Non-Associate

Acceptable Use Procedure for Assignment at JM Family Enterprises, Inc. (JMFE)

Purpose

To provide Authorized Users with a procedure to assist them in complying with the Non-Associate Information Security and Acceptable Use Standards.

Procedures

Strong Password Best Practices

When you create a password, you should create strong passwords for the best security. Try using these tips:

- Easy-to-remember tips are to create an acronym from a piece of information, or a child's nursery rhyme.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase.

Mary had a little lamb could be: ***M@ryHdaLtt!l@m8***

- Relate your password to a favorite hobby.

  For example: ***iLuv2PlayF()()tB@LL***

Also remember these requirements:

- Avoid using passwords that are found in the dictionary or are family names or special dates.
- Never write down passwords or store them in a file for retrieval.
- Passwords must be a minimum of 8 characters in length and should include upper and lower case letters, numbers and/or symbols.

Sending Secure Email Messages Outside of JM Family

First and foremost, make sure the information you are emailing outside of JM Family's network *needs to* include Sensitive Information. For example, if you need to email a spreadsheet to a vendor, review it before sending to make sure all the columns of data are actually necessary for the

vendor to have.

If not, delete the applicable rows or columns (don't hide them!). If you still need to transmit Sensitive Information by email, be sure to send it securely by encrypting it.

Using JM Family's encryption tool is easy. Simply type the word "*Confidential*" in the subject line of your email message. This ensures your email will be sent using JM Family's secure email system. The recipient will receive an email with instructions on how to login to our secure email system, so you may want to let them know ahead of time that you've sent them an encrypted message that they will have to access by logging in to our system. They will follow the prompts to create a password to gain access to the encrypted email you sent.

Accessing JM Family Information From Home or Remotely

If you need to access files from home or when you travel, you can connect remotely by using a two-factor authorization token provided by ITS. You will need to contact the Service Desk at 888-739- 6800 to request a token, which must be authorized by a member of JMFE leadership.

Storing Information Securely on an External Storage Device

An external storage device provides storage for information in a very convenient way. Some examples of external storage devices are USB memory sticks, CD or DVD. If you need to store Sensitive Information on an external storage device, it must be secured using an approved JM Family encryption tool. You will need to contact the Service Desk at 888-739-6800 to request special authorization to copy Sensitive Information to an external storage device and you can request the tool that will enable you to encrypt files on the approved external storage device.

As a general rule, never use an untrusted external storage device to store your files or plug into your computer. If you find a USB stick or other storage device and you don't know who it belongs to, do not plug it in to a computer but contact The Service Desk for instructions to transfer the device to ITS for analysis.