Information Security Policy

Effective: November 2020

Updated: June 2025

Governing Laws, Regulations, and Standards

Guidance	Section / Link
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.
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
National Institute of Standards 800-171	Guidelines for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

Roles and Responsibilities

Roles	Responsibility
RTI Staff and Contractors	Comply with requirements set forth in this policy Client copy available: RTI Information Security Policy
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 Officer (CISO) and Office	The Chief Information Security Officer (CISO) is the executive responsible for an organization's information and data security. Office of the Chief Information Security Officer (OCISO) and staff assured that all network, digital, and IT activities comply with RTI's ISMS, IT Policies, Procedure/s, and regulatory security standards.
Global Technology Solutions (GTS)	Responsible for the governance of RTI's network, maintenance of the infrastructure, and functionality of corporate systems.

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 helps 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*

Introduction

This Information Security Policy (ISP) outlines RTI's IT security measures to comply with data protection requirements. Information security is a collective responsibility, requiring the participation of every RTI system user. Therefore, all users will be familiar with this policy and adhere to it.

Protecting company information and systems is crucial. Security will include controls to mitigate threats, and ensure data confidentiality, integrity, and availability.

- **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 establish guidelines for protecting RTI's data and information systems, ensuring compliance with regulatory requirements, and minimizing risks and potential incidents. It aims to maintain the confidentiality, integrity, and availability of RTI and client data through an Information Security Management System (ISMS) and consistent security controls.

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 aim to establish a standard level of security and control across the organization. Unauthorized deviations from the Information Security Management System (ISMS) and standards are prohibited. These standards and the ISMS are effective from the initial publication of this document. A copy of other RTI IT Policies is available on the Chief Information Security Office | RTI site. If Business Units (BUs) need additional security and control solutions due to specific project contractual requirements, the BU project should create project-level policies and procedures.

External Regulations

Data stored and managed on RTI's network will comply with applicable external regulations. These regulations may include:

- 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

Information Security and Classification of Electronic Information

RTI protects client and enterprise information by classifying and securing it. The Office of the CISO maintains standards for the use and disclosure of this information, which can only be used for RTI business purposes. Information from third parties is used according to contractual agreements. Refer to RTI Policy 14.2 for details on classification and handling of electronic data.

Office of the CISO

The Office of the Chief Information Security Officer (OCISO) at RTI enhances cybersecurity and system resilience by promoting shared responsibility across the business. OCISO services include threat assessment, risk management advice, security training, incident management consultation, and policy development. They ensure compliance with legal and security standards, conducting reviews or audits to verify adherence and manage corrective actions while minimizing disruptions and maintaining records of IT system events. The Office of the CISO can be reached at OCISO@rti.org.

IT Operations Management

IT Operations Management teams are responsible for creating procedures to support security policies, designating roles, and managing information processing facilities. Their duties include:

- Deploying code controls to prevent malicious software
- Protecting information exchanges with third parties
- Ensuring data protection in transit
- Managing infrastructure changes to minimize outages
- Integrating data protection into systems and applications
- Designing controls and audit trails in application systems
- Incorporating cryptographic controls for information protection
- Implementing security testing and adhering to development standards
- Utilizing change control and vulnerability scanning processes
- Decommissioning or isolating legacy applications that cannot be updated with security patches
- Infrastructure monitoring, network monitoring and application monitoring.

Policy Statements

IT Administrators will create, implement, and maintain standards and procedures to manage data risks, ensuring Information Security aligns with ISMS. These measures protect the Confidentiality, Integrity, and Availability (CIA) of all information systems and data, regardless of its creation, distribution, or storage. Cost-effective security controls are tailored to match the risk and sensitivity of the data and will comply with legal requirements. When exceptions are occasionally necessary, IT has implemented procedures for requesting exceptions and required approvals. IT reserves the right to monitor RTI computer resources and users to ensure compliance with policies.

Access Controls

The primary purpose of access controls is to protect sensitive information and systems from unauthorized access. Access control ensures that only authorized users can access specific resources, thereby maintaining the confidentiality, integrity, and availability of data. Access privileges granted to an individual are for the sole use of that individual and are not to be shared. RTI IT will maintain the following:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information
2. Account Management: System information accounts shall be managed effectively, including activation, modification, periodic review, and disabling or removal upon termination of the associated contract.
3. Access Enforcement: Logical access to information and system resources shall be restricted to approved authorizations only. This includes enforcing limits on unsuccessful login attempts and mandating the use of strong passwords.
4. Information Flow Enforcement: Controls shall be implemented to manage the flow of information within RTI systems and between interconnected systems, including limiting the use of external connectivity options to approved authorizations only.
5. Separation of Duties: Duties shall be separated to ensure that different tasks and responsibilities are assigned to different individuals or teams.
6. Least Privilege: The principle of least privilege shall be employed, ensuring that users are granted only the access necessary to accomplish their assigned tasks.

Audit and Accountability

Audit and accountability is to ensure transparency, accuracy, and compliance within an organization. Audits provide an independent evaluation of financial records, operations, and processes, identifying discrepancies, fraud, or inefficiencies. This section outlines how audit logs are managed to support and detect security incidents and aid investigations. RTI's system monitoring detects inappropriate actions in real time, while system auditing identifies them afterward. RTI IT will maintain the following:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information
2. Audit Events: IT shall determine and document the events that require auditing.
3. Content of Audit Records: Audit records must contain sufficient information to identify the event, its source, and its outcome.
4. Audit Storage Capacity: Adequate storage capacity shall be allocated for audit records.
5. Audit Review, Analysis, and Reporting: Audit records shall be reviewed, analyzed, and reported for any signs of inappropriate or unusual activity.
6. Audit Reduction and Report Generation: Provide the capability to generate audit reports and reduce audit record volume
7. Time Stamps: Internal system clocks shall be used to generate time stamps for audit records.
8. Protection of Audit Information: Audit information shall be protected from unauthorized access, modification, and deletion.

Assessment, Authorization and Monitoring

Assessment, authorization and monitoring help to evaluate the security controls in an information system to determine their effectiveness. This involves identifying vulnerabilities and ensuring compliance with security policies. This section outlines how information systems are securely managed throughout their lifecycle, from initial assessment to continuous monitoring. RTI IT will maintain the following:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management

and security of information
2. Control Assessments: Conduct regular assessments of security controls to evaluate their effectiveness.
3. Information Exchange: Manage the exchange of information between systems through formal agreements such as interconnection security agreements.
4. Risk Register (aka POA&M): Develop and maintain a plan of action to address identified weaknesses and deficiencies from control assessments.
5. Authorization: Assign a senior official to authorize system operations, ensuring compliance with security requirements before commencement.
6. Continuous Monitoring: Implement a continuous monitoring strategy to ensure ongoing assessment of control effectiveness.

Awareness and Training (AT)

RTI's Information Security Awareness training outlines that all workforce members, including management, understand the ISMS and the security implications of their actions. This reduces the likelihood of security breaches through hacking or social engineering. The aim is for users to grasp the risks of using information technology, how to defend against threats, and how to respond to security incidents. RTI IT will maintain the following:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information
2. Security Awareness Training: All personnel shall receive basic security awareness training upon hire and annually thereafter.
3. Role-Based Security Training: Specialized training tailored to the roles and responsibilities of personnel shall be provided.
4. Security Training Records: Records of security training activities shall be maintained.

Clean Desk

A clean desk is necessary for workspaces to secure and protect sensitive and confidential information from an unauthorized view. This part details the requirements for all personnel:

1. 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.
2. File cabinets containing sensitive or confidential information must be kept closed and locked when not in use or when left unattended.
3. 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.
4. 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. (Note: USB is prohibited by default. Approved exemption is required for use.)

Configuration Management

RTI's standardized configuration settings ensure efficient and secure deployment of information systems and components. Without these standards, systems might be deployed that do not meet RTI security requirements or compromise connected systems' security. This section outlines several key requirements to ensure that information systems are properly configured and managed. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information
2. Baseline Configuration: Establish and maintain baseline configurations for information systems.
3. Configuration Change Control: Manage changes to the configuration of information systems using a formal change control process.

4. Security Impact Analysis: Analyze the security impact of changes to the information systems.
5. Access Restrictions for Change: Restrict access to change information systems to authorized personnel only.
6. Configuration Settings: Establish and document configuration settings for system components that reflect the most restrictive mode consistent with operational requirements. This includes restricting and disabling the use of nonessential programs, functions, ports, protocols, and services.
7. Least Functionality: Configure information systems to provide only essential capabilities.
8. Information System Component Inventory: Maintain an inventory of information system components.

Contingency Planning

Contingency planning prepares for unexpected events that could disrupt normal operations. This section outlines how RTI IT will manage the readiness for emergencies and disruptions. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Contingency Plan: IT shall establish, maintain, and implement a contingency plan for their information systems.
3. Contingency Training: IT shall provide training for personnel on their roles and responsibilities within the contingency plan.
4. Contingency Plan Testing: IT shall test the contingency plan to ensure its effectiveness.
5. Alternate Storage Site: IT shall identify and establish an alternate storage site to ensure the availability of critical information.
6. Alternate Processing Site: IT shall identify and establish an alternate processing site to ensure the continuity of operations.
7. Telecommunication Services: IT shall ensure the availability of telecommunication services during a contingency.

Documentation Management

Document management will establish a framework for how IT manages its documents throughout their lifecycle.

1. The IT Policies will be reviewed every three years, unless a change necessitates an earlier update.
2. Procedures must be reviewed annually, unless a change necessitates an earlier update.
3. Modifications to content will necessitate retraining, whereas corrections of non-content changes (such as spelling errors) will not.
4. All amendments to the ISMS, policies, or security standards will receive authorization from OCISO and be published accordingly.
5. Each document type will have an owner, reviewer, and approver, with changes recorded in the system of record.
6. All policies and procedures will be managed and maintained within the system of record for IT controlled documents.

Identification and Authentication

Identification and authentication is to verify the identity of users accessing a system or resource. Identification involves recognizing a user, typically through a username or ID, while authentication confirms that the user is who they claim to be, often through passwords, tokens, or biometric data. This section outlines how only authorized users and devices can access information systems, reducing the risk of unauthorized access and potential security breaches. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information
2. Identification and Authentication: Uniquely identify and authenticate organizational users, such as employees and contractors, before granting access to information systems.
3. Device Identification and Authentication: Uniquely identify and authenticate devices before establishing connections.
4. Identifier Management: Manage user identifiers by ensuring they are unique, assigning them to authorized users, and disabling them after a defined period of inactivity.
5. Authenticator Management: Manage system authenticators, including passwords, tokens, and biometrics, to ensure their strength and protection.
6. Authenticator Feedback: Ensure that feedback provided during the authentication process does not compromise the authenticator.
7. Disposal: Create and maintain standards for the secure disposal of client and enterprise information, ensuring that information is not recoverable after disposal and certificates of destruction are obtained.

Incident Response

RTI is committed to maintaining the confidentiality of customer information. The OCISO is responsible for investigating any security incidents, including breaches of security policies, and collaborates with various departments to address these issues to effectively monitor and manage security incidents, preventing unnoticed threats that could cause significant harm. An operational incident-handling capability is implemented for information systems minimizing the impact on operations and improving overall security posture. There are several key requirements to effectively respond to security incidents. Here are the main points:

1. Procedure/s: procedures shall be developed and disseminated to ensure proper management and security of information
2. Incident Response Training: Key personnel shall receive training on their roles and responsibilities within the incident response process.
3. Incident Response Testing: The incident response capability shall be tested regularly to ensure its effectiveness.
4. Incident Handling: A comprehensive incident handling capability for security incidents shall be implemented, encompassing preparation, detection, analysis, containment, eradication, and recovery.
5. Incident Monitoring: Incidents shall be tracked and documented to ensure proper management.
6. Incident Reporting: Incidents shall be reported to appropriate authorities and stakeholders. Incident reporting and notification will be managed by OCISO and involve the incident response team.
    - Investigations will be conducted by OCISO or in collaboration with other departments.
    - Incident will be reported to the appropriate internal and external officials.
7. Incident Response Assistance: Incident response support shall be provided to users as required.

Media Protection

Media protection is to safeguard both physical and digital media containing sensitive information from unauthorized access, disclosure, alteration, or destruction. This section outlines several key requirements to ensure that information system media is properly protected. Here are the main points:

1. Procedure/s: procedures shall be developed and disseminated to ensure proper management and security of information

2. Media Access: The use of non-IT managed external devices (e.g., USB, network-based) for workstations is not permitted. If an exception is granted, the external device should encrypt files based on client requirements and sensitivity of the information.
3. Media Marking: Information system media must be marked to indicate the classification level of the information.
4. Media Storage: Information system media must be securely stored.
5. Media Transport: Information system media must be protected and controlled during transport.
6. Media Sanitization: Information system media must be sanitized before disposal or reuse.

Personnel Security

The purpose of personnel security is to ensure that individuals in sensitive positions are trustworthy, reliable, and loyal. This section outlines several key requirements to ensure that personnel are properly vetted and managed to protect information systems. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Position Risk Designation: All positions shall be assigned risk designations, and screening criteria shall be established for individuals filling those positions.
3. Personnel Screening: Individuals must be screened prior to authorizing access to information systems and rescreened periodically.
4. Personnel Termination: System access shall be disabled, credentials revoked, exit interviews conducted, and security-related property retrieved upon termination of employment.
5. Personnel Transfer: The need for access authorizations shall be reviewed and confirmed when personnel are reassigned or transferred.
6. Access Agreements: Access agreements shall be developed and documented for personnel, and these agreements shall be signed before access is granted.
7. External Personnel Security: Personnel security requirements shall be established for external providers, ensuring compliance with organizational policies.

Physical and Environmental Security

Physical and environmental security is to protect RTI's physical infrastructure and environment from unauthorized access, and damage. This section outlines several key requirements to ensure that information systems and their supporting infrastructure are physically protected. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Physical Access Authorizations: Develop and maintain a list of individuals authorized to access facilities. Issue authorization credentials and remove access when it is no longer required.
3. Physical Access Control: Enforce physical access authorizations at entry and exit points. Verify individual access authorizations and control ingress and egress.
4. Access Control for Transmission: Control physical access to system distribution and transmission lines.
5. Access Control for Output Devices: Control physical access to output devices to prevent unauthorized access.
6. Monitoring Physical Access: Monitor physical access to facilities to detect and respond to physical security incidents.
7. Visitor Access Records: Maintain and review visitor access records. Ensure visitors are escorted by RTI personnel at all times in facilities where information systems are located.

8. Power Equipment and Cabling: Protect power equipment and cabling from damage and destruction.
9. Emergency Lighting: Employ and maintain automatic emergency lighting for emergency exits and evacuation routes.
10. Fire Protection: Implement fire protection measures.

Planning

Planning ensures that security measures are effectively integrated into the lifecycle of information systems. This section outlines several key requirements to ensure that IT effectively plan and manage their security and privacy programs. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. System Security and Privacy Plans: Develop comprehensive security and privacy plans for their information systems. These plans should clearly outline the security and privacy requirements, and the controls implemented to satisfy these requirements.
3. Rules of Behavior: Establish and document rules of behavior for all users accessing information systems. These rules must provide clear guidelines and expectations for user conduct.
4. Security and Privacy Architectures: Develop robust security and privacy architectures. These architectures should detail the requirements and methodologies for safeguarding information and ensuring privacy protections.

Position Risk Designation

Proper position risk designation is the foundation of an effective security program. The CISO assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of a staff, contractor, vendor or intern and establishes the risk level of that position. The position risk designation assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on Institute security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of screening is conducted for a position as well as continuous training.

Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. The more sensitive information the position has access to the higher the risk, thus the additional training the staff may have to complete to ensure acknowledgement of responsibilities with the level of system privileges they have. All RTI staff are screened and complete initial security awareness training upon initial hiring. RTI staff also receive annual training required, as well as training on an ongoing basis that aligns with their primary job responsibilities.

IT Position	Responsibilities	Logical Access	Physical Access to Datacenter	Position Risk Designation Level (1- 5, with 5 being high risk)
Help Desk Analyst	First Level IT Support	Yes	No	2
Network Administrator	Maintenance of RT! networks	Yes	Escorted	4
Firewall Administrator	Maintenance and monitoring of firewalls	Yes	Escorted	4

	at RTI			
Server Administrator	Operation and updates of Windows and Linux-based servers at RTI	Yes	Escorted	3
Domain **Administrator**	Management of domain settings and GPO at RTI	Yes	Escorted	5
System Administrator	Software and overall system administration and management	Yes	Escorted	3
Security Operations Staff	Security monitoring of settings, logs; incident response	Yes	Escorted	4
Backup Administrator	Maintenance of systems used for data backup and data restores	Yes	Escorted	4
Database Administrator	Maintenance and monitoring of SQL and Oracle based databases at RT!	Yes	Escorted	4
Data Center Operations	Facility and overall maintenance of primary and backup data centers	Yes	Yes	3

Privacy & Data Protection

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

Program Management

Develops and implement a comprehensive risk management strategy across RTI IT. This section outlines several key requirements to ensure that IT effectively manage their information security programs. Here are the main points:

1. Information Security Program Plan: Develop and disseminate an organization-wide information security program plan that provides an overview of the security requirements and describes the program management controls and common controls in place.
2. Senior Information Security Officer: Appoint a senior information security officer responsible for developing, implementing, and maintaining the information security program.
3. Information Security Resources: Ensure that adequate resources are allocated to implement the information security program.
4. Risk Register (POA&M) Process: Establish a process for developing and maintaining plans of action and milestones to address security weaknesses.
5. Information System Inventory: Maintain an inventory of information systems to ensure proper management and oversight.
6. Security Awareness and Training Program: Implement a security awareness and training program for personnel.
7. Insider Threat Program: Establish an insider threat program to detect and respond to insider threats.
8. Mission or Business Process Definition: Define mission or business processes to ensure alignment with security requirements.

Risk Assessment

Risk assessments assist in identifying and evaluating risks to RTI's information systems. This section outlines several key requirements to ensure that IT effectively identify, assess, and manage risks to their information systems. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Security Categorization: RTI shall categorize its information systems and the information they process, store, and transmit.
3. Risk Assessment: RTI shall conduct risk assessments to identify threats and vulnerabilities, determine the likelihood and impact of adverse events, and assess the potential harm.
4. Vulnerability Monitoring and Scanning: RTI shall monitor and scan for vulnerabilities in its systems and applications, using tools that facilitate interoperability and automate parts of the vulnerability management process.
5. Technical Surveillance Countermeasures Survey: RTI shall employ technical surveillance countermeasures surveys at defined locations and frequencies.
6. Risk Response: RTI shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with their risk tolerance.
7. Risk Acceptance: RTI shall allow risk mitigated within its risk-appetite and shall be recorded as an exception to standards or policy, with written approval from senior leadership, guided by strategic objectives and risk management disciplines.
8. Privacy Impact Assessments: RTI shall conduct privacy impact assessments for systems, programs, or activities before developing or procuring IT that processes PII or initiating new collections of PII.

Supply Chain Risk Management

Assist to identify, assess, and mitigate risks associated with the supply chain of information systems and products. This section outlines several key requirements to ensure that Supply Chain effectively manage risks. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Supply Chain Risk Management Plan: A supply chain risk management plan shall be established and implemented to identify, assess, and mitigate supply chain risks.
3. Supply Chain Controls and Processes: Controls and processes shall be implemented to manage supply chain risks effectively.
4. Supply Chain Risk Assessments: Risk assessments shall be conducted to identify and evaluate supply chain risks.
5. Supply Chain Risk Monitoring: Maintain ongoing monitoring of important IT supply chain risks and the effectiveness of risk management controls.

System and Communications Protection

System and communication protection ensures the integrity, confidentiality, and availability of information systems and their communications. This section details essential requirements for secure protection:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Separation of System and User Functionality: Ensure that user functionality is distinct and separate from system management functionality.
3. Security Function Isolation: Maintain strict isolation between security functions and non-security functions.
4. Information in Shared System Resources: Prevent unauthorized and unintended

information transfer via shared system resources by limiting network ports, protocols, and services.

5. Denial-of-Service Protection: Implement measures to protect against and limit the effects of denial-of-service events.
6. Boundary Protection: Monitor and control communications at external and key internal interfaces and establish subnetworks for publicly accessible components.
7. Transmission Confidentiality and Integrity: Safeguard the confidentiality and integrity of transmitted information.
8. Network Disconnect: Terminate network connections at the end of sessions or after a defined period of inactivity.

System and Information Integrity

System and information integrity ensure that information systems function properly and securely without unauthorized alterations. This section outlines key requirements to maintain the integrity and security of information systems. Here are the main points:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Flaw Remediation: Must identify, report, and correct information system flaws.
3. Malicious Code Protection: Protections against malicious code must be implemented and monitored for such code.
4. Information System Monitoring: Information systems must be monitored to detect attacks and indicators of potential attacks.
5. Security Alerts, Advisories, and Directives: OCISO will receive, generate, and disseminate security alerts, advisories, and directives.
6. Software, Firmware, and Information Integrity: Integrity verification tools must be employed to detect unauthorized changes to software, firmware, and information.
7. Malicious Code Protection: Malware and spam protection mechanisms must be implemented.
8. Information Input Validation: The integrity of information inputs must be validated.

System and Services Acquisition

System and services acquisition aims to ensure that information systems and services meet security and privacy needs. This section highlights essential requirements for acquiring, developing, and managing IT systems securely.

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Allocation of Resources: RTI shall determine and allocate the necessary resources to ensure the protection of information systems and services.
3. System Development Life Cycle: Security and privacy considerations shall be incorporated throughout the entire system development life cycle.
4. Acquisition Process: Security and privacy requirements shall be included in all acquisition contracts for systems, components, and services.
5. System Documentation: The organization shall obtain or develop comprehensive documentation that describes the secure configuration, installation, operation, and maintenance of systems.
6. Security and Privacy Engineering Principles: Security and privacy engineering principles shall be applied in the specification, design, development, implementation, and modification of systems.

System Maintenance

System maintenance ensures the efficient and reliable operation of information systems. This section covers key requirements for proper maintenance.

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Controlled Maintenance: Schedule, perform, document, and review records of maintenance and repairs on information system components, ensuring that only pre-authorized personnel are permitted to perform maintenance. Remote maintenance activities must be monitored and audited upon completion.
3. Maintenance Tools: Approve, control, and monitor the use of maintenance tools.
4. Non-local Maintenance: Approve and monitor non-local maintenance and diagnostic activities.
5. Maintenance Personnel: Ensure that personnel performing maintenance on information systems have the required access authorizations.

Vulnerability Disclosure

RTI is committed to ensuring the security of its approved hosted environments and protecting their client's information. The Office of the CISO (OCISO) tracks, disseminates and discloses vulnerabilities that impact the RTI hosted and managed infrastructure as required. OCISO performs regular vulnerability scans and when a vulnerability is found:

1. Procedure/s: Procedures shall be developed and disseminated to ensure proper management and security of information.
2. Owners and technical SMEs shall be notified of vulnerabilities, and provided with known information on severity, patches, and mitigations available, and if the vulnerabilities are currently being exploited in the wild.
3. Technical SMEs shall make every effort to avoid degradation of user experience, disruption to production systems, and destruction or manipulation of data when mitigating or remediating vulnerabilities.

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.