11:01:06:00 Cloud Computing

Purpose:

This policy outlines the best practices and approval processes for using cloud-based computing, storage, and software services to support the processing, sharing/transfer, storage, and management of DSCC institutional data.

Cloud computing services are application and infrastructure resources that users access via the Internet. These services, usually 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 a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online 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 prior notification and approval from the Office of the Vice President for Technology. It is intended to establish a process whereby employees can utilize cloud services without jeopardizing college data and computing resources. This is necessary to protect the integrity and confidentiality of Dyersburg State Community College data and the security of the college network.

Scope:

This policy applies to all employees in all departments at all locations of the college.

This policy pertains to all external cloud services, e.g. cloud-based email, document and file storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. This policy does not cover the use of social media services (such as Facebook, Twitter, Instagram, etc.). Personal accounts for cloud services (i.e., accounts created with personal e-mail addresses – not a dscc.edu account) should not be used to conduct college business and should not be used to transfer, store or distribute college data.

The Vice President for Technology (who is also the Chief Information Officer) is responsible for the development and maintenance of this policy.

Policy:

Selection and Use of Cloud Computing Services and Resources

• The Vice President for Technology (or a designee) will certify any cloud-computing vendor to ensure they adequately address security, privacy and all other IT management requirements. If an employee is not sure if a service or product is a cloud-based service, please contact the Office of the Vice President for Technology and a determination will be made.
• 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 Vice President for Technology. Additionally, agreements requiring signatures must be routed through the DSCC contract approval process and signed by the President.
• The use of such services must comply with the college's other related data system use policies, including, but not limited to, the following:
◦ 11:01:01:00 – Information Technology Policy
◦ 11:01:02:00 – Information Security
◦ 11:01:05:00 – Cyber Incident Reporting and Response Policy
◦ 11:02:03:00 – Monitoring and Filtering Internet Use
◦ 11:02:04:00 – Computing, Network and Communications Acceptable Use
◦ 11:02:05:00 – Administrative Software Usage
◦ 11:04:05:00 – Password Management Policy
• 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 MyDSCC portal, Employee tab, Employee Quick Clicks, Computer Services and Telecommunications page.

Cloud Services Usage 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.

Confidentiality Level	Description	Cloud Use

Confidentiality Level	Description	Cloud Use
Regulated Institutional Data	All Institutional data that is governed by privacy or information protection mandates required by law, regulation, contract, binding agreement, or industry requirements.	Cannot use self-provisioned cloud services to store, process, share, or otherwise manage regulated institutional data without working with the DSCC Contract Officer or TBR Contract Officer to develop the appropriate contractual safeguards. Can only use a contractually (locally or centrally) provisioned cloud service once you have confirmed with your Data Owner and the CIO that the service is appropriate for regulated institutional data. Not all centrally and locally provisioned services are designed to handle regulated data.
Confidential Institutional Data	Institutional data that is meant for a very limited distribution —available only to members of the Dyersburg State community on a strictly need-to-know basis.	Should not use self-provisioned cloud services to store, process, share, or otherwise manage confidential institutional data without ensuring that a service's safeguards are appropriate for confidential institutional data. Should only use a centrally or locally provisioned cloud service once you have confirmed with your manager and the CIO that the service is appropriate for confidential institutional data. Not all contractually provisioned services are designed to handle confidential institutional data.

Confidentiality Level	Description	Cloud Use
Administrative Institutional Data	Institutional data that is meant for a limited distribution; available only to members of the Dyersburg State community that need the institutional data to support their work. This institutional data derives its value for Dyersburg State, in part, from not being publically disclosed.	Should not use self-provisioned cloud services to store, process, share, or otherwise manage administrative institutional data without ensuring that a service's safeguards are appropriate for administrative institutional data. Should only use a centrally or locally provisioned cloud service once you have confirmed with your Information Steward that the service is appropriate for administrative institutional data. Not all contractually provisioned services are designed to handle administrative institutional data.
Public Institutional Data	Institutional data that is meant for members of the Dyersburg State community and in some cases wide and open distribution to the public at large. This institutional data does not contain any confidential information.	May use self-provisioned cloud services to store or manage public institutional data with caution. User should ensure that using these cloud services does not violate any licensing agreements. May use contractually provisioned cloud services to store or manage public institutional data.

Compliance:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or suspension.

Definitions:

Cloud Computing – The delivery of computing services over a proprietary network or the Internet. Services include infrastructure services, development platforms and software applications.
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/or 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 that is personal in nature and not related to college business.)

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.

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, Yahoo.

Revision History:

Policy written 06/07/18 by Vice President for Technology.
Policy approved by Administrative Council on 06/14/2018
