Policy Title: **ENCRYPTION**

Sending, receiving, and storing sensitive information using unencrypted methods can lead to the compromise and disclosure of sensitive Fox Valley Technical College (FVTC) data. FVTC personnel must use encryption when sending and storing sensitive data. This includes social security numbers, credit card numbers, or any other data that is personal in nature. This policy applies to all devices with sensitive FVTC data stored on them, the transfer of sensitive FVTC data, and personnel who are responsible for or have access to sensitive FVTC data.

All laptops, workstations, and portable devices that are used to store or access sensitive FVTC data require encryption. IT will provide, install, configure, and support encryption on laptops, workstations, or portable devices that need to be encrypted. FVTC provided staff devices are encrypted prior to distribution.

When sending and storing sensitive data is necessary, it must be encrypted or delivered through an encrypted channel. If the encryption method requires a password, that password must be communicated through a different method. All email communications involving email addresses outside of FVTC require encryption if the messages contain sensitive data.

Any sensitive FVTC data placed on a medium such as a CD, DVD, or portable device must be encrypted. Archiving sensitive FVTC data to a physical medium is not permitted. IT manages data archival in a secure and controlled data center.

Individuals who require encryption for other purposes or are unsure if they are correctly encrypting sensitive FVTC data should contact the IT help desk.

*Adopted: 09/27/17*
*Reviewed: 11/7/18*
*Revised: 11/7/18*