UNIVERSITY OF Cincinnati	**COLLEGE OF ENGINEERING AND APPLIED SCIENCE** **Operating Policy**	
Category: Information Technology **Applicable for:** CEAS Faculty, Staff, Students, and Affiliates	**Encryption** **Effective Date:** January 1, 2018	**Document Owner:** CEAS Sr. Associate Dean for Operations & Finance **Responsible Office:** CEAS Dean

Background

Computers and computing equipment are essential tools for conducting the teaching, research, and public service missions of the university/CEAS. Appropriate encryption must be used to protect the confidentiality, integrity and availability of data stored and transmitted over electronic communication networks, such as student records and intellectual property. This policy addresses standards for encrypting restricted data on mobile devices.

Policy

Restricted data stored on mobile devices, such as laptops, external storage drives and cellular phones, must be encrypted to protect the confidentiality, integrity and availability of such data stored and transmitted over electronic communication networks. At a minimum, the following factors must be considered when determining whether or not encryption must be used when storing or sending electronic data:

1. The sensitivity of the data;
2. The risks to the data if they are not encrypted;
3. The expected impact to CEAS functionality and work flow if the data are encrypted;
4. Alternative methods available to protect the confidentiality, integrity and availability of the data;
5. The ability of the recipient of the data to decrypt the data received.

Encryption must always be used when highly sensitive data, such as export controlled data, research data, passwords or other restricted data, are stored and transmitted over electronic communication networks. All encryption used to protect the confidentiality, integrity and availability of data must be approved by CEAS IT.

Procedure

Laptops
Effective January 1, 2018, all newly purchased laptop computers within the CEAS that store or access restricted data are required to be encrypted. Laptop computers include mobile devices that run on Windows, Mac or Linux operating systems. Considering current encryption methods are seamless and transparent to the end user, the CEAS will encrypt all laptop devices regardless of use or storage of restricted data on such devices. When new laptop devices are purchased with university funds and configured by CEAS IT (OCC and department IT staff), such devices will be encrypted prior to being distributed.

Other Mobile Devices
Users must set a passcode or biometric code on other mobile devices purchased with university funds, such as iOS and Android.

Exceptions
Exceptions to encrypt a laptop may be granted if there is found to be any disruption or interference with the use and compatibility with other systems or software. Exceptions to encrypt may also be granted where international travel restrictions prohibit encryption. If traveling to countries with encryption restrictions, only unencrypted devices should be taken. Exceptions will only be granted if there is no restricted data to be stored or accessed from that device. Exceptions to encryption requirements must be approved by CEAS IT only after a risk assessment has been conducted. CEAS IT will maintain a list of exceptions and will periodically audit such devices to ensure there is no storage of restricted data.

Encryption keys will be maintained by CEAS IT to ensure safekeeping. Exceptions to key maintenance may be granted in the event an industry partner requires otherwise.

External USB Storage Devices
All external USB storage devices used within the CEAS that store restricted data are required to be encrypted. USB devices can be purchased with built-in encryption technology, or users may utilize the USB encryption software that is available through the laptop's operating system

Smartphones, Tablets and Other Personally Owned Portable Devices
All personally owned portable devices, including but not limited to smartphones and tablets, that store or access restricted data are required to be encrypted. Because these are generally personal devices and cannot be managed centrally, it is the owner's (user's) responsibility to ensure compliance and proper configuration of such devices. CEAS IT can provide assistance upon request. This is typically done through setting a passcode or biometric code on the device.

Email
All email communications containing restricted data are required to be encrypted. To send a secure (encrypted) Email, type the word **encrypt** as the first word in the subject line of the email message.

Related Links/Procedures/Policies

- Data Protection Policy 9.1.1
- Acceptable Use of Information Technology

A complete list of all information technology-related policies can be found at the UC Information Technologies (IT@UC) and the UC Information Security (InfoSec) websites.