monitoring of firewalls)	Yes	Escorted	4
Help Desk Analyst (First Level IT Support for On-Premises and Cloud Environments)	Yes	No	2
Network Administrator (Maintenance of RTI on-premises networks and cloud networking services)	Yes	Escorted	4
Security Operations Staff (Security monitoring of settings, logs; incident response)	Yes	Escorted	4
Server Administrator (Operation and updates of Windows and Linux-based servers at RTI)	Yes	Escorted	3
System Administrator (Software and overall system administration and management)	Yes	Escorted	3

Physical and Environmental Security

The Physical and Environmental Security approach is focused on protecting RTI physical infrastructure, cloud services, and environments from unauthorized access, damage, and security threats. Procedures outline management and security of information, authorizing and controlling physical and cloud-based access to facilities and systems, securing output devices, monitoring facility and cloud service access, keeping detailed visitor access records, and escorting visitors when required. Additional procedures include safeguarding power equipment and cabling, maintaining emergency lighting for safe evacuation, and enforcing fire protection measures.

For cloud services that support RTI, the Cloud Service Provider (CSP) is responsible for establishing comprehensive physical and environmental security measures within their data centers. The Office of the Chief Information Security Officer (CISO) performs annual compliance assessments to verify that these controls are properly implemented.

Planning

Security and privacy measures are thoroughly integrated throughout the entire lifecycle of information systems. This approach requires the creation and sharing of procedures for effective information management, the development of comprehensive system security and privacy controls, the documentation of clear rules of behavior for all users, and the design of robust architectures to safeguard information and maintain privacy protections.

Privacy & Data Protection

RTI maintains a dedicated privacy and data protection function responsible for ensuring adherence to all relevant regulatory and contractual data requirements, and for providing guidance on the correct identification, management, and safeguarding of data.

Program Management

A comprehensive risk management strategy is in place to guide IT operations in effectively managing the RTI infrastructure information security program which is captured in this information security policy. A Chief Information Security Officer has been appointed to oversee the program, allocating adequate resources to support its implementation, and establishing a process for creating and maintaining risk registers to address identified security weaknesses. Additionally, the program maintains an inventory of information systems for proper oversight, implements a security awareness and training program for personnel, and has established an insider threat program to detect and respond to potential internal risks. Mission and business processes are also clearly defined to ensure alignment with the established security requirements.

Risk Assessment

The Office of the Chief Information Security Officer (OCISO) will establish and maintain a comprehensive risk assessment program to identify, evaluate, and manage risks to its information systems. Procedures will be developed and disseminated for information security management, categorize information systems and the data they handle, and perform regular risk assessments to determine threats, vulnerabilities, and potential impacts. Additionally, they will implement ongoing vulnerability monitoring and technical surveillance countermeasures, respond appropriately to assessment findings within the organization's defined risk tolerance, and document risk acceptance decisions with approval from senior leadership.

Supply Chain Risk Management

A strong Supply Chain Risk Management program links information security with procurement to manage risks across systems and services. It defines roles, requires third-party due diligence, includes security requirements in contracts, and reviews vendors according to company risk appetite for consistent, auditable oversight.

System and Communications Protection

RTI maintains the integrity, confidentiality, and availability of its information systems through clear security procedures. These include separating user and system functions, isolating security operations, preventing unauthorized data transfers, guarding against denial-of-service attacks, monitoring interfaces, protecting transmitted data, and promptly ending network sessions after completion or inactivity.

System and Information Integrity

A strong commitment is made to maintaining the integrity and security of information systems by establishing and upholding procedures for managing and safeguarding information. This includes promptly identifying and addressing system flaws, implementing protections against malicious code, continuously monitoring for potential attacks, distributing security alerts and directives, utilizing integrity verification tools to detect unauthorized changes, enforcing defenses against malware and spam, and validating the integrity of all incoming information.

System and Services Acquisition

RTI will implement an information security and privacy program that embeds security and privacy requirements in all stages of system and service acquisition, development, vendor qualification, and lifecycle management.

The program will define, document, and enforce these requirements on a risk-based approach; adopt secure development practices; manage and qualify third-party vendors and services based on established criteria; test and evaluate; maintain thorough documentation and configuration; provide ongoing support and training; and ensure continuous compliance monitoring. RTI is committed to protecting its information assets throughout their lifecycle.

System Maintenance

Maintenance must be planned, authorized, documented, and monitored to protect system confidentiality, integrity, and availability. Both internal and external work requires approved personnel, methods, and tools, along with tight access controls. Risk management and change

control govern all operations, including remote and component handling, with strict protocols and recordkeeping for security and accountability.

Vulnerability Disclosure

The Office of the Chief Information Security Officer (OCISO) is responsible for tracking, communicating, and disclosing vulnerabilities that affect the infrastructure. OCISO will conduct regular vulnerability scans, notify relevant system owners and technical subject matter experts (SMEs) of identified vulnerabilities with details on severity and mitigation guidance, and ensure remediation efforts are prioritized to maintain system integrity and minimize impact on users and operations.

Definitions

Term/Acronym	Definition
Document Management System (DMS)	A system used to retrieve, track, manage, and store documents.
Information Security Management System (ISMS)	A framework of policies and procedures that help RTI manage and protect their sensitive information.
Vulnerability	a "weakness in an information system, system security procedure/s, 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

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".