	Georgia Technology Authority	
Title:	**Contingency Planning**	
PSG Number:	**SS-08-045**	
Effective Date:	**03/31/2008**	**Review Date: 12/01/2024**
Synopsis:	Establishes the requirements for agencies to have a plan to sustain or recover critical operations in the event of a system disruption or disaster	

PURPOSE

A computer security event has the potential to disrupt computer operations thereby disrupting critical mission and business functions. The need to maintain security and other regulatory requirements does not go away when an organization is processing in contingency mode. Contingency planning directly supports an organization's goal of continued operations while maintaining the necessary protection levels.

Contingency planning allows an organization to plan and develop interim measures necessary to recover, restore or maintain critical business and IT operations following or during an emergency or system disruption. Business and IT operations are vulnerable to three classifications of threats:

> **Natural**—e.g., hurricane, tornado, flood, and fire
> **Human**—e.g., operator error, sabotage, implant of malicious code, and terrorist attacks
> **Environmental**—e.g., equipment failure, software error, telecommunications network outage, and electric power failure

This standard outlines the requirements for developing and implementing a plan for continuing or recovering critical operations during and/or after an emergency or disruption.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(9) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

TERMS and DEFINITIONS

Business Continuity Coordinator (or Contingency Planning Coordinator) - The specific employee or position assigned responsibility for preparing and coordinating the business continuity process. This individual should typically be from a business organization in the agency, not from the IT organization.

Business Impact Analysis (BIA) - A process designed to identify critical business functions, assess the potential quantitative (financial) and qualitative (non-financial) impacts of an incident, and prioritize and establish recovery time objectives.

Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disasters. (Below are other terms often used interchangeably but are a suite of plans intended to prepare for and execute contingency efforts)

- **IT Contingency Planning** refers to the dynamic development of a coordinated recovery strategy for IT systems (major application or general support system), operations, and data after a disruption.
- **Business Continuity Plan (BCP)**: The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.
- **Disaster Recovery Plan (DRP)**: A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Continuity of Operations Plan (COOP): A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

STANDARD

Agencies shall identify the potential risks that may adversely impact their critical business functions and develop continuity and recovery strategies and plans designed to ensure the availability of the agencies' essential functions, services and communications in the event of a natural, man-made, or environmental emergency or disruption.

Agency heads shall create and implement a management structure for business continuity within the agency to include a named Business Continuity Coordinator and for directing the development and execution of a viable disaster recovery and business continuity program.

The Business Continuity Coordinator shall:

- Coordinate with internal and external points of contact (POC) associated with the critical business functions to conduct a Business Impact Analysis (BIA).

    - The BIA shall provide information that:
        - Identifies critical business functions, services, and interdependencies
        - Links critical services and functions to support resources (technology, staff and facilities)
        - Characterizes the system requirements, processes, and interdependencies
        - Identifies disruption impacts including financial and non-financial losses
        - Estimates allowable outage times
        - Determines contingency requirements and priorities
        - Identifies continuity and recovery strategies (backups, alternate sites, manual etc)
        - Estimates implementation costs
- Oversee the development, implementation, exercise and maintenance of contingency plans.
    - The contingency/recovery plans shall:
        - Have executive management support and sign-off
        - Ensure continued or restored lines of leadership, public safety, critical business/IT functions, and essential constituent service within a reasonable period of time
        - Identify key personnel, roles and responsibilities
        - Identify reporting and management structure
        - Identify preventive controls
        - Avert or minimize the impacts of financial, legal or regulatory exposure
        - Provide detailed recovery execution strategies, processes and procedures.
        - For the most critical applications/processes, be exercised and reported annually to confirm the accuracy and the overall readiness of the plan.
        - Be maintained in a ready state that accurately reflects current system requirements, procedures, organizational structure, and policies.
- Be the agency’s central point of contact for plan activation and ensure that key personnel are aware of their roles and responsibilities and can execute the plan.
- Conduct periodic training and awareness programs

Business Continuity and Disaster Recovery plans shall be maintained in the state’s chosen repository as defined in the enterprise office productivity suite standard.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Business Continuity and Disaster Recovery (PS-08-025)
Disaster Recovery - System Backups (SS-08-046)

REFERENCES

NIST SP 800-12 Introduction to Computer Security NIST Handbook
NIST SP 800-34 Contingency Planning Guide
NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities