

## **SECURITY COMPLIANCE EVALUATIONS PROCEDURE**

The Department Information Security Officer (DISO) is responsible for evaluating the security safeguards of all Department of Mental Health (DMH) information systems to ensure compliance with the DMH Privacy and Security Compliance Program Policy.

### **I. Periodic Evaluation by the DISO**

- a. The DISO or designee must prepare a written evaluation DMH's security Safeguards, including a review of the viability of DMH's Privacy and Security Compliance Program Policy.
- b. The DISO's approval is required before any change developed and recommended is made to any security policy or security procedure.

### **II. Evaluation Upon Occurrence of Certain Events**

- a. If one or more of the following events occur, the policy evaluation process described in Section I, must be immediately implemented:
  1. Changes in any of the regulatory, compliance, and/or accreditation security regulations or privacy regulations.
  2. New Federal, State, or local laws or regulations affecting the privacy or security of confidential and/or sensitive information.
  3. Changes in technology, environmental processes, or business processes that may affect DMH's Privacy and Security Compliance Program Policy.
  4. The occurrence of a serious security violation, breach, or other security incident after which the analysis conducted under DMH Policy No. 552.01, Security Incident Report and Response Policy, indicates that policies and/or procedures need to be added or modified.
  5. Changes in any County or DMH policies and/or procedures that may affect the DMH Privacy and Security Compliance Program Policy.

### **III. Evaluation of Facility Procedures by DMH Facilities**

Periodically, the DMH CIO or his/her designee must evaluate the security aspects of the DMH Privacy and Security Compliance Program Policy, as applicable to the Department, the Department's own security policies and procedures, and the implementation, operation, and maintenance of such policies and procedures. The purpose of such internal evaluation is to determine DMH's compliance status and make any changes necessary in order to become compliant, and/or to demonstrate and document compliance with the DMH Privacy and Security Compliance Program Policy and DMH's own security policies and procedures.

#### **IV. Internal Audit of Security Policies and Procedures**

All security-based policies and procedures, including the implementation, operation, and maintenance of such policies and procedures, are subject to periodic audits by DMH's internal Audit Department and/or DISO or his/her designee.