Massachusetts Department Of Corrrection **POLICY**		Effective Date 7/30/2021	Responsible Division Deputy Commissioner, Administration
		Annual Review Date 9/17/2026	
Policy Name 103 DOC 758 E-MAIL		M.G.L. Reference: M.G.L. c. 4, § 7(26); M.G.L. c. 93H, § 3; M.G.L. c. 268A, §23(b); E.O. 283; E.O. 532; Fed. R. Civ. P. 34; Fed. R. Civ. P. 37	
		DOC Policy Reference:	
		ACA/PREA Standards:	
Attachments Yes ☐ No ☒	Library Yes ☐ No ☒	Applicability: Staff	
Public Access Yes ☒ No ☐		Location: DOC Central Policy File Institution Policy File	

PURPOSE:
To establish Department of Correction (Department) policy regarding Electronic Mail ("E-mail").

RESPONSIBLE STAFF FOR IMPLEMENTATION AND MONITORING OF POLICY:
Deputy Commissioner of Administration
Assistant Secretariat Chief Information Officer

CANCELLATION:
103 DOC 758 cancels all previous Department policies, statements, bulletins, directives, orders, notices, rules or regulations regarding e-mail access that are inconsistent with this policy.

SEVERABILITY CLAUSE:
If any part of 103 DOC 758 is for any reason held to be in excess of the authority of the Commissioner, such decision shall not affect any other part of this policy.

TABLE OF CONTENTS

758.01	Definitions	3
758.02	General Policy	4
758.03	Approved E-mail Application	5
758.04	Acceptable Users	6
758.05	Prohibited Uses	6
758.06	Training	7
758.07	Annual Report	7
758.08	No Expectation of Privacy	7
758.09	E-mail Retention Guidelines and Procedures	7
758.10	Review Date	11

758.01 Definitions

Archive- To copy files to a long-term storage medium.

Assistant Secretariat Chief Information Officer ("ASCIO")- An employee of the Executive Office of Public Safety and Security ("EOPSS") who is the administrator of the Department of Correction's Office of Technology and Information Services("OTIS"), which provides Department employees with the technology to perform their duties efficiently, while maintaining the security and integrity of all technology systems.

Commonwealth of Massachusetts Information Technology Solution Management ("COMiT")- The web-based service request management tool used by all EOPSS employees to report Information Technology ("IT") issues and/or request IT services from the secretariat's Office of Technology and Information Services ("OTIS").

Electronic Mail ("E-Mail")- The transmission of messages electronically over communication networks. The messages can be entered from a keyboard or electronic files. Sent messages are stored in electronic mailboxes until the recipient retrieves them.

Encryption- The translation of data into a secret code.

MassMail - The current approved official collaboration/e-mail software in use by the Department.

Litigation Hold Letter- Written communication directing employee(s) to segregate and suspend the destruction of certain documents and data that are, or arguably may be, relevant to a threatened or pending litigation. A litigation hold prevents destruction, alteration, or mutilation of evidence and applies to both paper based documents and electronically stored information.

Metadata- Information included with e-mail, including, but not limited to: the mailing addresses, date/time stamp, routing instructions and transmission and receipt information.

Office of Technology and Information Services ("OTIS")- The Division that delivers technology throughout the Department of Correction. Its mission is to provide employees with the technology to perform their duties efficiently, while maintaining the security and integrity of all technology systems, hardware, software and related technology.

Records Conservation Board ("RCB"): Established pursuant to G.L. c. 30, § 42, the RCB is comprised of the State Librarian, Attorney General, State Comptroller, Commissioner of Administration, Supervisor of Public Records, and Chief of the

Archives Division in the Department of State or their designees. The RCB is empowered to require all state agencies to identify the records maintained and to set standards for the management and preservation of such records and to establish schedules for the destruction or transfer of such records no longer needed for business.

Statewide Records Retention Schedule: A schedule for retention of state records produced pursuant to G.L. c. 4, §7, cl.26; G.L.c.30, §42; and G.L.c.66, §§1,8 and 9. This schedule, approved by the RCB, sets the retention periods for all executive branch records, including state records being managed by contracted service providers, regardless of form.

758.02 General Policy

1. When using their state issued e-mail addresses, i.e., (Username@doc.state.ma.us) or (first.last@state.ma.us), users shall regard e-mail messages as the equivalent of letters sent on official letterhead. As such, users shall write all e-mail messages in a professional and courteous tone.

2. Although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

3. Subject to certain exceptions in the law, e-mail messages are considered public records, copies of which may be requested by any member of the public. Even deleted messages may still exist on back up tapes and be subject to disclosure.

4. The daily flow of e-mails represents an impact on network capacity. E-mail shall only be used to communicate official business to recipients. Employees who are the recipients of non-business related e-mail are required to discard them, and shall under no circumstances forward them to anyone. E-mail attachments that are received from an unknown party shall be considered suspicious and shall not be opened until the sender's identity can be confirmed, as many viruses are spread using e-mail.

   The Internet offers a variety of electronic mailing lists. These mass-mailing lists come from servers managed by a wide range of organizations. To receive the mass-mailings one must subscribe to the list using their Internet e-mail address. Employees are not to subscribe to mailing lists if the content is not related to their job functions. Recreational examples would be "joke of the day", "horoscope", "trivia", "Daily Word", etc. Each of these mass-mailings use limited network

capacity and storage capacity that should be used for other, business related purposes. Any employee wishing to subscribe to such lists, for business related purposes, must have prior approval, from their Superintendent/Division Head.

758.03 Approved E-mail Application

Massmail is currently the approved official collaboration/e-mail software in use by the Department. Department employees/contractors may use the network to access other e-mail services (America OnLine, Yahoo mail, Hotmail, etc) for business related purposes, with the approval of their Superintendent/Division Head. Using the network to access these services without prior approval is viewed as a violation of the established Rules and Regulations of the Department and disciplinary action, up to and including termination, may occur for documented violations.

1. Encryption

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

The Department's e-mail application has its own built-in encryption because it is a closed proprietary system. When communication is opened to the Internet, proprietary encryption is lost for messages routed through the Internet to non-approved systems. The automatic forwarding of a user's e-mail to an outside e-mail account is prohibited unless specifically approved by the Superintendent/Division Head in collaboration with the EOPSS ASCIO. Nevertheless, the user needs to understand that once a mail message leaves the Department's mail server, there is no encryption protection on that message or attachment.

The forwarding of a user's e-mail shall have a pre-determined time period unless the forwarding goes through a secure server or site (i.e. Blackberries) and is approved by the ASCIO. If there is suspicion of a security breach, the ASCIO shall terminate the forwarding of e-mail and report it to the Superintendent/Division Head.

2. Public Groups

Public groups or distribution lists are available to e-mail users, however, approval is needed from the ASCIO. Requests shall be submitted via COMiT. Once approved, the responsibility of providing changes the group rests with the requester and not the OTIS. Requests shall be logged via COMiT.

3. Mass-Mailings

OTIS shall send any mailings to all staff in the Department. Anyone wishing to send a message to everyone shall have prior approval from the ASCIO. The request shall be sent via COMiT.

758.04 Acceptable Uses

The Department believes that e-mail empowers users and makes their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, employees and contractors are encouraged to use e-mail fully in pursuit of the Department's goals and objectives.

Employees in the National Association of Government Employees' ("NAGE") Units 1, 3 and 6 are authorized to receive and read e-mail notices sent to them from NAGE. These e-mails may refer employees or provide a link to the NAGE website for additional information, or refer employees to other websites or sources of information.

This does not, however, confer the right to engage in union business during work time and with work computers.

758.05 Prohibited Uses

1. Unless such use is reasonably related to a user's job, it is unacceptable for any person to use e-mail:

    - in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal;
    - for any political purposes;
    - for any commercial purposes;
    - to send threatening or harassing messages, whether sexual or otherwise;
    - to access or share sexually explicit, obscene, or otherwise inappropriate materials;
    - to infringe any intellectual property rights;
    - to gain, or attempt to gain, unauthorized access to any computer or network;
    - for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
    - to misrepresent either the agency or a person's role at the agency;
    - to distribute chain letters;
    - to access online chat sites;
    - to libel or otherwise defame any person(s).

2. Participation in any prohibited use is viewed as a violation of the established Rules and Regulations of the Department and is subject to disciplinary action, up to and including termination and/or referral to the District Attorney for documented violations.

758.06 Training

1. The Division of Staff Development shall offer training as needed to Department personnel in the use of approved e-mail software.

2. Each Superintendent, Division Head or Unit Director shall ensure that personnel under their supervision are properly trained in the use of the Department's approved e-mail software.

758.07 Annual Report

Annually, the Commissioner, Deputy Commissioners, Assistant Deputy Commissioners, General Counsel, Superintendents and Division Heads shall review the list of approved e-mail users under their respective accounts. This report, called "Account Reports", is available at any time via the Department's Intranet under Intranet Applications.

758.08 No Expectation of Privacy

The Department's approved e-mail application is the property of the Commonwealth of Massachusetts and is to be used in conformance with this policy. The Department retains and, when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, shall exercise the right to inspect any user's computer, and data contained in it, and any data sent or received by that computer. Users should be aware that system administrators, (both within the OTIS and the Commonwealth's Information Technology Division), routinely monitor network traffic in order to ensure proper network operations. Use of the approved e-mail software constitutes express consent for the Department to monitor and/or inspect data that users create or receive and any messages they send or receive.

758.09 E-mail Retention Guidelines and Procedures:

1. General Information

   a. All e-mail records sent and received during the course of an employee's responsibilities may, depending on their content, be Public Records as defined by M.G.L. c. 4, §7, cl. 26, and shall not be deleted except in accordance with this policy. E-mails that are Public Records shall be saved by the custodian or keeper of that Public Record to a permanent electronic record system and

preserved in accordance with the current Massachusetts Statewide Records Retention Schedule. The contextual or "envelope" information [metadata] included with an e-mail, which contains the mailing address, date/time stamp, routing instructions and transmission and receipt of information, constitutes part of the e-mail and shall be retained as part of any printed or electronically stored version of the e-mail. It is the content of the e-mail and not the type of media on which it is stored that determines how long it must be retained.

b. The custodian or keeper of an e-mail shall preserve that e-mail, unless the e-mail is not required to be preserved under the retention schedule. You are the custodian or keeper of: (a) all business e-mails you send, and (b) business e-mails you receive if you are one of the primary recipients of the e-mail or you are the only one receiving it within your agency. You are not the custodian or keeper of an e-mail if you are simply copied on the e-mail sent to another employee of the Department, and, as such, you are not generally required to retain the e-mail. Exceptions may exist in connection with litigation or other legal disputes. You should comply with any instructions you receive from the Department's Legal Division or the Attorney General's Office to retain records, even if you are not the custodian or keeper of the e-mail under this policy.

2. Requirements Applicable to Retention of Email Records

a. Dependent upon their "content," e-mail records are subject to the same records management principles as all other records of the Department. The Secretary of the Commonwealth and the RCB identify e-mail as a transitory messaging system and not as a primary record keeping system; however, e-mails with business "content" that pertain to Department operations must be retained as Public Records. Records retention standards issued by the Supervisor of Public Records and the RCB must be implemented for e-mail as well as for analogous paper records. Once the "content" or subject matter of a message is determined, the custodian of the e-mail must consult the current Massachusetts Statewide Records Retention Schedule to determine how long the record must be preserved. Prior to destroying records or transferring them to the State Records Center or State Archives, the records custodian shall submit Form RCB-2, Application for Destruction Permission, to the Superintendent/Division Head for review and approval. Once approved, the Form RCB-2 shall then

be sent to the RCB to obtain permission for the destruction of the records. No records may be disposed of without the approval of the RCB.

b. If an e-mail is sent or received during the course of an employee's responsibilities and pertains to the business of his/her office, it is likely to be a "Public Record," and therefore shall be retained in accordance with the current Massachusetts Statewide Records Retention Schedule. The Department's Legal Division should be consulted with any questions regarding the Public Records law.

c. Approval from the RCB is required before any "Public Records" (including e-mail "Public Records") may be destroyed. There are, however, some categories of e-mails that do not have to be retained under the current Massachusetts Statewide Records Retention Schedule after their administrative use has ceased, and, if properly deleted, do not need to be produced as public records or in response to a discovery request. Some of the types of e-mails that ordinarily do not need to be retained and can be deleted from your e-mail are:

- Program transitory correspondence encountered in the daily administration of the unit and its programs, including acknowledgments, courtesy correspondence, declined invitations, meeting announcements, scheduling changes.
- Documents scheduling meetings, travel, appointments and events, including calendars and related lists and postings unless they relate to activities of executives or persons in policy-making positions. The person responsible for arranging a work-related event or creating a policy should preserve the documents related to those actions.
- Out-of-office replies
- Thank you messages
- Communications regarding routine office policies and procedures, such as handling mail, opening hours, storm coverage
- Duplicate messages/attachments
- Junk mail or spam
- Published reference materials collected from sources outside the agency
- Replies to routine questions and information requests - for example, address and hours open, requests for forms
- Incoming listserv messages
- Media advisories, news and press releases and web announcements sent for informational purposes unless you were involved in the drafting or review of these documents

- E-mails sent to another employee within the Department, with a copy sent to you as long as you are not the custodian or keeper of that e-mail as described above.
- Reports, meeting minutes and publications that are distributed to you for your convenience as a member of a group or committee and are not needed to support other files. If the group has a secretary or record keeper maintaining copies, you do not need to keep an additional copy.

For all other e-mails pertaining to Department business and operations not on this list, check with the Department's Legal Division or consult the current Massachusetts Statewide Records Retention Schedule prior to destruction. Department employees are encouraged to become familiar with the retention requirements that apply to their particular responsibilities. The schedule is arranged by subject matter and will tell you how long the e-mail should be kept, based on its content. If the schedule provides that the record may be destroyed "after administrative use ceases," the record may be deleted after that time. If the schedule requires a specific number of years for retention, the record cannot be destroyed until that time has elapsed and a written request is submitted to and approved by the RCB.

Proper records management and maintenance, including e-mail management and maintenance, is an individual responsibility. Users of the Department's e-mail system should contact their supervisor if they have questions or concerns regarding proper records maintenance.

3. Retention for Litigation Purposes

Upon receipt of a litigation hold letter placing a Department employee on notice that litigation is or may be forthcoming, the employee shall comply with the terms of such letter and shall:

- Suspend the deletion, overwriting or any other destruction of e-mail and/or other electronic records and/or paper records relevant to the subject matter of said litigation, even if in the normal course of operations said records could be destroyed or deleted pursuant to the Massachusetts Statewide Records Retention Schedule. The records subject to the requirement herein cover all electronic information wherever it is stored, including at the employee's work station, on a laptop, or on a home computer if utilized for work. Such records include all forms of electronic communication (e.g. e-mail, word processing, calendars, voice messages, videos, photographs, and information in personal data assistants (PDAs)).
- Information must be preserved in its original electronic form, so that all information contained within it, whether visible or

not, is also available for inspection. In other words, it is not sufficient to make a hard copy of an electronic communication.

- Preserve all new paper documents and records that are generated after receipt of the litigation hold letter that could be considered relevant to this dispute, and maintain such documents and records in a manner in which they can be readily retrieved upon the request of the Department's Legal Division.
- Notify the Department's Legal Division of the identity of any other employee or person whom the recipient of the litigation hold letter believes possesses relevant paper and electronic records.
- If the litigation hold letter was not received from the Department's Legal Division, notify the Department's Legal Division that he/she has received a litigation hold letter.
- Notify COMiT that any destruction or overwriting of email, network back-up tapes and/or other media for his/her account should be suspended.
- Notify the Department's Legal Division if he/she is aware of becomes aware that any e-mail relevant to the subject matter of said litigation has been deleted or destroyed.

The obligation to preserve e-mail and electronic and paper records relevant to the subject matter of said litigation is ongoing. Therefore, the recipient of a litigation hold letter shall provide a copy of the litigation hold letter to any person who is designated to act for the employee in his/her absence. Upon vacating his/her position, the employee shall provide a copy of the litigation hold letter to his/her successor. Additionally, any Department employee who leaves his/her current position shall contact COMiT and request that COMiT preserve his/her e-mails and other electronic records.

758.10 Review Date

This policy shall be reviewed annually from the effective date by the Deputy Commissioner of Administration. The party or parties conducting the review shall develop a memorandum to the Commissioner with a copy to the Central Policy File indicating the review has been completed. Recommendations for revisions, additions or deletions shall be included.

In the event of a department wide loss of computer infrastructure; a contingency plan for Continuity of Operations Plan (COOP) is located in the Deputy Commissioner of Administration's Office.