State of California – Department of Rehabilitation

MEMORANDUM

To: All DOR Employees (DORALL)

From: Armel Biscocho, Deputy Director

Administrative Services Division

Kathi Mowers-Moore, Deputy Director

Vocational Rehabilitation Policy & Resources Division

Date: April 16, 2020

Subject: **Interim Policy – Using Email for Electronic Signatures**

This memorandum provides guidance on the Department of Rehabilitation (DOR) interim policy regarding the use of email communication as an acceptable substitution for electronic signatures during California’s declared State of Emergency related to COVID-19.

# ISSUE

The DOR recognizes the challenges involved in balancing consumer, vendor, stakeholder, and DOR staff needs, as well as implementing creative service delivery solutions to meet the circumstances related to COVID-19. The DOR acknowledges the dedication and commitment of DOR staff and our partners to continue to serve all consumers during this time of uncertainty and change.

**In order to prioritize the health and safety of our consumers, partners, and staff, and proactively do our part to minimize the spread of COVID-19,** DOR is identifying creative service delivery solutions and innovative ways of conducting business to meet immediate, short-term, and long-term needs of consumers, vendors, stakeholders, and staff.

# Background

On March 4, 2020, Governor Newsom declared a State of Emergency and on March 19, 2020, Governor Newsom issued a Stay at Home order statewide and declared government operations as essential. To further the purpose and intent of these orders, DOR is rapidly operationalizing its Electronic Signatures Policy to allow critical program services and business operations to continue.

Pursuant to the department’s Electronic Signatures Policy, adopted in December 2018, DOR shall use and accept electronic signatures. While DOR continues to develop new, accessible, and long-term electronic signature solutions, DOR staff and partners are permitted to utilize email correspondences as substitutes for signatures.

# Policy/Procedure

Effective immediately, for the duration of the California State of Emergency and until further notice, DOR will accept email correspondence as an acceptable means of electronically signing most internal and external documents and forms. (Refer to [Section E](#_The_Following_Documents) for a list of forms for which email is not considered an acceptable substitute for signature at this time.)

This policy includes the acceptable use of email as signature for business services, administrative, and accounting processes. Email correspondence is also considered an acceptable substitute for a signature received from program recipients and participants, cooperative partners, service providers, vendors, and DOR staff.

The DOR is currently exploring other options that could be used as acceptable signature substitutions and will provide guidance on other options, as appropriate, at a future date. At this time, telephone calls and text messages are not acceptable substitutes for signatures.

## The following language must be included in every email sending an electronically-signed document:

1. Each individual must agree to accept electronic signatures and conduct the transaction electronically. Whether the parties agree to conduct a transaction electronically is determined from the context and surrounding circumstances, including the parties' conduct.
2. An individual must have the ability to refuse to accept electronic signatures or conduct future transactions electronically.
3. The electronic signature must be attributable to the person signing.
4. Each individual must be able to keep the electronically-signed document.
5. Each individual should identify if a change is made in the electronic record. If the change is not identified, the agreement may be voided by the individual who was not made aware of the change.
6. If a notice of right to cancel is required, an electronic record may only be used if the notice of cancellation may also be an electronic document. The notice of right to cancel is only required in certain types of contracts.

## Options for Storing Electronically-Signed Documents

1. If a record is required to be retained, the requirement is satisfied by retaining an electronic record of the information in the participant’s record of services (e.g., as an attachment, or hardcopy), if it accurately represents the information contained in the final form.
2. It is critical that all relevant email correspondences be saved and logged for later retrieval. For example, applicable emails must be saved as attachments to the appropriate participant’s electronic record of services in *Aware* or attached to an invoice for services.

## Use of Social Security Numbers and Sensitive Information

In an effort to ensure the protection of participant, vendor, and provider information, DOR is undergoing a full review of forms that currently require either a Social Security Number (SSN) or Tax Identification Number (TIN). Some of these forms may be modified in the near future to either remove or strike the SSN/TIN fields for the duration of the declared State of Emergency. In the meantime, staff are asked to exercise prudence when utilizing email correspondences that may include sensitive or confidential information, and to take the following measures:

1. While email may be temporarily suitable for signature purposes, DOR recognizes an ethical obligation to discourage the transmission of sensitive and confidential information over insecure or unencrypted channels. Before sending confidential information, ensure the accuracy of the email address. Never send full Social Security Numbers over email.
2. Advise participants, vendors, and providers not to include their full SSN via email, and to be aware of the risks when sending out
3. Encrypt email communications that may contain sensitive information. Refer to [Attachment 1](#_Attachment_1:_How) for instructions on using Microsoft Outlook to encrypt email and attachments, or for alternate encryption options.

## The Implementation of this Interim Policy Does Not Guarantee the Use of Email as a Permanent Substitution for Electronic Signatures.

1. The DOR is actively working on more robust and accessible solutions for electronic signatures and may pilot new initiatives at any time.
2. Additionally, this interim policy does not guarantee the fully acceptable use of electronic signatures for all processes beyond the California State of Emergency, as some of those processes are dependent on state or federal regulation, or policies imposed by oversight agencies.

## Documents That May Not Be Electronically Signed

The following documents may not be electronically signed at this time:

* DR 260 Consent to Release and Obtain Information
* SSA 3288 Social Security Administration – Consent for Release of Information

# Resources

The DOR Team Managers and District Operations Support (DOS) Managers may contact [program.policy@dor.ca.gov](mailto:program.policy@dor.ca.gov) with policy questions.

Contract Administrators may contact the Cooperative Programs Section email at [cssinfo@dor.ca.gov](mailto:cssinfo@dor.ca.gov) and cooperative partners may contact the DOR Cooperative Program Specialist assigned to your program.

Community Rehabilitation Programs may contact the DOR Community Resources Development Section email at [crdssinfo@dor.ca.gov](mailto:crdssinfo@dor.ca.gov) or the DOR CRD Specialist assigned to your program.

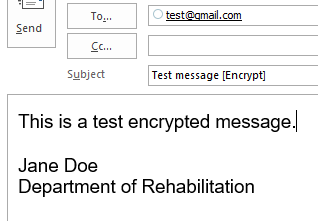
Contractors and DOR staff with questions regarding contract and procurement please email [contractsinfo@dor.ca.gov](mailto:contractsinfo@dor.ca.gov). For accounting questions, please email [acctnginfo@dor.ca.gov](mailto:acctnginfo@dor.ca.gov).

# Attachment 1: How to Encrypt Confidential Information

The following instructions are also available on the InDOR intranet, at the following link: <http://indor/itsd/information-security-privacy-office/how-to-encrypt-confidential-information>.

## How to Encrypt Email Messages Containing Confidential Information

If you have confidential information to send electronically, encrypted email messages can easily be done by typing the word “encrypt” within square brackets anywhere on the **Subject** line of the message (see the following example: **[encrypt]**). The word “encrypt” can be in upper or lower caps, or any combination thereof, as the functionality is not case sensitive.



The recipient will then receive an email with an attachment providing them with the instructions on how to open up the message. The easiest way to open up the message is for the recipient to choose the option for a one-time or single-use passcode.

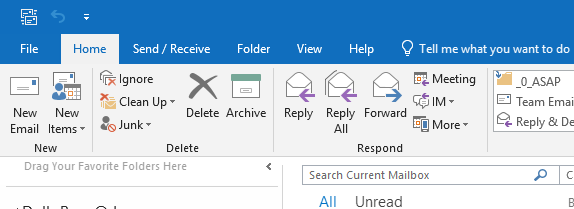
**Note:** Encrypted email being sent between DOR employees will appear as if unencrypted and will not require a password to access.

A guide from Microsoft on using the One Time Passcode option when recipients receive an encrypted email: <https://blogs.office.com/en-us/2014/10/03/one-time-passcode-office-365-message-encryption/>

## How to Encrypt Microsoft Products Containing Confidential Information

All Microsoft products have the ability to be encrypted with password and that is an alternate solution that you can use.

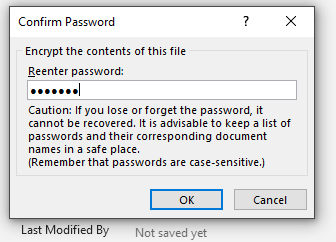
1. Within the Microsoft document (e.g., Word, Excel), select the **File** tab.



1. Under the **Info** tab on the left, select **Protect Document**.



1. Select **Encrypt with Password**.
2. Enter a password of your choice. Press **OK**.
3. Reenter your created password to confirm. Press **OK**.



1. The document is now password encrypted and will require the created password to open the document.

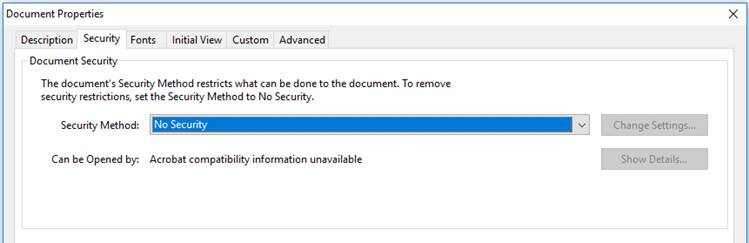
**Note:** Be advised that this password cannot be retrieved if lost. Also, it is highly discouraged to use a password already associated to other user accounts or logins, such as using the same password as Outlook login.

## How to Encrypt Adobe PDF File Containing Confidential Information

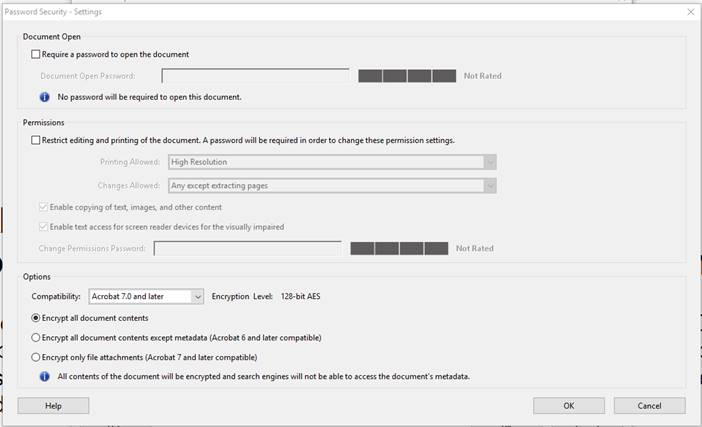
For .PDF documents, in order to password encrypt the document, you must either have access to Adobe Acrobat or have someone who has access to Adobe Acrobat protect the document.

The steps are as follows:

1. Make sure that you open up the document with Adobe Acrobat, not Adobe Reader.
2. You can find out if you have access to Adobe Acrobat by right-clicking on the document and choose **Open with** > Adobe Acrobat.
3. Once the document is open, click on the **File** tab.
4. Click on **Properties**, the click on the **Security** tab.



1. On the **Security Method** section, choose **Password Security** from the dropdown box.
2. Click on the box **Require a password to open the document**.
3. Create a password and press the **OK** button.



If you have any questions about this message, feel free to email the Information Security Office at [ISO@dor.ca.gov](mailto:ISO@dor.ca.gov?subject=Question%20about%20encrypting%20the%20message).