

EDINBORO UNIVERSITY OF PENNSYLVANIA

CLOUD STORAGE POLICY

Policy No. C065

Recommended for Approval by Mr. Guilbert Brown, Vice President Finance and Administration

Approved by Dr. David Werner, Interim President on February 2, 2016

Review Date: As Required

INTRODUCTION

Cloud storage services are readily available tools used for accessing, storing, processing or transmitting University related data. These tools, regardless of whether they are personally or University owned, are governed by the procedures provided herein if they are used in conjunction with University Confidential or Sensitive data. The University's Information Security and Data Classification Policy C056 categorizes data into three security levels: Confidential, Sensitive and Public. This document focuses on the Confidential and Sensitive data types, hereafter referred to as University data. University Public data is not governed by such limitations.

PURPOSE

Edinboro University maintains data essential to the performance of University business. All members of the University community have a responsibility to protect University data from unauthorized generation, access, modification, disclosure, transmission, or destruction. The object of this document is to assist Edinboro employees in understanding the security risks associated with using unapproved cloud storage services when working with University data.

POLICY

The use of cloud services such as but not limited to Microsoft OneDrive, Google Drive, Apple iCloud, or Dropbox for university business requires a contract with the providing company that has been approved by System legal counsel. PASSHE maintains a list of approved cloud services at <https://secure.passhe.edu/af/ss/Pages/Software%20Agreements.aspx>.

The use of the cloud services must comply with applicable System and University policies. Edinboro University will only allow University data to be stored on cloud services where the approved service contract expressly guarantees the encryption of data in transit and at rest. No

University data can reside on any cloud service that does not provide strong encryption nor be able to be transmitted or received without strong encryption.

Requests for cloud services must be routed to Edinboro University's Chief IT Officer. If you use cloud services that are not approved, you are responsible for any and all implications that result and you will not be represented or indemnified by the University. Any decision to use cloud services for the storage of University data in the cloud should take into account the risks and liabilities related to its security, privacy, retention, access and compliance.

DEFINITIONS

Data Encryption: Conversion of data into code for confidentiality or security using an encryption algorithm.

Strong Encryption: An encryption method that uses a very large number as its cryptographic key. The larger the key, the longer it takes to unlawfully break the code. Today, 256 bits is considered strong encryption.

REFERENCES:

PASSHE-CITO-Cloud-Framework-11-12-2015 -

<https://secure.passhe.edu/af/ss/Documents/PASSHE-CITO-Cloud-Framework-11-12-2015.pdf>

Edinboro University Information Security and Data Classification Policy C056 -

[http://www.edinboro.edu/directory/offices-services/hr/policies/documents/Information Security and Data Classification Policy.pdf](http://www.edinboro.edu/directory/offices-services/hr/policies/documents/Information%20Security%20and%20Data%20Classification%20Policy.pdf)

CONTACT INFORMATION:

Vice President Finance and Administration

219 Meadville Street

Edinboro, PA 16444

814-732-2585