

## SYSTEM ACCESS CONTROL PROCEDURE

### I. Contingency Operations

- A. Identify systems and data and their location that, if lost, will be reestablished and/or restored as a part of the Department's Disaster Recovery Plan or Emergency Mode Operation Plan.
- B. Identify the Workforce Members who need facility and/or system access in the event of a disaster or emergency.
- C. Create and implement a backup authentication scheme to regulate facility access in the event of a disaster or emergency. Since electronic means cannot be relied upon during an emergency, a "manual" authentication scheme should also be developed.
- D. When determining these access means, emergency communication means must be considered to ensure authorized access is granted in the event an obstacle is encountered.
- E. The contingent access scheme must be tested periodically to ensure operational functionality.

These procedures must be coordinated with other Department of Mental Health (DMH) contingency plan components, including DMH Policy No. 550.03, Facility IT Contingency Plan Policy.

### II. Facility Security Plan

The Facility Security Plan is intended to limit physical access to a facility's electronic information systems and the areas in which they are housed. It is also intended to allow physical access to a facility's electronic information systems and the areas in which they are housed to Workforce Members who need access in furtherance of County business.

To accomplish this purpose, DMH is taking a "layered approach." This means that the facility access measures will be "layered"—the more sensitive an area or system, the more restrictive the access control.

#### A. Exterior of Premises

The Facility Security plan must:

1. Clearly define the security perimeter of the premises and buildings.
2. Ensure that the perimeter defined above is physically sound (i.e., no gaps in which a break-in is relatively easy).
3. Ensure that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.

4. Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).
5. Provide for a reception area (staffed at least during business hours in which visitors may access the building through a single entrance to the area).
6. Define the instances in which visitors are allowed, including the areas they may visit and any escort requirements.
7. Ensure that any fire doors on the security perimeter are alarmed, have a self-closing mechanism, and are compliant with fire regulations.
8. If any of the measures in 1 through 7 above are determined not to be feasible, the Plan must provide a justification and must ensure the security of the premises through other sufficient means.

B. Interior of Premises

The Facility Security Plan must:

1. Ensure that any necessary physical barriers are extended from real floor to real ceiling.
2. Ensure that all doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices.
3. Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).
4. Ensure that all doors and windows lock by default and that adequate security measures are in place for windows at ground level.
5. Intrusion detection systems are included where appropriate to provide additional security to interior premises and buildings.
6. Ensure that vacant secure areas are locked and periodically inspected.
7. If any of the measures in 1 through 6 above are determined to not be feasible, the Plan must provide a justification and must ensure the security of the premises through other sufficient means.

C. Facility Equipment

The Facility Security Plan must:

1. Ensure that any facility equipment requiring additional levels of protection be isolated from other equipment to the extent possible.

2. Position workstations such that monitor screens and keyboards are not directly visible to unauthorized persons.
3. Provide controls to guard against equipment theft, such as closed-circuit television monitoring devices, alarms, locks, and controlled access.
4. Provide controls to guard against fire damage, such as smoke detectors, fire alarms, and fire extinguishers as reasonable to protect the electronic information system.
5. Provide controls to guard against water damage, such as elevating workstations and other equipment as reasonable to protect the electronic information systems.
6. Provide controls to ensure that air quality is maintained that is appropriate for the equipment, such as air conditioning, heating, dust filters, and air dehumidifiers/humidifiers, as reasonable to protect the electronic information systems.
7. Provide controls to guard against damage caused by vibrations or electrical supply interference.
8. Provide controls to guard against power surges and outages, such as multiple power feeds, backup generators, and uninterruptible power supplies.
9. If any of the measures in 1 through 8 above are determined to not be feasible, the Plan must provide a justification and must ensure the security of the information through other sufficient means.

III. Access Control and Validation

The Department of Mental Health Chief Information Officer (DMH CIO) or his/her designee must ensure that the System Managers/Owners and/or Facility Managers:

- A. Configure facility access controls to allow Workforce Members access based on the least approved access rights and privileges.
- B. Include a means to update the facility access control settings to reflect Workforce Member status changes.
- C. Ensure that visitors sign in upon entering the facility.
- D. Ensure that visitors are escorted by appropriate personnel where required by the Facility Security Plan.
- E. Ensure that Workforce Members testing and/or revising software programs are identified, authenticated, and authorized to perform those activities.

IV. Maintenance Records

The DMH CIO or his/her designee must

- A. Identify the physical components of the facility that are relevant to information technology (IT) security (e.g., hardware, walls, electronic systems, doors, and locks).
- B. Approve and oversee any IT-security-related physical modifications to the facility.
- C. Create a maintenance record or log and ensure that it is updated for each such modification.
- D. Ensure proper chain-of-custody for pertinent items like keys and access codes.