Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

System Access & Authorization Control Policy

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
7/31/2023	2.1	Addition of Machine to Machine Guidance and Confidential classification	Khalid

Each Resource Innovations employee, contractor, and associate shall be given access to devices, systems, and applications based on the concept of least privilege and only be given access to devices, systems, and applications to do their job.

Employee Access to Resource Innovations Systems

Access to Resource Innovations systems and third-party accounts owned by Resource Innovations will only be granted on a need-to-know basis, as defined by the responsibilities of the position held and the duties of that position.

Access control and management are divided into multiple phases of an account lifecycle: creation, privilege management, authorization, password management, audit, and revocation.

Authorization: Role-Based Access Control

- In most cases, Resource Innovations employees are granted access to Resource Innovations systems according to their role and/or team.
- The system and or data owner is responsible for maintaining a list of roles and associated access scope for team members.
- If a Resource Innovations employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the Policy outlined in “access requests” below.

Creation: Access Requests

- Access requests for Resource Innovations employees are made by employees and their managers.
- Access requests should be made to the Resource Innovations employee or employees who manage the relevant resource(s).
- The system and or data owner will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.
- When granting access, employees will ensure grants are scoped to the minimum breadth and duration to complete the relevant business task. Root access will not be granted unless absolutely necessary to perform the job function.

In addition, the employee(s) must accept the company’s Acceptable Use Policy before access will be granted.

Privilege Management

- Resource Innovations’ system or data owners will determine and maintain appropriate assignment of privilege within Resource Innovations’ devices, systems, and applications.
- Resource Innovations’ IT team will determine and maintain appropriate assignments within supporting infrastructure.

Account Audit

- Systems and data owners of Key Systems, as defined by the IT System Inventory, shall conduct, at a minimum, an annual access control audit of the systems under their control.

Revocation: Role Changes & Termination

- Managers must notify Resource Innovations' IT team if an employee has been terminated or changes role.
- In the case of termination, the former employee's access is required to be revoked within reasonable timelines as defined by company procedural commitments.
- In the case of a role change, the employee's access should be revised within reasonable timelines as defined by company procedural commitments.
- In some cases, access will be revoked as a disciplinary measure for policy violation.

Machine to Machine

All communications between endpoints, such as network devices, server-to-server, and machine-to-machine (M2M) communications, must be secured through encrypted digital certificates or digital credentials. Under no circumstances are machines allowed to bridge or route traffic from unsecured third-party networks or devices without authorization from the security and IT teams.

Employee Authentication to Systems

Authentication

Each Resource Innovations employee shall have a unique user ID and password that identifies them as the user of a Resource Innovations IT asset or application. All assets, applications, and vetted third-party platforms may be required to have two-factor authentication configured.

Password, Key, and Certificate Management

As specified in the Acceptable Use Policy and Password Policy, Resource Innovations employees must use complex passwords and, where possible, use multi-factor authentication for all Resource Innovations-related accounts. User passwords must conform with the restrictions set forward in the Resource Innovations Password Policy. Please see the Acceptable Use Policy and Password Policy for further details and guidance.

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.

System Access & Authorization Control Policy			
System Access & Authorization Control 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