CSUN | INFORMATION TECHNOLOGY

ENCRYPTED REMOVABLE MEDIA

ENCRYPTION

Encryption is a process of scrambling readable text into random text so an unauthorized user cannot interpret the data. During the data encryption process, a unique key called an encryption key is generated (e.g. passphrase/password, string of characters). To decrypt and view this data, a user needs to input the encryption key.

It is best practice to follow industry standards and policies. The National Institute of Standards and Technology (NIST) provides guidelines. For more information visit NIST's Guide to Storage Encryption Technologies for End User Devices. Advanced Encryption Standards (AES) is an encryption algorithm which has been adopted by the U.S. Government and is used worldwide.

CSU DATA HANDLING & STORAGE POLICY

Per CSU Policy 8065 – Information Security Asset Management, Level 1 data stored electronically must be encrypted using strong encryption methods.

Data owners are responsible for classifying their data and identifying procedures that must be followed to ensure the integrity, security, and appropriate level of confidentiality of this information is maintained. Please review CSU Data Classification to identify the data class of your information. Data owners must use CSUN Confidential Box (not the same as myCSUNBox) as a secure solution to store Level 1 data in the cloud. Level 1 data stored locally on a workstation or on a USB drive must be encrypted.

DATA STORAGE RISKS

Removable media are devices such as USB drives, External Hard Drives, or CDs/DVDs. Confidentiality of information stored on removable media may be breached due to loss or theft of the physical device. In addition, malicious actors may gain physical or logical access to the removable media compromising the confidentiality of the data stored within.

Due to these risks it is important for data owners to ensure proper handling of sensitive information. Encryption provides a layer of security and provides a level of assurance that data stored on removable media cannot be accessed without the encryption key (password or passphrase).

PRODUCT RECOMMENDATIONS

There is a wide array of commercial off the shelf products in the marketplace that offer onboard encryption. When selecting a product ensure it uses the AES encryption standard. Below are several product options that are acceptable for Level 1 data. Please ensure proper key management and sharing is in place to maintain confidentiality of the information.

Removable Media	Encryption Standard	Recommended Devices
USB Drives	AES 256 bit Encrypted	• Kingston Data Traveler • SanDisk Extreme • Imation IronKey
External Hard Drives	AES 256 bit Encrypted	• Western Digital My Passport • LaCie Rugged Secure

NEED HELP?

If you have any questions please contact the CSUN Information Security Office by phone at (818) 677-6100, by email at iso@csun.edu, or visit us at https://www.csun.edu/it/security.