

# 9400-P200: Information Security Planning

## I. PURPOSE

This policy sets requirements for the inclusion of information security into the agency's business continuity plans related to information technology (IT) resources. As a matter of good practice, agencies develop business continuity plans that include disaster recovery to sustain critical functions in the event of a disaster and to resume full operations as soon as possible.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as "agencies").

## III. POLICY

- A. Agencies shall develop, test, review, and maintain coordinated plans for business continuity and recovery. Agency heads shall ensure that provisions for information security are included in their contingency/recovery plans.
- B. Exercises or tests shall be conducted and all information security concerns identified to update and /or retest the plans as appropriate.
- C. Agency heads shall ensure that IT requirements for the recovery of their agency assigned to the Information Technology Division (ITD) for fulfillment are coordinated with ITD.
- D. Agencies shall conduct a risk assessment of events that can cause interruptions and mitigate risks based on the potential impacts to the business of the agency.
- E. The Data Stewards shall review the business continuity plans and make recommendations for additional technical and/or non-technical security controls in areas that may present unacceptable risks in terms of confidentiality, integrity, and/or availability.
- F. As applicable, Information Resource Owners or their designees shall review the contractual requirements for outsourced recovery facilities to ensure that all levels of security services are defined and ensure that information security controls are equal to or greater than the security controls afforded to the information by the agency.
- G. As applicable, Information Resource Owners or their designees shall evaluate outsourced backup service providers on their ability to fulfill their contracted levels of service and provide information security controls equal to or greater than the security controls afforded to the information by the agency.

**CIO Approved Date: 02/01/2010**