

Information Security Policies
Hard Drive Encryption Policy

Version: 1.0

Effective Date:

9-23-11

Approved by:

IT Advisory
Committee

Hard Drive Encryption Policy

1.0 Purpose

This policy establishes requirements for hard drive encryption as a means of protecting Keuka College Information Technology resources. The impact of intrusion, theft, carelessness or other mitigating factors can be minimized by proper application of hard drive encryption.

2.0 Scope

This policy applies to all faculty, staff and students at Keuka College who maintain, enter or otherwise process sensitive college owned data. In addition this policy applies to all users of mobile devices containing Keuka College owned information.

3.0 Policy

All information handled by any user will be classified per the Data Classification Policy. Below is a list of the minimum requirements that must be met to comply with this Hard Drive Encryption Policy. This list is not all-inclusive and can be amended to by the Information Technology Services (ITS) Director or equivalent on an as needed basis.

If the data is deemed sensitive (based on the information classification spectrum) it will be transmitted and stored in a secure manner using industry standards and best practices in encryption.

All mobile devices (provided platform support is available) will use full disk encryption as well as support remote wipe of all (or at minimum sensitive) data on the device.

Any other computing systems not covered in the list above should use data encryption technologies that are approved by the Information Technology Services Director.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by the Information Technology Services (ITS) Director. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Encryption keys will be managed by the Information Technology Services (ITS) Director, and will be held in escrow. All encryption applications will be installed and managed by Information Technology Services (ITS).

4.0 Enforcement

To be defined by the standards and procedures documents

5.0 Definitions

Users – Faculty, Staff, Students, and other members of the Keuka college community that use or interact with the Keuka College network in any fashion.

Information – For the purposes of this document, any organized data stored in electronic form.

Sensitive Information – Data that is classified as sensitive per the Data Classification Policy

Mobile devices – Laptops, tablets, smartphones, eReaders, and other portable electronic devices are examples of mobile devices (this list is not all inclusive).

Proprietary Encryption – An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem – A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem – A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

3/16/2011 – rev 1.0 – Document Created

7.0 Policy Impact Statement

This policy will affect all users handling sensitive data in the Keuka College community. A hard drive encryption policy allows Keuka College to conform to industry standards and uphold Information Technology Services (ITS) guiding principals in regard to the protection of sensitive data handled by the college. This is one of the primary methods of mitigating potential data loss at Keuka College.