**California Department of Rehabilitation**

**Multi-Factor Authentication – Vendor Reference Guide**

The Department of Rehabilitation’s (DOR’s) VR Connections Portal Multi-Factor Authentication (MFA) feature is a two-step authentication process that allows vendors to securely access DOR authorizations via the Portal. This feature is similar to current banking and healthcare systems requiring users to prove their identity with two verification factors to gain access to their account. The MFA feature is being introduced in the VR Connections Portal in accordance with the California Government Code Regulation (11549.3), which states that sensitive/personal information must be protected.

The DOR is providing vendors with three methods to complete the MFA when they login:

1. Email
* Log into Portal using your email address and password
* An email will be sent to you with a short code to complete the login
1. Text
* Log into Portal using your email address and password
* A text will be sent to you with a short code to complete the login
1. Salesforce Authenticator App
* Download the Salesforce Authenticator App to a mobile device
* Log into the Portal using your email address and password
* The App will generate a code at login to complete the login

This prevents anyone who does not have access to your email address, password, and additional verification factor from accessing the Portal and your account information.

Initial Signup for MFA – Vendor Information

* You will receive an email, similar to the one below, when you are being sent a DOR authorization:



* If you do not already have an MFA account, the link will take you to a registration page like this:



* Please enter an Authorization Number previously issued from DOR to your company to confirm your identity. This is a one-time confirmation. (NOTE: For new vendors only, you can enter the current Authorization Number).
* **Create a password and confirm it. Ensure password is sufficiently complex and meets the minimum requirements. (Minimum password length is 10 and must include alpha and numeric characters)**
* You will then select a preferred MFA method (Email, Text, or Authenticator App - see below). NOTE: Once you select an option, you cannot change it.

Email Verification Code

* You will receive an email with the code to enter in the Verify Identify Box

Text Message Verification Code

* You will receive a text message with the code to enter in the Verify Identify Box

Salesforce Authenticator App

* Open the Salesforce Authenticator App
* Your Vendor’s connected accounts are listed, and each has its own 6-digit code
* Select the correct Vendor account and enter the 6-digit code in the browser (each code expires after 30 seconds)
* NOTE: The MFA App is available for both iOS and Android devices.
* Click Sign Up to begin.

Logging in once the Vendor has established an MFA Account:

* You will receive an email notification that an authorization has been issued to you, like the one shown above.
* You can then log into your account with your password:
	+ Based on the MFA method you selected during registration; you’ll be able to complete your login (example below represents the email MFA method):



* After completing MFA, you will then be logged into the Portal and can open and access the authorization.

For more information, please visit the DOR’s VR Connections webpage at

<https://dor.ca.gov/Home/VrcIntro>