

INFORMATION ACCESS MANAGEMENT PROCEDURES

I. Risk Analysis

The Department of Mental Health Chief Information Officer (DMH CIO) must ensure that System Managers/Owners conduct risk assessments.

The persons assigned to conduct the risk assessment shall complete the following two forms, according to the guidelines indicated below:

- A. "System Description Report" characterizing the information technology (IT) system environment, and the delineation of the system boundary. The "System Description Report" shall cover:
 - a. System identification
 - b. Responsible organization
 - c. System contacts
 - d. System general operational status
 - e. General system classification:
 - i. Criticality (Supportive=1, Informative=2, Critical=3)
 - ii. The Sensitivity Score, which represents the highest level score from the three areas of confidentiality, integrity, or availability:
 - 1. Confidentiality (Low=1, Medium=2, High=3)
 - 2. Integrity (Low=1, Medium=2, High=3)
 - 3. Availability (Low=1, Medium=2, High=3)
 - iii. System environment
 - iv. System interconnection
 - v. Applicable laws or regulations affecting system
 - vi. Information Security Levels
- B. A "Risk Analysis Report" that describes the threats and vulnerabilities and then measures the risk. The "Risk Analysis Report" shall consist of:
 - a. A threat statement containing a list of threat-sources that could exploit system vulnerabilities
 - b. A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources
 - c. A list of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event
 - d. A likelihood of occurrence rating (Negligible, Very Low, Low, Moderate, High, Very High, Extreme)
 - e. A magnitude of impact rating (Insignificant, Minor, Significant, Damaging, Serious, Critical)
 - f. A risk level rating (High, Moderate, Low)

II. Risk Management

- A. The DMH CIO must ensure that System Managers/Owners develop and implement plans to mitigate the risks identified in the Risk Analysis Report. Both mitigation plans and justifications for not mitigating risks must be provided to the Department Information Security Officer (DISO) for review and approval.
- B. In deciding which security measures to use, the DMH CIO, DISO, and System Managers/Owners must take into account the following factors when the security (confidentiality, integrity, or availability) of electronic confidential and/or sensitive information is at issue:
 - a. The size, complexity, and capabilities of DMH and its facility;
 - b. The technical infrastructure, hardware, and software security capabilities;
 - c. The costs of security measures; and
 - d. The probability and criticality of potential risks to electronic confidential and/or sensitive information.
- C. The risk management process must consist of the following components:
 - a. DMH must implement security measures and safeguards sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The level, complexity, and cost of such security measures and safeguards must be commensurate with the risk classification of each such system.
 - b. With respect to electronic Protected Health Information (PHI), DMH must implement security measures and safeguards that are sufficient to:
 - i. Ensure the security (confidentiality, integrity, and availability) of PHI;
 - ii. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
 - iii. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the DMH Privacy and Security Compliance Program; and
 - iv. Ensure DMH workforce members' compliance with the DMH IT security policies and procedures.
 - c. DMH network, system, and application must be secured in accordance with DMH Policy No 107.02, DMH Privacy and Security Compliance Program pertaining to administrative, technical, and physical safeguards.

- d. To the extent DMH reassesses the potential risks and vulnerabilities of a system, as part of a periodic review, it must update the security measures and safeguards for such system to reflect any changes in the risks and vulnerabilities assessment.
 - e. The security measures and safeguards implemented for DMH must be documented and submitted to the DISO or designee for prior approval.
 - f. The persons assigned to conduct the risk management shall complete a "Risk Management Report" that provides recommendations for control implementation and consists of the following elements:
 - i. Recommended safeguards and actions
 - ii. Residual occurrence likelihood
 - iii. Residual impact severity
 - iv. Residual risk level
 - v. Justification for recommended safeguards and actions
- D. Each System Manager/Owner shall complete a "DMH Master Security Management Report" consisting of the key information from the "System Description Report," the "Risk Analysis Report," and the "Risk Management Report."

III. Information System Activity Review

- A. The DMH CIO must ensure that System Managers/Owners develop and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.
- B. The information systems activity review process must consist of the following:
 - a. Internal review procedures must be implemented to regularly review records of information system activity, such as system and application logs, access reports, and security incident tracking reports.
 - b. To ensure that system activity for all systems is appropriately monitored and reviewed, DMH must follow at least the minimum procedures outlined below:
 - i. An internal review procedure must be established and implemented by the DISO or his/her designee to regularly

review records of system activity. The internal review procedure may utilize system and application logs, activity reports, or other mechanisms to document and manage system activity.

- ii. System and application logs, activity reports, or other mechanisms to document and manage system activity must be reviewed at intervals commensurate with the associated risk of the information system. The interval of the system activity review must be done regularly. Mission critical systems should be reviewed monthly.
- iii. The DISO or his/her designee must create a System and Application Control and Review Plan. This plan must include:
 1. Systems and applications to be logged,
 2. Information to be logged for each system,
 3. Procedures to review all system and application logs and activity reports, and
 4. The system and application reviewer must not be the same person overseeing and/or managing the system or application.

Security incidents such as activity exceptions and unauthorized access attempts that are detected must be logged and reported immediately to the appropriate System Managers/Owners and the DISO or his/her designee in accordance with the DMH Policy No. 552.01, Security Incident Report and Response Policy.