Policy Title:	Cloud Computing Policy
Category:	Information Security
Effective Date:	December 15, 2017
This Administrative Policy Applies to:	Suffolk County Community College
Responsible Office:	Information Technology
Approved by:	President's Cabinet

SUMMARY

This Cloud Computing Policy establishes a process to ensure that protected private or sensitive information owned by or in the possession of Suffolk County Community College (the College) is not inappropriately stored or shared using cloud computing technologies, as well as to ensure the effective and secure use of approved cloud computing technologies throughout the College.

For purposes of this Policy, the definition of cloud computing corresponds to the National Institute of Standards and Technology (NIST) definition found in NIST Special Publication 800-145, but in summary, cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or personal computer.

All College employees and others who have access to the College’s Information Technology resources are bound to follow this policy. All departments must demonstrate compliance with the requirements of this policy, including documentation as part of their normal and periodic assessments.

SCOPE

This policy is applicable to all employees, contractors, vendors or others who have access to Information Technology resources owned or operated by the College. Any information not specifically identified as the property of other parties, that is transmitted or stored on the College's resources, is the property of the College.

This policy is only one piece of the College’s program for information security; individuals should review the College’s other Information Technology Policies, which are available at: https://www.sunysuffolk.edu/legalaffairs/policies.jsp#tab-d12e3-2.

REASON FOR POLICY

This policy endorses the **approved** use of cloud computing technologies that comply with recognized information security best practices and sufficiently address other information security considerations associated with cloud computing which are relevant to the College. While cloud computing can facilitate collaboration and the sharing of information, it exposes the College to additional risk.

It is incumbent upon the College and its employees to understand the risks of cloud computing technologies before approving their use with respect to information owned by or in the possession of the College. Cloud computing technologies can present the following information security and data privacy concerns:

- Loss of control over the College's data or information;
- Loss of security or privacy of, or unauthorized access to, College data or information;
- Loss or theft of College data or information;
- Compliance with FERPA and other laws or regulations governing data confidentiality and privacy;
- Use of the College's data or information by a third party; and
- Reliance or dependency on the cloud computing service.

Through this policy, the College is implementing guidelines for the types of data and security measures that are appropriate for the use of cloud computing technologies at the College, as well as establishing the role of the Chief Information Officer (CIO) and the College General Counsel in any decision-making process associated with the use of cloud computing by any of the College's departments or offices.

POLICY

The following constitutes the College's cloud computing policy for College employees and all others accessing the College's Information Technology (IT) resources, data, and information.

College enterprise systems, where a College user identification and password is required, are approved for storage of College information and data, consistent with the College's IT Policies and best practice. The College's Data Classification Standards classify and describe the data maintained by the College. The College General Counsel will determine the type(s) of data (if any) that can be stored, manipulated, or exchanged on a cloud computing service and, in consultation with the CIO, any conditions or restrictions on the use of a cloud computing service for the type of data. However, Category I Regulated Private Data, may never be stored or shared on a cloud computing service unless specifically evaluated and approved by the College General Counsel, CIO, and the College President. Category I Regulated Private Data includes social security numbers, driver's license numbers, State-issued non-driver ID numbers, bank/financial account numbers, credit/debit card numbers, passport numbers, electronic protected health information, and trade secrets.

The CIO must be included in any cloud computing services decision-making process. Authorization from the CIO is required prior to the establishment or use of any cloud computing service or cloud computing service contracts for the storage, manipulation, or exchange of College communications or data.

Personal cloud computing service accounts **may not** be used for the storage, manipulation or exchange of College-related communications or information owned by or in the possession of the College, except as specifically authorized by the College General Counsel and the CIO.

Contracts for Cloud Computing Services

Any use of cloud computing services for work-related purposes must be formally authorized in advance by the CIO or his/her designee, with a written contract, approved by the College General Counsel or his/her designee, specifying particular terms for the protection of the College's data.

For any cloud computing services that require users to agree to Terms of Service or End User License Agreements, such agreements must be reviewed and approved in advance by the CIO and/or College General Counsel, or designee.

The CIO or designee must certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor. Contracts should address:

- Data transmission and encryption requirements;
- Authentication procedures;
- Security and access controls, including intrusion/breach detection and prevention procedures;
- Security, virus, malware, etc. scanning requirements;
- Compliance with College policies and applicable law/regulation;
- Data ownership, retention, and recovery; and
- The vendor's use of any data stored in the cloud.
- Clear delineation of responsibility and liability in the event of a security breach

Compliance with Legal, Regulatory, and Policy Requirements

The use of a cloud computing service must comply with the College's existing Information Technology Policies. The use of such services must also comply with all laws and regulations governing the handling of personally identifiable information (PII), corporate financial data, or any other data owned or collected by the College, as identified in the College's Data Classification Standards.

Approved Cloud Computing Services

The Office of Information Technology Services will maintain a listing of all approved cloud computing services which outlines the extent to which the cloud computing service has been approved for use at the College, including:

- Which types of data may be stored or exchanged through the particular cloud computing service; and
- Which department(s), office(s), or individual(s) have been approved to use the cloud computing service.

The Office of Information Technology Services will also maintain a listing of any cloud computing services that have specifically been disapproved for use, in order to avoid duplicative requests for review.

RESPONSIBLE OFFICE CONTACT INFORMATION

Office of Information Technology Services, Suffolk County Community College

For questions or comments, submit all inquiries and requests for future enhancements to the Chief Information Officer for Suffolk County Community College. Attention:

Vice President of Information Technology / Chief Information Officer
Suffolk County Community College
533 College Road
Selden NY 11784

Questions may also be directed to the College's IT Helpdesk at (631) 451-4357

RELATED POLICIES & PROCEDURES

- SUNY Procedure, Information Security Guidelines, Procedure Document 6608
- Suffolk County Community College Policy on Information Security Access
- Suffolk County Community College Policy Statement on Privacy and Confidentiality
- Suffolk County Community College Management Standard of Protected College Information in Transit and Storage

OTHER RELATED INFORMATION

The following are references to related State and Federal policies and standards on cyber security.

- New York State Information Security Policy, NYS-P03-002 (March 2017)
- United States Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 800-145 “The NIST Definition of Cloud Computing” (Sept. 2011).

Authority

Policy recommended by Suffolk's Information Security subcommittee, and approved by the President's Cabinet in accordance with Suffolk Policy protocols on December 15, 2017.
