Sending Personnel Images Securely

Human Resource Services Division

Employment Security Department
WASHINGTON STATE

Overview

Confidentiality around our staff personnel files is critical and sending the images electronically provides us with opportunities to create the transfer of this information more secure than through the mail. For the purposes of this process there are two primary recipient categories that personnel images would be sent to:

1. ESD Staff – this can include employees, managers/supervisors or administrative assistants.
2. Other Agencies or Non-Governmental Entities – other agencies, schools, unions, attorneys, etc.

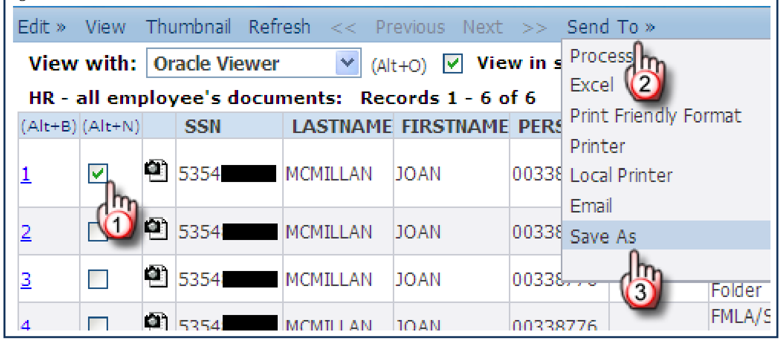
The steps below will be used whenever sending confidential images outside the HRSD.

Export Process for Documents:

NOTE: You must do this one at a time for each image. For a Larger Set of Documents or an Entire File please contact the HRSD scanning operations team.

1. Select the image from imaging system by checking the box next to the record you want (see Figure 1).
2. From the menu, select “Send To »”
3. Select “Save As”.
4. When prompted, select “Save” and browse to a location you would like to save the image to. Pick a location you will be able to easily locate (create a folder on your desktop for example).
5. The system will provide a system generated name for the image (TIF is an image format). Change that name to something you can easily identify to that document (for example, “JoanMcMillan.TIF”. Do NOT use something confidential like a combination of SSN and name.
6. Click the “Save” button.

Figure 1



View with: Oracle Viewer (Alt+O) ☑ View in s

HR - all employee's documents: Records 1 - 6 of 6

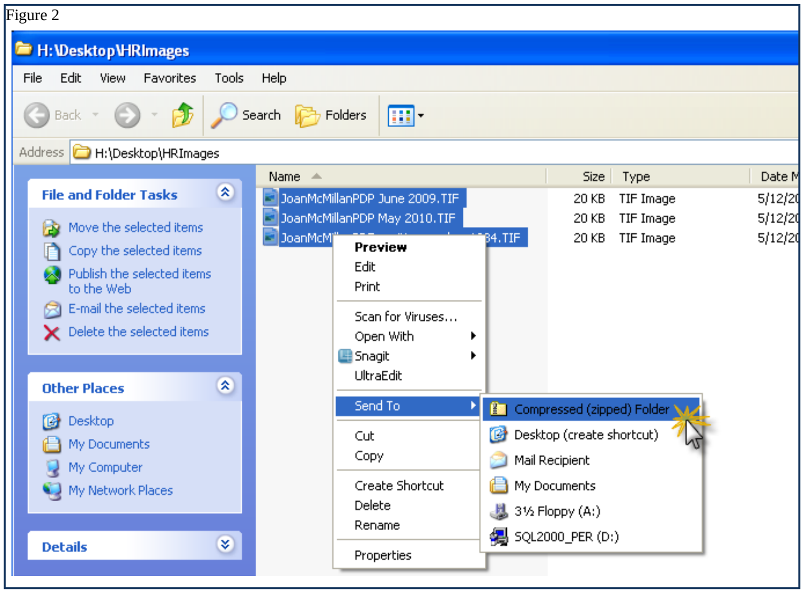
(Alt+B)	(Alt+N)		SSN	LASTNAME	FIRSTNAME	PERS
1	☑		5354[redacted]	MCMILLAN	JOAN	00338
2	□		5354[redacted]	MCMILLAN	JOAN	00338
3	□		5354[redacted]	MCMILLAN	JOAN	00338
4	□		5354[redacted]	MCMILLAN	JOAN	00338776

Even if this document is going to a person within the agency, you must still determine whether the document should be considered confidential before you attach it to an email and send it. If it is confidential or leaving the agency, use the process defined below for “Password Protecting a File(s)”.

Password Protecting a File(s):

1. Open the folder with the document(s) you would like to password protect.
2. Select them (hold the Ctrl and the Shift key to select multiple)
3. Right click on the highlighted documents and select “Send To” and “Compressed (zipped) Folder” (See Figure 2).
4. A folder will be created that contains all the documents you had selected.
5. Open that *.zip folder by double clicking.
6. Select “File”, “Add a Password…”
7. At the prompt, provide a password.
8. Select the Back button to move up one level. While the zip folder can be opened, when anyone tries to open the documents within it, they will be prompted for a password.

Figure 2



Name	Size	Type	Date M
JoanMcMillanPDP June 2009.TIF	20 KB	TIF Image	5/12/20
JoanMcMillanPDP May 2010.TIF	20 KB	TIF Image	5/12/20
JoanMcM…4.TIF	20 KB	TIF Image	5/12/20

Process for securely sending a Password Protected ZIP File

In order to add an additional level of security and confidence, always follow-up after sending the file with a phone call to the recipient to provide the password to access. Do not include the password in the email to ensure that even if the wrong person intercepts or receives the file accidentally, they cannot view the contents. By using two different methods to deliver the entire package (file + password), we can ensure that delivery is secure.

NOTE: The agency email system will not allow a file more than 30MB to be sent. You will receive an undeliverable message but this will be rare. If this happens, you can use a CD to deliver the file.

Once the file is ready to go and there is a password, there are three methods to send it to the recipient. For all methods, you should provide the password to the zip on a phone call to ensure you have the right recipient and that it wasn't intercepted and viewable.

A. **Internal ESD email** – Attach the zip file to your email message and send it. Call with password.
B. **External email** (any other agency or non-governmental entity) – the process for sending an email attachment to an external email recipient should always include the **secure e-mail standard for the agency**. Remember to include the characters *.key (followed by a space) before your subject on the subject line of the email to utilize the encryption functionality. *For more information on using the agency secure/encrypted email system, contact the agency help desk.*
C. **CD** – after "burning" or copying the zipped and password protected file to a CD, send the CD in a sealed envelope to the recipients address and follow up with the password either via email or phone. Do NOT include the password in the envelope.

Contact Information

Imaging System or LiquidOffice

send an e-mail to esditsdimaging@esd.wa.gov (**ESD GP ITSD Imaging** in Outlook) and one of the Enterprise Imaging Team will contact you.

Secure Email

contact the agency help desk at 877-397-1212 or use the Requestor Console located on Insideesd.