College Manual of Policies and Procedures

Title: **Bring Your Own Device (BYOD) and Mobile Device Policy**	Date: 08/21/2013	Number:	200.102
Section: General Administration/Computer	Maintained by: Technology Advisory Group (TAG)	Created: Reviewed by TAG: Last Revised: Effective:	04/20/2013 04/24/2013 08/12/2013 02/01/2014

Bring Your Own Device (BYOD) and Mobile Device Policy
for use of Personal Mobile Computing/Storage Devices
to Store or Access the College's Confidential Information (CI)

Policy
Any mobile computing/storage device used to access and/or store Confidential Information (CI) is subject to all College information security policies. In addition, when accessing and storing the College's CI with Personal Mobile Computing /Storage devices, users agree to and will abide by the current **"Procedures and Implementation Information for Bring Your Own Device (BYOD) and Mobile Devices,"** found published on the Cayuga Campus Technology website at: https://www.cayuga-cc.edu/it/policies-procedures-guidelines/

Introduction
Tablets, eReaders, smartphones, laptops, and other mobile computing, storage, and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect the physical devices, the information they contain, and the users utilizing the devices. With the increasing use of these devices, it is necessary to establish a policy governing their use when storing or accessing the College's CI.

An effective best practice to secure CI is to **not to store it on mobile devices**. As a matter of policy and best practice, CI should always be secured by storing CI only on College servers and using secure communication technologies when accessing CI remotely (e.g. VPN, HTTPS, CCC-secure, etc.).

College business requirements may, on occasion, justify storing CI on mobile computing/storage devices. In these cases, it is the responsibility of the user to recognize that CI stored on these devices is at increased risk for theft, loss, breach, and inadvertent exposure. Users are required to ensure that they are in compliance with all aspects of this policy to keep the data secure.

Purpose
This policy is necessary to protect the confidentiality, availability, and integrity of CI while stored, transmitted, or processed on mobile devices. The intent of the policy is to protect the College's CI by applying rules and configuration standards for personal mobile computing/storage devices that access or store any of the College's CI.

Scope
This policy applies to any mobile computing/storage device that is used to store or access CI irrespective of who owns the device. This policy will not supersede other existing policies developed by College, but may introduce more stringent requirements than current policies dictate.