Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

Business Continuity 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	Added Confidential classification	Khalid Maletan

Purpose

The purpose of the Business Continuity Policy is to establish business process continuity, availability, and security of Resource Innovations information systems in the event of an emergency, disaster, or other significant business disruption that interferes with Resource Innovations' ability to deliver company services.

Scope

This Policy applies to all Resource Innovations' employees, temporary employees, volunteers, interns, and Resource Innovations vendors who:

- Support one or more critical business functions as defined by Resource Innovations
- Provide a service or application with high availability requirements

Roles and Responsibilities

The Director of Information Security is designated as the corporate management liaison responsible for the business continuity program. Resolution of issues in the development of, or support of, all business continuity and disaster recovery plans and associated activities should be coordinated with the Security Committee.

Site Security Contact will be responsible for implementing the business continuity plans under the direction of the incident response team and oversight by the Director of Information Security.

Business Impact Analysis

Resource Innovations shall conduct a business impact analysis (BIA) to identify critical services, recovery time objectives (RTO) and recovery point objectives (RPO), exposures to the continuous availability of services, security vulnerabilities, and possible mitigation strategies. The BIA will be submitted to the Security Committee for review and identification of critical business functions which are to be addressed through business continuity planning. Upon approval by the Security Committee, the BIA will be distributed to BCP Coordinators for completion of business continuity plans. The BIA will be updated annually and presented to the Security Committee for review.

Business Continuity Planning

Business continuity plans (BCPs) are to be developed, maintained, and periodically tested to address key risks and critical processes for personnel, technology, and facility requirements in the event of a Disaster. The objective of the BCP is to coordinate the recovery of critical business functions with a focus on the following priorities:

- Ensure the safety of employees and visitors in the office buildings.
- Mitigate threats or limit the damage that threats can cause.
- Have advanced preparations to ensure that critical business functions can continue.
- Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.
- BCP plans shall be reviewed and communicated to Resource Innovations staff, at a minimum, annually or if there is a significant change.

The following groups will be responsible for developing BCPs in accordance with the procedures outlined in the Business Continuity Management Procedures.

- Corporate (HR, Finance, Legal, Executive, IT)
- iEnergy
- Grid Management

To ensure that any damage or disruptions to critical IT assets supported by Corporate Information Technology (IT) can be quickly minimized and that these assets can be restored to normal or near-normal operation as quickly as possible, disaster recovery planning will be incorporated into each group's BCP, as applicable. Corporate IT will coordinate with the listed groups to develop disaster recovery plans (DRPs) to meet the RTO and RPO objectives identified in the BIA for that group.

Plans must be reviewed and tested annually with a minimum of a tabletop walkthrough of the plan with findings documented, along with a plan for remediation of discrepancies found during the testing process.

Business unit heads will coordinate with the incdent response team and Site Security Contact during a Disaster to identify which BCPs are triggered to go into effect.

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			
Business Continuity 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

Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

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