MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject: Enterprise Technology Security Council	***Number:*** 245.19 Amended
Date: August 17, 2016	***By Direction of:*** Sharon P. Minnich, Secretary of Administration

Contact Agency:
Office of Administration, Office for Information Technology, Enterprise Information Security Office, Telephone 717.772.8600, Email: ra-ciso@pa.gov

This directive establishes policy, responsibilities, and procedures to ensure that the commonwealth secures its critical and sensitive Information Technology (IT) assets, and creates an Enterprise Technology Security Council (ETSC). Marginal dots are excluded due to major changes.

1. **PURPOSE.** To establish policy, responsibilities, and procedures for the Office of Administration, Office for Information Technology (OA/OIT) and ETSC to deploy enterprise-wide IT security practices, including establishing product standards, IT security policies, technical reviews of agency systems, and establishing procedures, and protocols, in alignment with OA's responsibilities under *Executive Order 2016-06, Enterprise Information Technology Governance*.

2. **SCOPE.** This directive applies to all individuals in departments, boards, commissions, and councils (hereinafter referred to individually as an "agency" and collectively as the "enterprise") under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow the policy and procedures stated in this directive.

3. **OBJECTIVES.**

   a. Create and preserve effective processes that create a continuous enterprise security life cycle.

   b. Maintain a formal collaboration and reporting relationship between OA/OIT and all agencies, which addresses the need for a comprehensive enterprise security approach.

c. Disseminate recommendations and directives on enterprise security policies, processes, procedures, and solutions as determined by OA/OIT and the ETSC.

4. DEFINITIONS.

a. Agency Information Security Officer (ISO) / IT Administrator. Employees responsible for the administrative work in managing security programs within an agency's centralized information security unit.

b. Chief Information Security Officer (CISO). The Commonwealth's senior-level executive responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes to reduce information and IT risks. The CISO responds to incidents, establishes appropriate standards and controls, manages security technologies, and directs the establishment, implementation and enforcement of IT security policies and procedures.

c. Electronic Communication System. Any method of electronic communication or information system that generates, stores, transmits, or displays information, including, but not limited to:

(1) The commonwealth's Metropolitan Area Network;

(2) Local Area Networks;

(3) The Internet;

(4) News groups;

(5) Bulletin board systems;

(6) Intranets;

(7) Social media;

(8) Blogs;

(9) Computer hardware;

(10) Software programs;

(11) Applications;

(12) Voice mail systems;

(13) Telephones;

(14) Faxes;

(15) Radio;

(16) Cellular and smartphones;

(17) Electronic mail and messaging systems;

(18) Instant Messaging;

(19) Text Messaging;

(20) Cloud storage solutions;

(21) Video conferencing and transmissions; and

(22) Electromagnetic, photo-electronic, and other electronic media or devices.

d. Enterprise Technology Security Council (ETSC). A team of Commonwealth employees who will assess security policies, procedures, and solutions within the commonwealth's IT systems, services, and resources and develop recommendations for increasing their effectiveness.

e. Information Assets. Include, but are not limited to, the following: data and information in electronic form which is created, gathered, accessed, or maintained by or on behalf of a Commonwealth agency.

f. IT Resources. Any commonwealth computer system, Electronic Communication System, or electronic resource used for electronic storage and/or communications, including, but not limited to:

(1) Servers;

(2) Laptops;

(3) Desktop computers;

(4) Copiers;

(5) Printers;

(6) Wired or wireless telephones;

(7) Cellular phones or smartphones;

(8) Tablets;

(9) Wearables;

(10) Pagers;

(11) All other mobile devices; and

(12) Commonwealth contractor-provided IT Resources of all kinds.

5. POLICY. *Executive Order 2016-06, Enterprise Information Technology Governance* permits OA/OIT to formulate and implement an ETSC for the purpose of providing recommendations on enterprise security policies, processes, procedures, and solutions.

6. RESPONSIBILITIES.

a. ETSC shall:

(1) Make recommendations aimed at improving the security of Commonwealth IT Resources and the Information Assets that reside on them.

(2) Assess and address security concerns, risks, vulnerabilities, and promote enterprise-wide security best practices and governance to increase the security of Commonwealth Information Assets and IT Resources.

(3) Monitor security policies, procedures, and solutions within the Commonwealth's IT Resources and develop recommendations for increasing their effectiveness.

(4) Develop IT self-assessment tools for internal security auditing and compliance and make recommendations for enterprise security best practices.

(5) Create cost effective and comprehensive security initiatives.

(6) Inform and advise OA/OIT on policies which permit compliance with federal and state law regarding the collection, maintenance, use, and security of Information Assets.

b. OA/OIT shall:

(1) Maintain an enterprise-wide approach to information security, including appropriate security awareness training and education, and effective IT Policies (ITPs).

(2) Create ITPs which permit compliance with federal and state law regarding the collection, maintenance, use, and security of Information Assets.

(3) Establish and implement prudent, reasonable, and effective practices for the protection and security of Information Assets and IT Resources, which include the protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification, or destruction.

(4) Develop effective mechanisms for responding to incidents, breaches, or misuse of Commonwealth Information Assets or IT Resources, in accordance with information security policies.

(5) Reduce the overall and specific risk of breach or misuse of Commonwealth Information Assets and IT Resources and the associated damage and cost of breach or misuse.

c. Agency ISO / IT Administrator shall:

(1) Comply with IT security policies established by OA/OIT.

(2) Implement immediate corrective actions to address security violations.

(3) Communicate compliance actions, remediation actions, security-oriented waiver requests and OA/OIT's responses, and other actions associated with IT security to appropriate agency stakeholders.

7. PROCEDURES. The OA/OIT Enterprise Security IT Policies (designated "ITP-SEC") outline detailed practices and specific enterprise product standards relative to IT security.

This directive replaces, in its entirety, *Management Directive 245.19*, dated, May 3, 2006.