

Title:	DRAFT USG Continuity of Operation Plan Policy		
Policy Number:	2009-Julian Date	Topical Area:	Security
Document Type:	Standard	Pages: Words: Lines:	5 1,387 182
Issue Date:	May-09	Effective Date:	Immediately
POC for Changes:	USG Office of Information Security (OIS)		
Synopsis:	Requires the University System Office (USO), USG Institutions and the GPLS to formally develop a backup and recovery plan, incident response and reporting policy, and a disaster recovery plan		

Purpose

Continuity of Operations Planning (COOP) and Continuity of Government (COG) ensure the continuity of essential functions through a wide range of emergencies and disasters. Today's changing threat environment and recent natural and man-made emergencies demonstrate the need for COOP/COG capabilities and plans at the University System Office (USO), the University System of Georgia (USG) Institutions and the Georgia Public Library Services (GPLS).

This policy requires the University System of Georgia System Office, each USG Institution and the Georgia Public Library Service to establish a plan to develop and maintain a Continuity of Operations Plan (C.O.O.P.) Program.

The program plan must include a backup and recovery plan for critical data/system, a computer security incident response (IR) and reporting plan, a disaster recovery (DR) plan and a business continuity (BC) plan for all critical data and information systems supporting the University System Office, USG Institution, and Georgia Public Library Service mission and operations activities. The program shall create plans for contingency and disaster response. These plans will be tested periodically to ensure they reflect current operating conditions and address current threats.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

BOR Policy Manual, Section 700
 USG Office of Information Security Program Policy
 USG Information Strategic Security Plan
 USG Information Security Program Reporting Policy

Guiding Principles

- The USG Continuity of Operations Plan Policy shall be developed following existing Standards, industry best practices and NIST guidelines.
- The USG Continuity of Operations Plan Policy will require the involvement of all USG institutions, USG System Office and the Georgia Public Library Service to ensure an effective System response to contingencies and disasters.
- The USG Continuity of Operations Plan Policy must incorporate the physical and logistical limitations of the USG operating locations.
- The USG Continuity of Operations Plan Policy will be aligned with the USG Emergency Operations Plan.

Policy

This policy shall establish a requirement to develop a formal program to develop, maintain, and evaluate plans to appropriately respond to a wide range of contingencies and disasters that may occur at all of the USG institutions, System Office and Georgia Public Library Service. The plans shall describe the actions to be taken before, during and after events that disrupt critical information system operations.

Backup / Recovery & Offsite Storage of Critical Data and Systems

Backup and retention schedules and procedures are critical to the recovery of an institution, the USO and GPLS' systems, applications and data. The detailed procedures for such a recovery should include hardware, software (including version), data file back up and retention schedules, off-site storage details, and appropriate contact and authority designation for personnel to retrieve media.

Offsite Storage Of Backup Material

Where possible, backup media will be stored at a suitable off-site location. For locations where off-site storage is not practicable or cost effective, C.O.O.P. leadership will designate an appropriate facility to serve as the off-site storage of backup media. A suitable facility is one within reasonable distance of the main campus or facility, but not likely to be immediately threatened by the contingency or disaster.

Incident Management

The University System of Georgia System Office, USG Institutions and the Georgia Public Library Service will establish a Computer Security Incident Response capability program to respond to and manage adverse activities or actions that threaten the successful conduct of teaching, instruction, research

and operations in the USG. The computer security incident response plan will follow existing USG policies, standards, industry best practices, ISO and NIST guidelines.

The University System of Georgia System Office, USG Institution and GPLS management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All institutions, the USO and GPLS are required to report information security incidents consistent with the security reporting requirements in this policy.

Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

Disaster Recovery Management

Each institution, the USO and GPLS must establish a Continuity of Operations Plan Program that provides processes supported by executive management and resources to ensure the appropriate steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the institution, the USO and GPLS have the ability to continue its essential functions during a business disruption or major catastrophic event. The program controls ensure that information is protected by providing for regular backup of automated files and databases, identifies and reduces risks, limits the consequences of the incident, and ensures the availability of information assets for continued business.

Disaster Recovery Planning

Disaster recovery planning (also known as business continuity planning) provides for continuity of computing operations in support of critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly migration toward the resumption of all computing services within an institution, the USO and GPLS following a business disruption. It is essential that critical IT services and critical applications be restored as soon as possible.

It is significant to recognize that no disaster recovery program is ever complete. All disaster recovery planning is based upon available knowledge and assumptions, and must be adapted to changing circumstances and business

needs, as appropriate. Strategies, procedures, and resources must be adapted as often as necessary in order to recover critical applications. Recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

The disaster recovery planning process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. Institutions, the USO and GPLS should consider the results of their risk analysis process and their business impact analysis when developing their Disaster Recovery Plan (DRP). Each institution, the USO and GPLS processes should culminate in a viable, fully documented, and tested DRP.

To provide for recoverability of new systems, all institutions, the USO and GPLS must include disaster recovery considerations and costs in project authority documents and budget proposals.

To improve the likelihood for the full recovery of key business processes, DRPs should be developed as part of a complete business continuity (BC) program, which includes emergency response and business resumption plans.

Institution, USO and GPLS Disaster Recovery Plan

Each USG institution, the University System of Georgia System Office and GPLS must maintain an Disaster Recovery Plan (DRP) identifying the computer applications that are critical to institution, the USO and GPLS operations, the information assets that are necessary for those applications, and the institution, the USO and GPLS' plans for resuming operations following an unplanned disruption of those applications.

Each institution, the USO and GPLS must keep its DRP up-to-date and provide an annual status document to the USG Office of Information Security. The annual requirements are:

- Each institution, the USO and GPLS must file a copy of its DRP Executive Summary
- Each institution, the USO and GPLS DRP must cover, at a minimum, ten topic areas, which are listed and described in the *Disaster Recovery Plan Documentation for Institutions*.

It is important to adapt the detailed content of each plan section to suit the needs of the individual institution, or USO or GPLS, with the understanding that DRPs are based upon available information so they can be adjusted to changing circumstances.

Applicability and Compliance

This policy applies to all USG information resources, systems, and technology

and to all users of these resources, systems and technology within the USG operating umbrella or connected to the USG information infrastructure. Compliance with this policy is mandatory.