Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Information Security Policy

Date	Version	Description	Author(s)
01/31/2022	1.0	Combined Nexant Resource Innovation Policies	Khalid Maletan
1/31/2023	2.0	Annual Review	Khalid Maletan
07/31/2023	2.1	Added Confidential classification	Khalid Maletan

Purpose

This Policy defines the mandatory minimum information security requirements for Resource Innovations. Resource Innovations may based on its business needs and specific client, legal or federal requirements, exceed the security requirements outlined in this document but must, at a minimum, achieve the security levels required by this Policy.

This Policy acts as an umbrella document for all other security policies and associated standards. This Policy defines the responsibility to:

- protect and maintain the confidentiality, integrity, and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, and financial and business transactions, compromise data, and result in legal and regulatory non-compliance.

This Policy benefits Resource Innovations by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures, and practices and know-how to protect information.

Scope

This Policy encompasses all systems, automated and manual, for which Resource Innovations has administrative responsibility, including systems managed or hosted by third parties on behalf of Resource Innovations. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

Security Policies

In addition to this Policy, Resource Innovation's security is governed by the following policies that are included in this Policy reference:

- Acceptable Use Policy
- Business Continuity Policy
- Asset Management Policy
- Backup Policy
- Change Management Policy
- Data Classification Policy
- Data Deletion Policy
- Data Protection Policy
- Encryption Key Management Policy

- Network Policy
- Password Policy
- Physical Security Policy
- Risk Assessment & Management Program Policy
- System Access & Authorization Control Policy
- Vendor Management Policy
- Vulnerability Management Policy
- Incident Response Policy
- Software/Systems Development Lifecycle Policy
- Information Security Policy

The term Information Security Policies refers to all the policies listed above. All security policies must be reviewed annually or when there has been a significant change.

Supporting Document

Policies are overarching documents that provide the bases of how Resource Innovations will implement its security posture. There are further documents that may be necessary to provide step-by-step instructions on how to implement the policies in a particular technology offering. These documents can be in the form of Standard Operating Procedures (SOP), Procedures, or Guidelines. These documents, at a minimum, shall comply with or enhance what is outlined in Resource innovations policies.

Key Terms and Definitions used in RI Security Policies:

Listed at the end of this Policy

Policy

Organizational Security

Organizational security requires both an information risk management function and a technical information security function.

- Resource Innovations must designate an individual or group to be responsible for the risk management function, assuring that:
- Risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and
- The management of information assets and information system-related security risks consistently reflects risk tolerance and is considered along with other types of risks to ensure mission/business success.
- Resource Innovations must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this Policy will refer to the individual or group designated as the Director of Information Security (DIS) or their appointed security representative. This function will be responsible for evaluating and advising on information security risks.
- Although the technical information security function may be outsourced to third parties, Resource Innovations retains overall responsibility for the security of the information that it owns.

Functional Responsibilities

Information Security Committee

The Information Security Committee is comprised of Resource Innovations' following positions:

- Chief Technology Officer – CTO, Executive Management
- Chief Administrative Officer – CAO, Executive Management
- VP of Marketing and Communications
- Director of Information Technology
- Director of Information Security
- Senior Legal Executive

The committee is responsible for the approval of all security policies and procedures, oversight and monitoring for compliance. The team has a direct line with the CEO and can communicate with the CEO whenever needed.

The Information Security Committee is responsible for the following:

- evaluating and accepting risk on behalf of Resource Innovations;
- identifying information security responsibilities and goals and integrating them into relevant processes;
- supporting the consistent implementation of information security policies and standards;
- supporting security through clear direction and demonstrated commitment to appropriate resources;
- promoting awareness of information security best practices through the regular dissemination of materials provided by the DIS/designated security representative;
- determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
- participating in response to security incidents;
- communicating legal and regulatory requirements to the DIS/designated security representative; and
- communicating requirements of this Policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third-party agreements.

The Director of Information Security is responsible for the following:

- act as Resource Innovations Privacy Officer
- maintaining familiarity with business functions and requirements;
- maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
- assessing compliance with information security policies and legal and regulatory information security requirements;
- evaluating and understanding information security risks and how to appropriately manage those risks;
- representing and assuring that security architecture considerations are addressed;
- developing the security program and strategy, including metrics to measure program effectiveness;
- establishing and maintaining enterprise information security policy and standards;

- assessing compliance with security policies and standards;
- advising on secure system engineering;
- monitoring external sources for indications of data breaches, defacements, etc.
- maintaining ongoing contact with security groups, associations, and relevant authorities;
- providing timely notification of current threats and vulnerabilities;
- providing awareness materials and training resources.
- advising on security issues related to the procurement of products and services;
- disseminating threat information to appropriate parties;
- participating in the development of enterprise policies and standards that considers Resource Innovations’ needs; and
- promoting information security awareness.

IT management is responsible for the following:

- supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s), which support the company’s information systems and business processes
- providing resources needed to maintain a level of information security control consistent with this Policy;
- identifying and implementing all processes, policies, and controls relative to security requirements defined by the business and this Policy;
- implementing the proper controls for information owners based on the data classification designations;
- providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
- fostering the participation of information security and technical staff in protecting information assets and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and
- implementing business continuity and disaster recovery plans.

The workforce and business are responsible for the following:

- understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted to them;
- protecting information and resources from unauthorized use or disclosure;
- protecting personal, private, and sensitive information from unauthorized use or disclosure;
- abiding by Acceptable Use Policy
- abiding by Data Classification Policy
- report suspected information security incidents or weaknesses to the appropriate manager and DIS/designated security representative.

Separation of Duties

- Separation of duties must be implemented, where appropriate, to reduce the risk of accidental or deliberate system misuse.
- Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails, and management supervision.
- The audit and approval of security controls must always remain independent and segregated from

the implementation of security controls.

Information Risk Management

- Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments as outlined in the Risk Assessment & Management Program Policy.
- Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, significant changes in program or process design, or in response to the discovery of a significant vulnerability.
- Risk assessment results, and the decisions made based on these results, must be documented.

Information Classification and Handling

- All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information must be classified on an ongoing basis as stipulated in the Data Classification Policy.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- Merging of information that creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- Each classification has an approved set of baseline controls designed to protect these classifications, and these controls must be followed.
- Resource Innovations must communicate the requirements for the secure handling of information to its workforce.
- Content made available to the general public must be reviewed according to a process that is defined and approved by Resource Innovations. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- PII must not be made available without appropriate safeguards approved by the Resource Innovations’ management team.
- For non-public information to be released outside the Resource Innovations or shared between other entities, a process must be established that at a minimum:
    - evaluates and documents the sensitivity of the information to be released or shared;
    - identifies the responsibilities of each party for protecting the information;
    - defines the minimum controls required to transmit and use the information;
    - records the measures that each party has in place to protect the information;
    - defines a method for compliance measurement;
    - provides a signoff procedure for each party to accept responsibilities; and
    - establishes a schedule and procedure for reviewing the controls.

IT Asset Management

- All IT hardware and software assets must be assigned to a designated business unit or individual.
- IT is required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Personnel Security

- The workforce must receive general security awareness training, including recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific Resource Innovations sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the Resource Innovations HR Team.
- Resource Innovations must require its workforce to abide by the Acceptable Use Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the Policy's requirements.
- All job positions must be evaluated to determine whether they require access to sensitive information and/or sensitive information technology assets.
- A process must be established within Resource Innovations to repeat or review suitability determinations periodically and upon change of job duties or position.
- The Resource Innovations' HR Department, in conjunction with the IT Department, is responsible for ensuring all issued property is returned prior to an employee's separation, and accounts are disabled, and access is removed immediately upon separation.
- All Resource Innovations employees must undergo background checks at the time of hire. Resource Innovations may rescind an employee's offer letter if their background check is found to be falsified, erroneous, or misleading.
- Resource Innovations employees who work remotely must follow these rules:
- All company-provided equipment and any equipment used to perform work must remain in the presence of the Resource Innovations employee or be securely stored.
- All of Resource Innovations' data encryption, protection standards, and settings must be followed for company-provided equipment and any equipment used to perform work.
- The confidentiality, security, and privacy of Resource Innovations' customers must be preserved by ensuring that no unauthorized individuals may view, overhear, or otherwise have access to Resource Innovations' customer data.
- All remote work must be performed in a manner consistent with Resource Innovations' security policies.

Cyber Incident Management

- Resource Innovations must have an Incident Response Plan and consistent standards to respond effectively to security incidents.
- All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the DIS/designated security representative as quickly as possible. If a

member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Director of Information Security or their manager or a senior executive directly.
- The information security response team must be notified at securityincident@resource-innovations.com of any cyber incident which may have a significant or severe impact on operations or security.

Physical and Environmental Security

- Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
- A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.
- Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
- All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of the information contained therein.

Account Management and Access Control

- Account management must employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users), which is necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).
- All access to systems must be provided through the use of individually assigned unique identifiers, known as user IDs.
- Associated with each user ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
- Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required.
- Automated techniques and controls must be implemented to terminate a session after specific conditions are met.
- Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
- Tokens must not be stored on paper or in an electronic file, hand-held device, or browser unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the DIS/designated security representative.
- Information owners are responsible for determining who should have access to protected resources within their jurisdiction and what those access privileges should be (read, update, etc.).
- Access privileges will be granted in accordance with the user’s job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with Resource Innovations’ missions and business functions (i.e., least privilege).

- Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
- All remote connections must be made through managed points of entry reviewed by the DIS/designated security representative.
- Working from a remote location must be authorized by management, and practices that assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

Systems Security

- Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.
- An individual or group must be assigned responsibility for the maintenance and administration of any system deployed on behalf of Resource Innovations.
- Security must be considered at system inception and documented as part of the decision to create or modify a system.
- All systems must be developed, maintained, and decommissioned in accordance with the Software/Systems Development Lifecycle Policy.
- Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
- All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time).
- Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

Network Systems:

- Connections between systems must be authorized by the management of all relevant entities and protected by the implementation of appropriate controls.
- All connections and their configurations must be documented, and the documentation must be reviewed by the information owner and the DIS/designated security representative annually, at a minimum, to assure:
  - the business case for the connection is still valid, and the connection is still required; and
  - the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
- A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
- Network management must be performed from a secure, dedicated network.
- Authentication is required for all users connecting to internal systems.
- Network authentication is required for all devices connecting to internal networks.
- Only authorized individuals or business units may capture or monitor network traffic.
- A risk assessment must be performed in consultation with the DIS/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Vulnerability Management

- All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.
- All systems are subject to periodic penetration testing.
- Appropriate action, such as patching or updating systems, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created and updated accordingly to document the planned remedial actions to mitigate vulnerabilities.
- Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the DIS/designated security representative. The DIS/ must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.
- The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the DIS/designated security representative for evaluation of risk.
- Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested, and followed at all times to minimize the possibility of disruption.

Operations Security

- System configurations must follow approved configuration standards.
- Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.
- Host-based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed
- Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
- Controls must be implemented, where feasible, to disable the automatic execution of content from removable media.
- Controls must be implemented to limit the storage of information to authorized locations.
- Controls must be in place to allow, where feasible, only approved software to run on a system and prevent the execution of all other software.
- All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
- All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.
- Systems that can no longer be supported or patched to current versions must be removed, or adequate measures must be implemented to mitigate the risk.
- Systems and applications must be monitored and analyzed to detect deviation from the access control requirements and record events to provide evidence and to reconstruct lost or damaged data.
- Audit logs and other security-relevant events must be produced, protected, and kept consistent with record retention schedules and requirements.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.
- Monitoring systems must be configured to alert incident response personnel to indications of

- compromise or potential compromise.
- Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
- Backup copies of Resource Innovations information, software, and system images must be taken regularly in accordance with the Resource Innovations' defined requirements.
- Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.
- Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Policy Compliance

Compliance Measurement

The IT and Information Security (IS) teams will verify compliance with this Policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the Policy must be approved by the IT and IS teams in advance and, if applicable, documented in the Resource Innovations Risk Register.

Non-Compliance

An employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Responsibility

The IT, IS, and RI managers are responsible for ensuring this Policy is followed.

Document Title			
Information Security Policy			
Version No.		**Version Date**	
2.1		July 31, 2023	
Approval Signoffs			
Name:	Catherine Carhart	**Name:**	Khalid Maletan
Title:	Chief Technology Officer	**Title:**	Director of Information Security
Signature:	CCarhart	**Signature:**	
Date:	July 31, 2023	**Date:**	July 31, 2023

Terms &Definitions

Access control – means to ensure that access to assets is authorized and restricted based on business and security requirements.

Attack – attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset.

Audit – systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Note 1: An audit can be an internal audit (first-party) or external audit (second party or third party), and it can be a combined audit (combining two or more disciplines)

Audit scope – extent and boundaries of an audit.

Authentication – provision of assurance that acclaimed characteristic of an entity is correct.

Authenticity – a property that an entity is what it claims to be

Availability – a property of being accessible and usable upon demand by unauthorized entity

Competence – ability to apply knowledge and skills to achieve intended results

Confidentiality – a property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Conformity – fulfillment of a requirement.

Consequence – the outcome of an event affecting objectives

Note 1: An event can lead to a range of consequences.

Note 2: A consequence can be certain or uncertain and, in the context of information security, is usually negative.

Note 3: Consequences can be expressed qualitatively or quantitatively.

Note 4: Initial consequences can escalate through knock-on effects.

Continual improvement – a recurring activity to enhance performance

Control – a measure that is modifying risk.

Note 1: Controls include process, Policy, device, practice, or other actions which modify risk

Note 2: Controls may not always exert the intended or assumed modifying effect.

Control objective – a statement describing what is to be achieved as a result of implementing controls.

Correction – action to eliminate a detected nonconformity.

Corrective action – action to eliminate the cause of a non – conformity and prevent a recurrence

Control Self-Assessment (CSA) – a technique used to assess the effectiveness of their risk management and control processes

Data Owner – A Data Owner has administrative control and has been officially designated as accountable for a specific information asset dataset.

Derived measure – a measure that is defined as a function of two or more values of base measures

Documented information – information required to be controlled and maintained by an organization and the medium on which it is contained.

Note 1: Documented information can be in any format and media and from any source.

Note 2: Documented information can refer to a management system, including related processes information created in order for the organization to operate (documentation) - Evidence of results achieved (records)

Effectiveness – extent to which planned activities are realized planned results achieved.

ERT – Emergency Response Team

Event – occurrence or change of a particular set of circumstances.

Note 1: An event can be one or more occurrences and can have several causes.
Note 2: An event can consist of something not happening.
Note 3: An event can sometimes be referred to as an "incident" or "accident".

Executive Management – A person or group of people who directs and controls an organization or business unit at the highest levels. This is designated as C – level positions, Executive Vice Presidents, Vice Presidents, and Senior Managers

External context – an external environment in which an organization seeks to achieve its objectives.
Note 1: External context can include:

- The cultural, social, political, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends that have an impact on the objectives of the organization and
- Relationships with, and perceptions and values of, external stakeholders.

Governance of information security – system by which an organization's information security activities are directed and controlled

Indicator – a measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to information needs.

Information asset – an asset that, like other important business assets, is essential to an organization's business and consequently needs to be protected

Information needs – insight necessary to manage objectives, goals, risks, and problems Information processing facilities – any information processing system, service or infrastructure, or the physical location housing it

Information security – preservation of confidentiality, integrity, and availability of information
Note 1: In addition, other properties, such as authenticity, accountability, non – repudiation, and reliability, can also be involved.

Information security continuity – processes and procedures for ensuring continued information security operations.

Information security event – identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security-relevant.

Information security incident – a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information security incident management – processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information security management system (ISMS) – set policies and processes for managing information security risks

Information sharing community – a group of organizations that agree to share information
Note 1: an organization can be an individual.

Information system – set of applications, services, information technology assets, or other information handling components

Integrity – property of accuracy and completeness.

Interested party – person or organization that can affect be affected by or perceive themselves to be affected by a decision or an activity

Internal context – an internal environment in which the organization seeks to achieve its objectives.

Note 1: Internal context can include:

- Governance, organizational structure, roles, and accountabilities:
- Policies, objectives, and the strategies that are in place to achieve them;
- The capabilities, understood in terms of resources and knowledge(e.g., capital, time, people, processes, systems, and technologies);
- Information systems, information flows, and decision-making processes (both formal and informal):
- Relationships with, and perceptions and values of, internal stakeholders;
- The organization's culture:
- Standards, guidelines, and models adopted by the organization: and
- Form and extent of contractual relationships.

ISMS Project – structured activities undertaken by an organization to implement an ISMS.
Level of risk – the magnitude of risk expressed in terms of the combination of consequences and their likelihood
Likelihood – chance of something happening.
Management system – set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.
Note 1: A management system can address a single discipline or several disciplines.
Note 2: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.
Note 3: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.
Measure – variable to which a value is assigned as a result of the measurement
Note 1: The term "measures" is used to refer collectively to base measures, derived measures, and indicators.
Measurement – Process to determine a value.
Note 1: In the context of information security, the process of determining a value requires information about the effectiveness of an information management system and its associated controls using a measurement method, measurement function, an analytical model, and decision criteria.
Measurement function – algorithm or calculation performed to combine two or more base measures
Measurement method – logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale
Note 1: The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

- Subjective: quantification involving human judgment; and
- Objective: quantification based on numerical rules.

Measurement results – One or more indicators and their interpretations that address information needs.
Monitoring – Determining the status of a system, a process, or an activity.
Note 1: To determine the status, there may be a need to check, supervise, or critically observe.
Nonconformity – Non-fulfillment of a requirement**.**
Non–repudiation – Ability to prove the occurrence of a claimed event or action and its originating entities.

Object – Item characterized through the measurement of its attributes.
Objective – Result to be achieved.
Note 1: An objective can be strategic, tactical, or operational.
Note 2: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, or process)
Note 3: an objective can be expressed in other ways, e.g., as an intended outcome, a purpose, an operational criterion, as an information security objective, or by the use of other words with similar meaning (e.g., aim, goal, or target).
Note 4: In the context of information system security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.
Outsource – Make an arrangement where an external organization performs part of an organization's function or process.
Note 1: An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.
Performance – measurable result.
Note 1: Performance can relate either to quantitative or qualitative findings.
Note 2: Performance can relate to the management of activities, processes, products (including services), systems, or organizations.
Policy – Intentions and direction of an organization as formally expressed by its top management.
Process – Set of interrelated or interacting activities which transform inputs to desired outputs.
Requirement – Need or expectation that is stated, generally implied, or obligatory.
Note 1: "Generally implied" means that it is custom or common practice for the organization and interested parties. That the need or expectation under consideration is implied.
Note 2: A specified requirement is one that is stated, for example, in documented information.
Residual risk – Risk remaining after risk treatment
Note 1: Residual risk can contain unidentified risk.
Note 2: Residual risk can also be known as "retained risk."
Review – Activity undertaken to determine suitability, adequacy, and effectiveness of the subject matter to achieve established objectives.
Review object – Specific item being reviewed.
Review objective – Statement describing what is to be achieved as a result of a review.
Risk – Effect of uncertainty on objectives.
Note 1: An effect is a deviation from the expected – positive or negative.
Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Note 3: Risk is often characterized by reference to potential events and consequences or a combination of these.
Note 4: Risk is often expressed in terms of the combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Note 5: In the context of information security management systems, information security risks can be expressed as the effect of uncertainty on information security objectives.
Note 6: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Risk acceptance – Informed decision to take a particular risk
Note 1: Risk acceptance can occur without risk treatment or during the process of risk treatment
Note 2: Accepted risks are subject to monitoring and review.

Risk analysis – Process to comprehend the nature of risk and to determine the level of risk
Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
Note 2: Risk analysis includes risk estimation.

Risk assessment – Overall process of risk identification, risk analysis, and risk evaluation.

Risk communication and consultation – Continual and iterative processes that an organization conducts to provide, share `or obtain information and to engage in dialogue with stakeholders regarding the management of risk.
Note 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability, and treatment of risk.
Note 2: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is A process that impacts a decision through influence rather than power; and input to decision-making, not joint decision-making.

Risk criteria – Terms of reference against which the significance of risk is evaluated.
Note 1: Risk criteria are based on organizational objectives and external and internal contexts.
Note 2: Risk criteria can be derived from standards, laws, policies, and other requirements.

Risk evaluation – Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable
Note 1: Risk evaluation assists in the decision about risk treatment.

Risk identification – Process of finding, recognizing, and describing risks
Note 1: Risk identification involves the identification of risk sources, events, their causes, and their potential consequences.
Note 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions.

Risk management – Coordinated activities to direct and control an organization with regard to risk.

Risk management process – Systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk

Risk owner – Person or entity with the accountability and authority to manage risk

Risk treatment – Process to modify risk
Note 1: Risk treatment can involve:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to a risk
- Taking or increasing risk in order to pursue an opportunity;
- Removing the risk source;
- Changing the likelihood;
- Changing the consequences; –
- Sharing the risk with another party or parties (including contracts and risk financing); and
- Retaining the risk by informed choice.

Note 2: Risk treatments that deal with negative consequences are `sometimes referred to as “risk mitigation,” “risk elimination,” “risk prevention,” and “risk reduction.”
Note 3: Risk treatment can create new risks or modify existing risks.

Senior Manager of Information Security (SMIS) – The senior manager who is in charge of implementing, managing, and measuring the effectiveness of the ISMS program within the company.

Security Incident – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening the confidentiality, integrity, and availability of information or Resource Innovations Systems. With regard to the availability of information systems or information, “Security Incident” excludes incidents caused by sources such as natural disasters and power failures.

Security Incident Response Team (SIRT) – A team of IT professionals and the SMIS that investigate and respond to IT Security related events.

Stakeholder – A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Technology Asset or Asset – IT equipment and software owned by Resource Innovations, which may include, but is not limited to:

- Desktop Computers
- Laptop Computers
- Tablets & Smartphones
- Servers
- Projectors
- Printers
- Standard Software

Threat – Potential cause of an unwanted incident, which may result in hard to a system or organization

Vulnerability – Weakness of an asset or control that can be exploited by one or more threats