POLICY 08:13:14
CLOUD COMPUTING

I. Purpose

The purpose of this policy is to outline appropriate practices and approval processes for using cloud computing services to support the processing, sharing, storage, and management of institutional data. Cloud computing services are application and infrastructure resources that users access via the Internet. These services, contractually provided by companies such as Apple, Google, Microsoft, and Amazon, provide the college computing services, platforms, and infrastructure to support a wide range of activities.

Cloud computing offers many advantages. However, without adequate controls, it also exposes individuals and organizations to threats such as data loss or theft, unauthorized access to networks, and more. This policy is to ensure that cloud services are not used without knowledge of Information Services. It is intended to establish a process whereby employees can use cloud services without jeopardizing college data and computing resources. This is necessary to protect the integrity and confidentiality of Pellissippi State Community College data and the security of the college network.

II. Scope

This policy applies to all employees in all departments of the college and pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.

This policy concerns cloud computing resources that provide services, platforms, and infrastructure that provide support for a wide range of activities involving the processing, exchange, storage, or management of institutional data. The policy does not cover the use of social media services. Personal accounts are excluded.

III. Definitions

Cloud Computing – The delivery of computing services over a proprietary network or the internet. Services include infrastructure services, development platforms and software applications.

Infrastructure-as-a-Service (IaaS) – Vendor provided computing resources such as servers (both physical and virtual), storage, networking components and other hardware such as firewalls or load balancers. The provider is responsible for the operating system and hardware while the customer is responsible for the application or software running on the service. *Examples*: RackSpace, Amazon, IBM, HP.

Institutional Data – Data elements created, received, maintained, recorded, or transmitted by or for the college for college business such as planning, managing, operating, controlling, or auditing college functions, operations, and mission. Institutional data formats include, but are not limited to, paper, electronic, audio, and visual. It does not include personal data, which is information created, collected, maintained, transmitted, or recorded by college owned devices, media, or systems in accordance with the Computer System Use that is personal in nature and not related to college business.

Platform-as-a-Service (PaaS) – Vendor provides an environment where the customer or developer can build and deliver web-based services over the Internet. *Examples*: Microsoft Azure, Google App Engine.

Software-as-a-Service (SaaS) – Vendor hosts software applications and the data for the customer. No part of the software resides on the user's computers. *Examples*: SalesForce, Google Apps, Office 365, Gmail, Hotmail, Yahoo.

IV. Policy

- The vice president of Information Services (or a designee) will certify any college provided cloud-computing vendor to ensure they adequately address security, privacy and all other IT management requirements.
- For any cloud services contracted by a department of the college that require users to agree to terms of service, such agreements must be reviewed and approved by the director of Networking and Technical Services or the vice president of Information Services and the vice president of Business and Finance.
- The use of such services must comply with the college's other related data system use policies, including, but not limited to, the following:

    - 08:13:01 Computer Usage
    - 08:13:02 Computer Account
    - 08:13:05 Computer System Use
    - 08:13:06 Bring Your Own Device (BYOD)
    - 08:13:08 Electronic Account Access
    - 08:13:09 Wireless Network
    - 08:13:12 Data Access Management
    - 08:13:13 Data Classification

    The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, financial data or any other data owned or collected by the college.

- Personal cloud services accounts may not be used for the storage, manipulation or exchange of college-related communications or college-owned data.
- Currently approved cloud services will be listed on the Information Technology Support website under Faculty and Staff Resources.
- Unauthorized use of cloud services may result in administrative, disciplinary, and/or legal actions.

IV. Cloud Use by Data Classification

When using an institution approved cloud service, use it only for institutional information classified as shown below. By default, all college data is classified as confidential unless the data owner classifies it at a different level. Pay special attention to access levels when sharing files and folders with other collaborators to ensure that data is not inappropriately shared. You may not use your personal cloud services account to collect, process, or store data covered by laws such as HIPAA, FERPA, FISMA, and GLBA. For more detail regarding data classification, refer to Policy 08:13:13 Data Classification

Confidentially Level	Description	Cloud Use
Restricted	Restricted Data is defined as data, in any format, that is *regulated* by law or contract. Regular audits of access to Restricted Data should be conducted by the data custodians and appropriate control measures are implemented by data custodians.	Can only use a college provided and provisioned cloud service once you have confirmed with Data Owner and IT staff that the service is appropriate for confidential institutional data. Not all cloud services are designed to handle regulated data. **This data MUST be encrypted when stored in a cloud service.**
Confidential	Confidential data is not protected by state or federal law. However, its loss or unauthorized use could impair the college functions, cause significant financial or reputational loss or possibly lead to legal liability.	Can only use a college provided and provisioned cloud service once you have confirmed with Data Owner and IT staff that the service is appropriate for confidential institutional data. Not all cloud services are designed to handle regulated data. **This data MUST be encrypted when stored in a cloud service.**
Public	Public data is any data that does not fall into the other classes. Public data does not pose a risk to the institution and may be publicly accessible but does not require public access. There are no restrictions on the storage or distribution of public data.	May use college provided cloud services to store or manage public institutional data. May use personal cloud services to store or manage public institutional data with caution. The user should always ensure that using these cloud services does not violate any licensing agreements.

Reviewed/Recommended: President's Council, November 20, 2017
Approved: President L. Anthony Wise, Jr., November 20, 2017