Policy IT008: Cloud Application Policy

Recommended for Approval by: Fawn L. Petrosky

Fawn Petrosky, Vice President for Finance

Approved by: Dale-Elizabeth Pehrsson

Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

This policy applies to all users including faculty, staff, students, contractors and guest users of Pennsylvania Western University (PennWest) accessing and using 3rd party services capable of sharing, processing, storing, or transmitting classified or sensitive data that is owned or leased by the University. This policy outlines best practices, licensing, and approval processes for using cloud computing services at PennWest.

B. Definition(s)

- **Cloud Computing** - At its simplest, cloud computing is a type of computing where both applications and infrastructure capabilities are provided to end users as a service through the Internet. Through cloud computing, entities no longer have to own their own computer hardware, infrastructure, platforms, or applications. By way of an example, software as a service (SaaS) application services are cloud computing services.
- **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. As computers become faster, the length of the key must be increased.

C. Policy

1. **<u>License Considerations</u>**

- **General Background Information** – PA State System Legal Information on "click-through" agreements

  Most new computer applications (even "free" ones available online), require a user to click a button that says "yes" or "I agree" before downloading or opening. These are known as "click-through" agreements and they are considered legal contracts. Commonwealth laws specify that only a very few designated employees have the

authority to enter into contracts on behalf of the university. If you are not one of the few with such authority and you click through an agreement, you are personally liable if a dispute arises. In other words, if you click-through an agreement without a University contract in place, you are responsible for any and all implications that result and you will not be represented or indemnified by the university.

- **Cloud License Agreements**

  The use of cloud services (Microsoft, Google, Apple, AWS, DropBox, etc.) for university business requires a contract that has been approved by System legal counsel. **The only approved cloud storage for both PennWest and PASSHE is Microsoft Teams/Sharepoint/OneDrive**. Requests for services not on the approved list should be routed to the Chief IT Officer at the university. If you use cloud services that are not approved, then you are responsible for any and all implications that result and you will not be represented or indemnified by the university.

  - Approved legal agreements must generally include terms on data security. See Information Security Policy for reference.
  - Through the collaboration of CITO and Strategic Sourcing, a web site will be created and maintained to document an itemized list of reviewed cloud agreements and the outcome of the review (approved, approved with restrictions, approved with acknowledged acceptance of risk, or rejected). An example of approved with restrictions may be the approach legal used with Apple Device Enrollment Program. Perhaps something along the lines of "Based on a review of this agreement, the risk associated with the use of the software is low". As such, it is permissible for the universities to participate in this program if they approve the acceptance of the risk and provide guidelines for the usage of the service in alignment with university information security policies.

2. **<u>Usage Considerations</u>**

- **Data**
  - The use of the cloud services must comply with applicable System and University policies, System information security and data classification policies or guidelines, federal and state laws and regulations, and recognized best industry practices. 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. Generally, cloud services may not be used to store or transmit "Restricted" information or "Sensitive" Data (as defined in the Information Security or Data Classification policy) unless the approved cloud service contract expressly guarantees the encryption of data in transit and at rest.
- **General Guidelines for Cloud Services**
  - The use of cloud computing resources and the data transmitted and stored with cloud resources is subject to the same policies, laws, regulations, and procedures that pertain to other electronic records at the university. This includes Right-To-Know, E-Discovery, and FERPA obligations. It also includes Intellectual Property, Copyright, and Export Control obligations. It is the responsibility of the employee using cloud services to ensure that all use is consistent with associated policies, procedures, laws and regulations.

- Any Restricted or Sensitive Data residing at or being transmitted to/from any vendor's cloud service must use strong encryption technologies. No Restricted or Sensitive data can reside on ANY cloud service that does not provide Strong Encryption, nor be able to be transmitted or received without Strong Encryption. University IT is required to make strong encryption the default storage and transmission mode for any use of any managed cloud services. Any cloud services that do not support Strong Encryption technology cannot be used for Restricted and/or Sensitive data.

- **Product Specific Guidelines**
  - For a given "approved" cloud service that does not fully comply with the security provisions of II.B.2 (strong encryption that can be configured by University IT in a managed cloud service) or any "approved with restrictions" cloud service, IT will develop a summary document to highlight specific guidance for the cloud service in question.

D. Procedure(s)

Not Applicable.

E. Related policies

Information Security Policy, Acceptable Use Policy, Data Classification Policy

F. Contact Information

Information Technology Services.

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.