

## **DMH FACILITY INFORMATION TECHNOLOGY CONTINGENCY PLAN PROCEDURES**

All of the following procedures will be performed by individuals in the Department of Mental Health Chief Information Office Bureau under the direction and review of the Department of Mental Health Chief Information Officer (DMH CIO) and Departmental Information Security Officer (0150).

The Department of Mental Health (DMH) Director or his/her designee is responsible for approving prioritization of the critical information systems to ensure the ranking accurately reflects the relative criticality of the Department's business functions.

The DMH CIO or his/her designee must ensure that a Contingency Plan containing the components in Sections I through VI below is created, implemented, tested, and updated for each DMH facility. The DMH Facility Information Technology (IT) Contingency Plans, including the components identified below, must be provided to the DISO for review and approval to ensure that the minimum IT Contingency Plan requirements are met.

The IT Contingency Plan consists of the following seven components:

### **I. Applications and Data Criticality Analysis (Attachment II)**

The Application and Data Criticality Analysis must identify IT Contingency Plan priorities based on the criticality and sensitivity of the applications and data within the facility. The Applications and Data Criticality Analysis must include:

- a. Identification of the assets (e.g., hardware, software, and applications) utilized by the facility that receive, manipulate, store and/or transmit confidential and/or sensitive information, as well as information necessary to ongoing business operations.
- b. Prioritization of applications and data based on the Criticality Score and Sensitivity Score found in the Facility Master Security Management Report (Risk Management Procedure).

### **II. Data Backup Plan (Attachment III)**

The Data Backup Plan must ensure that exact copies of critical data are retrievable. The Data Backup Plan must include the following steps:

- a. Identify the backup methods (e.g., full, incremental, or differential backup) and materials (e.g., CD-ROM, magnetic tape, or floppy disks) to be used, and the frequency of performing backups based on the criticality analysis.
- b. Assign a responsible person(s) to manually back up the data sets as determined, or to configure the backups to be done automatically by available tools. The backups will be inspected and tested to ensure that their contents are exact copies of the data archived, and that they are restorable.
- c. Assign responsible person(s) to catalog, store, and secure the backups in a suitable container and location for such purpose.
- d. Monitor and track storage and removal of backups; ensure all applicable access controls are enforced.

- e. Track the archive requirements for each backed-up data set; ensure they are maintained for the appropriate time period.
- f. Test the Data Backup plan as set forth in Attachment VII, Testing and Revision of Contingency Plan.

### **III. Disaster Recovery Plan (Attachment IV)**

The Disaster Recovery Plan must enable the restoration of lost data in the event of fire, vandalism, systems failure, or other disaster. The Disaster Recovery Plan must include the following steps:

- a. Assign and provide access rights to an authorized person(s) for the retrieval, loading, and testing of data backups
- b. Retrieval of the latest copy of the facilities' backed-up data from the secure location in the event of data loss. If the necessary data set(s) have not been archived, efforts will be made through formal channels (e.g., retransmission from original sources) to collect the data.
- c. Load the retrieved data in the order of predetermined criticality (especially with regard to the availability attribute), to appropriate components (in accordance with applicable access control policies), and test to ensure the data restoration was successful.
- d. Test the Disaster Recovery plan as set forth in Attachment VII.

### **IV. Emergency Mode Operation Plan (Attachment V)**

The Emergency Mode Operation plan must enable the facility to continue its operations and business processes in the event of fire, vandalism, systems failure, or other disaster, and safeguards the security of data. The Emergency Mode Operation Plan must be based on the criticality analysis for each IT Information System and must include the following steps:

- a. Identify the scope including the severity of the emergency (e.g., system only, facility-wide, DMH-wide) and the duration of the emergency (e.g., until repair, day, week, month, undetermined).
- b. Identify type of recovery (e.g., hot site, warm site, cold site, disk mirroring) that is required by the scope of the emergency.
- c. Identify emergency continuity personnel, including either backup personnel or personnel cross-trained to assure adequate staffing in the event of an emergency.
- d. Designate specific roles and responsibilities to initiate and maintain emergency mode operations, including information system and security personnel.
- e. Implement the following emergency access control requirements:
  - 1. Determine emergency access control requirements for emergency mode operations and ensure that the access control matrices reflect such requirements.

2. Give users additional privileges in the event of a crisis situation to access information as needed and in accordance with the above emergency mode operation procedures.
- f. Test the emergency mode operation procedures as set forth in Attachment VII, Testing and Revision of Contingency Plan.

**V. Command and Control Plan (Attachment VI)**

The Command and Control Plan must establish IT administrative procedures to follow in the event that an emergency occurs.

- a. The DMH CIO or his/her designee must integrate the DMH Facility IT Contingency Plan with existing DMH Facility Contingency Plan to establish command and control in order to support emergency management team members who can facilitate the flow of information as necessary to users.
- b. Develop a telephone call tree to disseminate important information within DMH and/or the DMH facility, as necessary.
- c. Each DMH facility must have in place a notification process to notify the appropriate persons within DMH and the DMH facility in the event any part of the IT Contingency Plan is executed.

**VI. Testing and Revision of Contingency Plan (Attachment VII)**

The Contingency Plan must be tested periodically in order to assure the workability of the Plan in the event of a disaster and/or emergency. If testing establishes the need for changes in existing IT Contingency Plan procedures, then those procedures must be revised.

- a. Conduct one or more of the following exercises to test the Contingency Plan (including Data Backup, Disaster Recovery, and Emergency Mode Operation Plans):
  1. Tabletop exercise of response to specific scenarios
  2. Technical restoration activities
  3. Supplier and/or services tests
  4. Complete drills of the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.
- b. Revise the Contingency Plan to address any deficiencies discovered during the testing activities. Focus on improvements to role and responsibility definitions, processes, practices, and strategies.
- c. Revise the Contingency Plan as needed if there are important changes involving personnel, contact information, suppliers, legislation, or business risks, processes, or strategies.
- d. Annually conduct one or more of the exercises to test the Contingency Plan as set forth in paragraph a. above, or when there are significant changes to the environment.

**VII. Workforce Contingency Plan Training** (Attachment VIII)

MH facilities must train and prepare designated workforce members as necessary regarding the Contingency Plan.