Columbus State University
Continuity of Operations
Planning (COOP) Policy

Revised 6/25/2018

1.0 **Background**
Continuity of Operations Planning (COOP), ensures the continuity of critical business and essential functions through a wide range of emergencies and disasters including localized acts of nature, accidents and technological or attack-related emergencies. The COOP is an effort to ensure that at minimum, the organization's support systems continue to operate and be available.

2.0 Purpose
The purpose of this policy is to establish a standard for recovery strategies that must be developed for information technology (IT) systems. This includes network connectivity, servers, data and support systems. Priorities for IT recovery must be consistent with the priorities for recovery of network connectivity and other critical processes that were developed during the operational business impact analysis (BIA).

3.0 Policy
The (COOP) shall be developed following existing standards, industry best practices, Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) guidelines, and the University Systems of Georgia (USG) Cybersecurity tools, and templates.

The (COOP) will require the involvement of all related critical CSU system business units, University Information Technology Services (UITS), and the Office of Information Security to ensure an effective organizational response to contingencies and disasters.

The (COOP) must incorporate the physical and logistical limitations of the organization, related critical systems, and resources.

4.0 Procedures

Create, implement, maintain and test the (COOP) that will allow appropriate response to a wide range of contingencies and disasters that may occur.

Describe the actions to be taken before, during and after events that disrupt critical CSU information system operations.

The Office of Information Security (InfoSec) will lead and collaborate with all CSU departments in performing and documenting (COOP) test plans. All plans must be tested at least once every 12 months and evidence of testing must be available upon request, and part of the continuity of operations plan (COOP) documentation.

The formal (COOP) processes must at minimum include:

- The backup and recovery processes, and plan for critical support systems.
- A cyber incident response process and plan.
- An Information System Contingency Plan (ISCP), Disaster Recovery Plan (DRP), or Business Continuity Plan (BCP) whichever is applicable for critical general support systems.

Related USG Policy
USG IT Handbook - Section 3.3 Continuity of Operations Planning