UNIVERSITY of NORTHERN COLORADO

Computer Encryption Policy

Purpose

To establish when encryption should be used on all institutional or personal computing devices.

Applies To

This Guideline applies to all students, faculty, staff, or other parties that store or manipulate University of Northern Colorado data who are using a personal or UNC issued computing device.

This does not apply to servers, appliances or networking devices, these are covered in separate policies.

Definitions

Encryption – The encoding of data for the purpose of making it inaccessible to all who do not have the decryption key.

Computing Device – In the context of this document this includes all computers, phones, or other data processing both personal and issued by the University of Northern Colorado.

Storage Device – All storage media which contains or interacts with or stores University data.

Strong Encryption – Currently AES (or similar standard) 128 bit or higher is considered strong encryption.

Full-Disk Encryption – The entire disk is fully encrypted.

File/Folder Encryption – Only a file or folder is encrypted the rest of the drive is not encrypted.

OIS – The Office of Information Security

Restricted Data – Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations, data protected by confidentiality agreements, and protected infrastructure data. The highest level of security controls should be applied to Restricted data.

Private Data - Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

Guidelines

All computing or storage devices issued by the University of Northern Colorado will be encrypted with a full disk encryption with a strong encryption algorithm.

All personal computing devices which store university data must use a file/folder encryption using a strong encryption standard for the secure storage of sensitive, *Restricted*, or *Private* data. Alternatively, full-disk encryption should be used to protect the any drive on which *Restricted* or *Private* data is stored. It is the responsibility of the individual who owns the device to comply with this policy.

All storage devices which contain sensitive, *Restricted*, or *Private* data must use a strong encryption standard to protect any sensitive or private data stored on the device.

An exception can be granted with the express written permission of the dean or assistant vice president. This exception must be filed with the Office of Information Security.

Revision History

Version	Published	Author	Description
1.0	2015/06/02	Matt Langford	Original publication.
1.1	2015/06/11	Matt Langford	Minor Updates
1.2	2016/08/17	Matt Langford	Annual Review. Format changes. Removal of obsolete text.
1.3	2017/07/20	Matt Langford	Annual Review. Minor updates to make Restricted and Private data in the guidelines more pronounced.
1.4	2017/06/05	Matt Langford	Annual Review. Removed date from footer.