**Windows and Linux Encryption**

***Microsoft Windows provides encryption tools to prevent loss of confidential data.***

* ***Encrypting File System (EFS) encodes files in order anyone who is able to get the files not to be able to read them. The files are only readable when we sign in to the computer using our user account. We can use EFS to encrypt individual files and entire drives. It is recommended to encrypt folders or drives instead of individual files. When we encrypt a folder or a drive the files contained are also encrypted. Even new files created in the encrypted folder are automatically encrypted.***
* ***BitLocker Drive Encryption provides another layer of protection by encrypting the entire hard drive. By linking this encryption to a key stored in a Trusted Platform Module (TPM), bitLocker reduces the risk of data being lost when a computer is stolen or when a hard disk is stolen and placed in another computer. In such scenario the thief will boot into an alternate operating system and try to retrieve data from the stolen drive or computer. With BitLocker that type of offline attack is neutered.***
* ***BitLocker To Go extends BitLocker encryption to removable media such as USB flash drives.***

***Linux provides a number of cryptographic techniques to protect data on physical devices such as hard disks or removable media. Such technique is Linux Unified Key Setup (LUKS). This technique allows the encryption of Linux partitions.***

***Using LUKS you can encrypt the entire block device which is well suited to protect data on removable storage or the laptops disk drive. LUKS uses the existing device mapper kernel subsystem and also provides passphrase strengthening for protection against dictionary attacks.***