Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Data Classification Policy

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

REVISION HISTORY

Date	Version	Description	Author(s)
01/31/2022	1.0	Combined Nexant Resource Innovation Policies	Khalid Maletan
01/31/2023	2.0	Annual Review	Khalid Maletan
07/31/2023	2.1	Detailed data classification tables added	Khalid Maletan

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Purpose

In order to effectively secure Resource Innovations' data, staff must have a shared vocabulary to describe the data and the corresponding protection it requires. This Policy describes how company data is classified and the levels of protection required for each classification.

Data Classification Standards

All Resource Innovations information and all information entrusted to Resource Innovations from third parties fall into one of four classifications in order of increasing sensitivity.

Scope

This data classification policy is to be applied to all Resource Innovations data, both physical and electronic.

Policy

Resource Innovations managers or information owners shall be responsible for managing and assigning classifications to information assets in accordance with this Policy.

- All documents must be labeled with their data classification.
- The default data classification if a store or file is not otherwise classified is Confidential.
- If any customer data is contained in a storage area, such as a SharePoint Site, folder, or database, all data in that storage area should be classified as Client/Customer Confidential.
- Whenever possible, if moving data out of its privileged storage area, the data should retain its classification and should be protected based on the original classification.
- All records stored in production databases containing information on program participants will be treated as Client/Customer Confidential.

All Resource Innovations staff shall be guided by the information category in their handling of all Resource Innovations information.

Data Classification Summary

Client/Customer Confidential	This is the highest and most protected data type it includes all client data records, contracts and agreements(NDA, MSA, SLA).
Company Confidential	RI legal documents, strategic plans, trade secrets or financial information. Employee PII and PHI information
Confidential *	Business Information available to all employees, such as general program documents, templates, routine emails and memos.
Public	Any document approved for publication

* Default classification if a store or file is not otherwise labeled.

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Client/Customer Confidential

Client/Customer-confidential data is information that, if made available to unauthorized parties, may adversely affect Resource Innovations customers. This classification also includes data that Resource Innovations is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. All program data specific to the program, such as contracts, project plans, pricing, client data, etc., is considered Client/Customer Confidential. This information is to be protected against unauthorized disclosure or modification. Client/Customer Confidential data should be used only when necessary for business purposes with the permission of the client and should be protected both when it is in use and when it is being stored, processed, or transmitted.

Client/Customer Confidential data includes any personally identifiable data for the customers of a client, such as names or addresses of program participants.

Unauthorized access can influence Resource Innovations' operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in customer and industry confidence.

Example Information	Access Control	Transmission	Document Disposal	Disclosure to Third Party	Document Storage
All client data records, Contracts and agreements(Contracts, MSA, SLA).	Restricted to individuals as authorized by managers and/or senior management	Any external email must be encrypted. Hardcopy documents or portable media must be sent by services with tracking records. External electronic transmission must be encrypted, for example using SFTP	Information held on electronic devices shall be securely erased using appropriate tools.Printed document shredding within the local environment or contracted secure disposal.	Only with authorization from managers and/or senior management. Covered by a non-disclosure agreement	Within lockable storage systems or within a secure area

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Company Confidential

Company confidential data is information that, if made available to unauthorized parties, might adversely affect Resource Innovations. This information is to be protected against unauthorized disclosure or modification and might be limited to executives, HR, and legal parties employed by or under contract with Resource Innovations and with appropriate non-dsiclosure and confidentiality provisions in place. The data owner of the Company's Confidential data is responsible for providing permission to individuals to access data that is under their purview. All Company Confidential data should be protected both when it is in use and when it is being stored, processed, or transmitted.

Unauthorized access has the potential to influence Resource Innovations' operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.

Example Information	Access Control	Transmission	Document Disposal	Disclosure to Third Party	Document Storage
RI Legal, strategic plans, trade secrets or financial information. Employee PII and PHI information	Restricted to individuals as authorized by managers and/or senior management	Any external email must be encrypted. Hardcopy documents or portable media must be sent by services with tracking records. External electronic transmission must be encrypted, for example using SFTP	Information held on electronic devices shall be securely erased using appropriate tools.Printed document shredding within the local environment or contracted secure disposal.	Only with authorization from managers and/or senior management	Within lockable storage systems or within a secure area

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Confidential

Confidential data is potentially sensitive information that should not be shared with the public. Confidential data generally should not be disclosed outside of Resource Innovations without pre-authorization from the data owner or management. It is the responsibility of the data owner to designate information as Confidential where appropriate. Unauthorized access has the potential to influence Resource Innovations' operational effectiveness, cause financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.

Data that has no classification should be treated as Confidential until such time as it is reclassified by the data owner.

Example Information	Access Control	Transmission	Document Disposal	Disclosure to Third Party	Document Storage
Business Information available to all employees, such as templates, information Security or HR policies and procedures	Employees, contractors, auditors, and authorized third parties	Transmission only to third parties with a business justification. Must always be transmitted over secure mechanisms and must be protected from inadvertent sharing.	Documents and data must be disposed of in a secure manner	With a business justification.	Within offices

Public

Public data is information that may be disclosed to any person regardless of their affiliation with Resource Innovations. The "Public" classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not require any level of protection from disclosure. While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside Resource Innovations, and no steps need to be taken to prevent its distribution.

Example Information	Access Control	Transmission	Document Disposal	Disclosure to Third Party	Document Storage
Any document approved for publication	No restriction	No restriction	No restriction	No restriction	No restriction

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

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			
Data Classification 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:		**Signature:**	
Date:	July 31, 2023	**Date:**	July 31, 2023