Resource Innovations
719 Main Street
Half Moon Bay, CA 94019

# Password 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 |

Resource Innovations' Password Policy describes how employees should generate, store, and retrieve their passwords for services they use on behalf of the company.

## Scope

This Policy applies to all employees, contractors, or vendors who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on Resource Innovations' infrastructure, whether in the cloud or on-premises.

## Password Generation

Resource Innovations employees must use unique, complex passwords, where possible, for all of their accounts that have access to Resource Innovations data, systems or applications.
The same password should not be used for multiple sites or accounts.
Passwords must be "Complex" and have at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character and are at least eight characters long.
Resource Innovations employees may not reuse passwords that are or were used elsewhere, e.g., passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services.
When creating end-user passwords for the first time and/or during a password reset, the IT team may force the end-user to change their password upon logging in for the first time and/or provide assistance in order to ensure the password is changed such that the new password is known only to the user.
Resource Innovations employees must use two-factor authentication, where applicable, for all accounts that have access to Resource Innovations data.

## Password Requirements from Services

The services that Resource Innovations uses to provide its offering may also enforce password rules, which all users (including Resource Innovations employees) must follow. The service offering team must, at a minimum, comply with or exceed the password requirements outlined in this Policy.

## Managing and Storing Passwords

Resource Innovations employees are strongly encouraged to use a Password Manager (i.e., LastPass or 1Password) to manage their passwords and generate sufficiently complex passwords.
All Resource Innovations system and user passwords must be encrypted when stored at rest within an application or database.
All Resource Innovations system and user passwords must be encrypted during transmission.
Under no circumstances should Resource Innovations employees share their account passwords with anyone, including other Resource Innovations employees, except in cases where the password is needed to mitigate issues with user accounts or hardware access as prescribed by the IT Team.

## 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** | | | |
| **Password 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 |