Version: 1.1

ENCRYPTED Database, documents, spreadsheets or files stored on FLC IT Department managed laptops, workstations, mobile devices or tablets	**YES.** Contact the IT department to verify that your system is encrypted. Idle screen saver enabled and password protected. Protect devices from theft or loss.	**CAUTION:** Do not upload, transfer or post Confidential Demographic Data on unsecured Wi-Fi networks. Do not leave device unattended in unsecure areas.	Collect and store the least amount of data necessary, for the least amount of time necessary. Follow applicable retention guidelines found at: www.fortlewis.edu/recordsmgmt	Return unused, damaged or end of life devices to Help Desk. Follow applicable disposal guidelines found at: www.fortlewis.edu/recordsmgmt
Databases, documents, spreadsheets or files on NON-FLC provided workstations, laptops, mobile devices, or tablets.	**NO.** Do not store confidential demographic data here.	**NO.** Do not upload, transfer or post confidential demographic data here.	**CAUTION:** If confidential demographic data found here, contact the IT department.	**CAUTION:** If confidential demographic data found here, contact the IT department.
Data stored on removable media: CD's, DVD's, Flash Drives	**NO.** Do not store confidential demographic data here.	**NO.** Do not upload, transfer or post confidential demographic data here.	**CAUTION:** If confidential demographic data found here, contact the IT department.	**CAUTION:** If confidential demographic data found here, contact the IT department.
FLC IT Department managed email account	**NO, with limited exceptions.** Do			

6 ced