A. Applicability

This policy shall apply to all e-mail systems used for any OMH purpose or as part of OMH business operations.

Specific implementation standards, based on existing and emerging OMH information systems, may provide specific technological and implementation details in support of this policy and should be consulted.

B. Policy Statement

Electronic Mail (e-mail) is one of the Office of Mental Health's (OMH's) core internal and external communication methods. To support compliance with the OMH's regulatory requirements, including the federal Health Insurance Portability and Accountability Act (HIPAA), New York State (NYS) Mental Hygiene Law, NYS Public Health Law, NYS ITS Information Security Policy NYS-P03-002, this policy provides a security framework for the use of e-mail.

C. Purpose

The purpose of this policy is to ensure that e-mail systems used by agency workforce members are used appropriately and securely, complying with all applicable statutory, regulatory and Agency requirements, and support Agency business functions. This policy advises all OMH workforce members and all users OMH e-mail systems of their responsibilities and provides guidance in managing information communicated by e-mail.

Comments and questions related to this policy and the associated standards should be addressed to the OMH Cyber Risk Coordinator (CRC).

D. Relevant Statutes and Standards

Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Standards
The Health Information Technology for Economic and Clinical Health (HITECH) Act
NYS Mental Hygiene Law
NYS Information Technology Policies
NYS ITS Security Policies and Standards
OMH Information Security Policy

E. Definitions

1. **Approved Encryption Method** means those encryption methods that have been publicly available, and which meet the Federal Information Processing Standard (FIPS) 140-3 Cryptographic Module Validation Program are accepted as secure, compliant with regulatory requirements and are approved by the OMH CRC.

2. **Encryption** means the process of transforming information (referred to as plaintext) using an algorithm or mathematical techniques (called cipher) to prevent it from being read or tampered with by anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

3. **OMH Information Assets** means one or more pieces of information contains OMH data is a communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

4. **Personal, Private, or Sensitive Information (PPSI)** means any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the Agency, its critical functions, its employees, its customers, third parties, or citizens of New York.
   PPSI includes information concerning a person which, because of name, number, personal mark or other identifier can be used to identify that person, in combination with:

   a) Social security number;

   b) Driver's license number or non-driver identification card number;

   c) Mother's maiden name;

   d) Financial account identifier(s) or other information which would permit access to a person's financial resources or credit;

   e) Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, and biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases;

   f) Information that identifies specific structural, operational, or technical information, including, but not limited to:

      i. Descriptions of technical processes and technical architecture;

ii. Plans for disaster recovery and business continuity;

iii. Reports, logs, surveys, or audits that contain sensitive information;

iv. Security related information (e.g., vulnerability reports, risk assessments, security logs);

v. Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by Agency executive management.

5. **Private Information means** (which may or may not include Protected Health Information) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

   a) Social security number;

   b) Driver's license number or non-driver identification card number; or,

   c) Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

   Private information excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records.

6. **Protected Health Information (PHI)** means individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium by a Covered Entity or Business Associate. "Individually identifiable health information" is information, including demographic data, that relates to:

   a) the individual's past, present or future physical or mental health or condition;

   b) the provision of health care to the individual; or

   c) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

7. **Security** means the safeguarding of (OMH) information against loss or misuse. Security must ensure the following:

   a) Confidentiality - protection of sensitive information from disclosure, restriction of

access to authorized users only;

b) Integrity - safeguarding the accuracy and completeness of information, assuring that information has not been corrupted, and

c) Availability - ensuring that critical information and services will be are available when needed.

F. Body of Directive

This policy directive consists of seven components:

1. Access to OMH E-Mail Services
2. Use of OMH E-Mail
3. Privacy and Access
4. Security
5. Management and Retention of E-Mail Communications
6. Roles and Responsibilities
7. Additional Information

1) Access to OMH E-Mail Services

E-Mail services are provided to OMH workforce members based on job function and available resources. OMH e-mail services may also be provided, following OMH CRC approval, to external business partners if there is a need for secure communications between OMH and the business partner, and other secure processes, such as business-to-business encryption, cannot be utilized.

2) Use of OMH E-Mail

OMH e-mail services, like other means of communications, are to be used primarily to support agency business. Users of OMH's e-mail systems may also use e-mail to communicate informally with others so long as the communication meets professional standards of conduct and adheres to the New York State Acceptable Use Of Information Technology Resources Policy (NYS-P14-001). Any usage of e-mail for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the State is strictly prohibited and may lead to disciplinary action.

E-mail that contains computerized correspondence, payment and billing information, or any individually identifiable patient data is considered confidential and as such, may not be communicated to another person, public or private health care provider or agency through the use of e-mail unless approved encryption methods are employed.

3) Privacy and Access

(a) There is no expectation of privacy in e-mail messages within the NYS mail system, and users are reminded e-mails are not personal or private. System administrators may access an employee's e-mail:

i. for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time);

ii. to diagnose and resolve technical problems involving system hardware, software, or communications; and/or

iii. to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

(b) Users are prohibited from accessing another user's e-mail without his or her permission and may do so only through an approved delegation mechanisms, such as Outlook delegation. OMH may allow third-party access as may be required by law, court order, warrant, subpoena or other administrative process, including internal agency investigations.

(c) E-mail messages sent or received in conjunction with agency business may:

i. be releasable to the public under the Freedom of Information Law;

ii. require special measures to comply with the Personal Privacy Protection Law;

iii. may be subject to discovery proceedings in legal actions.

4) Security

E-mail security is a joint responsibility of NYS system administrators and e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, and protecting their active sessions on the system, to prevent the use of their OMH e-mail account by unauthorized individuals. Users that utilize personally-owned devices to access State Entity data must comply with access methods described in the New York ITS Bring Your Own Device Standard (NYS-S14-012).

5) Management and Retention of E-Mail Communications

(a) E-Mail Messages and Attachments

Since e-mail is a communications system, messages should not be retained for extended periods of time unless otherwise guided by records retention requirements. Users should remove e-mail communications in a timely fashion. If information in an e-mail message would be considered agency business records and require retention for an extended period, it should be transferred from an individual e-mail system

account to an appropriate electronic or other filing system. If one can reasonably anticipate there may be litigation, there is a duty to preserve evidence, including e-mail and data that might be inadvertently destroyed as a result of automated network settings.

Shared mailboxes shall have clear and descriptive names, and a clearly defined owner. Permissions to a shared mailbox shall be based upon a defined business need, and each member shall have their own login credentials. E-mails and attachments in shared mailboxes shall be preserved.

(b) Records Communicated via E-Mail

E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the New York Arts and Cultural Affairs Law and specific program requirements.

i. Examples of records which could originate in e-mail include:

(1) Policies and directives;

(2) Correspondence or memoranda related to official business;

(3) Work schedules and assignments;

(4) Agendas and minutes of meetings;

(5) Drafts of documents that are circulated for comment or approval

(6) Any document that initiates, authorizes, or completes a business transaction; and,

(7) Final reports or recommendations.

ii. Some examples of messages that typically do not constitute records are:

(1) Personal messages and announcements;

(2) Copies of extracts of documents distributed for convenience or reference;

(3) Phone messages;

(4) Announcements of social events.

(c) Record Retention for Shared Mailboxes

Records communicated using e-mail need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed, and accessible in an existing filing system outside the e-mail system, or retained in a Shared Mailbox, in accordance with the appropriate program unit's standard practices.

Records communicated via e-mail will be disposed of within the record keeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning Records Disposition Authorization (RDA)s applicable to their program's records.

Users should dispose of copies of records in e-mail after they have been filed in a record keeping system and delete records of transitory or little value that are not normally retained in record keeping systems as evidence of agency activity.

6) Roles and Responsibilities

Agency executive management will ensure that policies are implemented by program unit management and unit supervisors. Program unit managers and supervisors will develop and/or publicize record keeping practices in their area of responsibility including the routing, format, and filing of records communicated via e-mail. NYS e-mail system administrators are responsible for e-mail security, backup, and disaster recovery.
All e-mail users must adhere to the NYS Acceptable Use of Technology Resources Policy and:

(a) Be courteous and follow accepted standards of etiquette.

(b) Protect others' privacy and confidentiality

(c) Consider organizational access before sending, filing, or destroying e-mail messages.

(d) Protect their passwords.

(e) Comply with agency and unit policies, procedures, and standards.

7) Additional Information

Questions regarding this standard should be directed to the OMH Cyber Risk Coordinator via e-mail to infosec@omh.ny.gov.