LOS RIOS COMMUNITY COLLEGE DISTRICT

Guidelines for sending High Risk Data via Email/Fax

To conform with Los Rios regulations 8871, the guidelines for sending High Risk Data via Email/Fax are provided below.

Email:

The Los Rios Community College District email system is an insecure communication medium. It is imperative and required by District regulations (R-8871, section 3.2.4) that high risk data not be sent in emails unencrypted, either in the email subject/body or as an attachment. If high risk data must be sent via email, the high risk data must be encrypted with 7-Zip, or Adobe Acrobat Pro. The password to unlock (decrypt) the encrypted attachment must be provided separately (e.g., by phone, in person, by stand-alone non-networked fax machine, or as a last resort via a second email that does not describe what it is). Below are links to the instructions on how to encrypt a document with 7-Zip and Adobe Acrobat Pro.

- How to encrypt using 7-Zip
- How to encrypt using Adobe Acrobat Pro

Fax:

The Los Rios Community College District fax server uses the email system, therefore, the District fax server is an insecure communication medium. Do not to send high risk data using a networked fax machine. The preferred method is to scan and then encrypt the document and email it (see 1st paragraph). If the information must be sent via fax, fax only from a stand-alone non-networked fax machine and make sure to contact the recipient to arrange for its receipt.

What is High Risk Data (District R-8871, section 3.1.1):

- Social security number
- Driver's license number or California identification card number
- Financial account number
- Credit or debit card number
- Medical information = any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- Health insurance information = an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
- Information or data collected through the use or operation of an automated license plate recognition system
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Please contact your IT department if you are having trouble finding or using the encryption software covered in the “How to” documents.

Last Modified: November 29, 2017