

COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF TECHNOLOGY AND SECURITY SERVICES
ADMINISTRATIVE DIRECTIVE 2018-1
ENTERPRISE SECURITY POLICIES AND AWARENESS TRAINING

October 5, 2018

I. AUTHORITY

M.G.L. Ch. 7D, Sec. 2¹

M.G.L. Ch. 7D, Sec. 3(a)²

II. BACKGROUND AND DEFINITIONS

- a. Prior to the establishment of EOTSS, cybersecurity governance in the Commonwealth Executive Department was decentralized, with each agency developing, implementing, and maintaining its own “written information security plan.” This has led to an inconsistent approach to risk management and cybersecurity governance. Furthermore, the emphasis on annually submitted written plans has not kept up with the need for continuous monitoring and risk management. As such, it is necessary to establish an enterprise approach to cybersecurity governance and risk management.
- b. Human behavior continues to be one of the greatest sources of cybersecurity risk, whether through intentional behavior or unintentional error. Cybersecurity best practice, as well as standards and guidelines established by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), indicates that regular cybersecurity awareness training is an effective way to reduce this risk.

III. OPERATIVE PROVISIONS

- a. This administrative directive formally adopts new enterprise security policies and standards for all executive department entities. Executive department entities includes all entities set forth in M.G.L. Ch. 6A, Sec. 2.
- b. The new enterprise security policies and standards adopted pursuant to this administrative directive shall supersede any existing policy or standard to the extent that any new policy or standard conflicts with or contradicts any existing policy. Any policy currently in existence that is not superseded remains in effect until expressly revoked or revised.
- c. As of the effective date of this directive, the enterprise security policies and standards located at the following URL are applicable to all entities within the Executive Department:

[HTTPS://WWW.MASS.GOV/CYBERSECURITY/POLICIES](https://www.mass.gov/cybersecurity/policies)

¹ “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.” M.G.L. Ch. 7D, Sec. 2

² The Executive Office of Technology Services and Security “shall have all powers necessary or convenient to carry out its duties, including, but not limited to,” the authority to “issue administrative directives pursuant to the authority set forth in this chapter which shall be binding on all executive department agencies and offices” M.G.L. Ch. 7D, Sec. 3(a).

Current versions of all applicable enterprise policies, standards, baselines, guidelines, and procedures will be kept at this URL. To maintain and improve the security posture of the Commonwealth, EOTSS will revise and supplement these enterprise documents annually, or more frequently, as needed.

- d. Within **120 days** from the date of this directive, EOTSS will collaborate with all Executive Secretariats and will work with each respective Secretariat to develop a compliance plan for the enterprise security policies and standards. It is EOTSS' goal to eventually ensure universal Executive Department compliance with the policies and standards adopted pursuant to this administrative directive, as soon as practicable. Nevertheless, EOTSS recognizes that full compliance may not be immediately achievable.

To that end, the compliance plan for each executive office (and agency within any executive office, where applicable) will provide a detailed schedule of compliance, along with any mitigating circumstances or granted exceptions.

No executive office nor any agency within any executive office shall be deemed to be out of compliance with the enterprise security policies and standards that are adopted by this Administrative Directive if (1) the executive office or agency within any executive office collaborates with EOTSS to establish a compliance plan during the one hundred and twenty (120) day period after the effective date of this administrative directive; or (2) during the period beginning after one hundred and twenty (120) days following the effective date of this administrative order, the executive office or agency within any executive office complies with the provisions of the compliance plan established in cooperation with EOTSS pursuant to this administrative directive. Notwithstanding anything to the contrary, Executive Secretariats may maintain additional security policies, provided that such additional security policies do not conflict with, and are supplemental to, the enterprise security policies and standards posted at the URL.

- e. All Executive Department employees (including contract employees AND VENDOR STAFF, WHERE APPLICABLE) with access to information technology resources are required to complete annual cybersecurity awareness training. In consultation with the Human Resources Division, EOTSS will provide an annual training curriculum updated to include the latest cybersecurity threats.
- f. The Executive Department shall continue to implement the maximum feasible measures reasonably needed to ensure the security, confidentiality, and integrity of personal information, as defined in Massachusetts General Laws (M.G.L.) Chapter 93H, and personal data, as defined in Massachusetts General Laws Chapter 66A.

Incidents involving a breach of security or unauthorized acquisition or use of personal information shall be immediately reported to EOTSS and to such other entities as required by the provisions of M.G.L. Chapter 93H, or any other applicable state or federal law, rule or regulation.

Nothing in this administrative directive shall be construed to eliminate, limit or otherwise constrain the duty of any executive office, or any agency within an executive office, to comply with any existing federal or state statute, law, rule or regulation to which it may be subject.

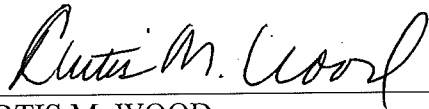
IV. GUIDANCE & COMPLIANCE

Please contact the following individual for clarification on the interpretation or application of this administrative directive.

Dennis McDermitt
Chief Information Officer
Chief Information Security Officer
Executive Office of Technology Services and Security
(617) 626-4403
Dennis.McDermitt@mass.gov

V. EFFECTIVE DATE

The provisions of this administrative directive shall become effective on the date of signature.³



CURTIS M. WOOD
SECRETARY

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES AND SECURITY

Date of Signature: October 5, 2018

³ If any provision of this administrative order or its application to any person or circumstance is held invalid by any court or administrative tribunal of competent jurisdiction, any such finding of invalidity shall not affect any other provision or application of this administrative directive that can be given effect without the invalid provision or application. To achieve this purpose, the provisions of this administrative order are declared to be severable. Nothing in this administrative directive shall be construed to contravene any state or federal law, nor to convene any provision of any collective bargaining agreement to which the Commonwealth is a party.