

# 3100-P160 – Communications and Operations Management

## I. PURPOSE

This policy establishes information security requirements for communications and operations management.

## II. SCOPE

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

## III. POLICY

A. Operating procedures shall be documented, verified, and approved.

1. Procedures shall be documented to address information security in operational activities such as but not limited to:
  - Processing and handling information.
  - Procedures for handling unexpected outages or technical difficulties (to include contact lists).
  - Restart and recovery procedures.
2. Procedures shall be verified to ensure they implement the desired Policy or Standard then approved by the responsible agency official.
3. Procedures used to implement Agency Information Security Policies shall be formally approved, per Policy 10100-P110, Security Policies, Standards, and Procedures. Changes to procedures shall be similarly verified and approved.

B. Segregation of duties.

1. When job functions or duties exist where there is a possibility of collusion or the likelihood that a conflict of interest exists (real or perceived), agencies shall, to the extent possible, separate those functions or duties.
2. Security administration and security reviews should be performed by different persons such as compliance reviews and audits per Policy 9400-P211, Policy and Technical Compliance.
3. Administrators of multi-user systems shall use multiple UserIDs that correspond to their day-to-day and administrator roles. Security-relevant activities attributed to the use of either UserID shall be logged.

## **3100-P160 – Communications and Operations Management**

### **C. Separation of environments.**

1. Systems used for development and testing shall be physically and/or logically segregated from systems used for production. See also Policy 9400-P180, Information Security in the System Lifecycle
2. Media used for development and test activities shall be clearly labeled as such and shall not be used on production systems unless all test data has been removed.
3. Production data shall not be used for development and testing unless test data will not allow testers to validate proper function. If production data is used in a test environment, it shall be protected as if it is still production data.
4. If production information must be used for testing, a copy of the data shall be made so that the live data will not be altered.
5. If production data is used, the physical or electronic output of tests using that data shall be strictly controlled and promptly destroyed when no longer needed.

### **D. Change Management for Information Security Controls.**

1. Other than typical day-to-day maintenance activities, such as maintaining user accounts and access permissions, all systems, networks, or applications used for processing, storage, and/or communications shall be included into a change management process to ensure that only authorized changes are made.
2. Change management procedures shall be used for all changes to software, hardware, and communications links, and shall define a controlled process for testing and promotion to the production environment.
3. The organizational head or designee shall have the authority to stop a development process if there are unresolved security concerns.
4. Changes shall be tested prior to going into production.

### **E. An incident management procedure shall be in place.**

1. See Policy 9400-P190, Reporting Security Events and Vulnerabilities.

**CIO Approved Date: 1/5/2011**