Information Security Summary Policy

Summary

The realization of Columbus State University's (CSU) core mission and goals depends a great deal on the use of technology. CSU's information assets such as networks, hardware, software, applications, and the information itself are all vital to the delivery of technology on campus. Protection of these assets from a variety of threats such as natural disaster, system failure, employee error, or malicious action is critical. Upholding the confidentiality, integrity, and availability of information and the resources used to process or store that information is paramount to computing at CSU.

Purpose

This summary policy and associated detailed policies intend to provide a comprehensive set of security guidelines that will ensure the appropriate and consistent protection of the University's information assets.

Policy

- CSU must protect its information assets from anything except authorized and intended use
- CSU must ensure the availability of the information assets that support its mission and goals
- CSU must operate in accordance with all applicable federal, state, and local laws

The entire University community (students, faculty, and staff) are responsible for protecting CSU's information assets and for using its resources in an effective, efficient, ethical, and lawful manner.

The individual policies and procedures address key areas of information security and, when combined, provide for an extensive framework that supports the open use of technology while also protecting CSU's critical information assets. Every person handling information or using University information systems must adhere to information security policies and procedures.

Related USG Policy

11.3 Information Security Policy

Last Update

4/16/2014

Responsible Authority

Chief Information Security Officer