MARYLAND STATE DEPARTMENT OF EDUCATION (MSDE)

AGENCY DIRECTIVE (AD)

NUMBER:
AD 21201-001

SUBJECT:
Security Awareness and Training Policy

EFFECTIVE DATE:
March 01, 2021

APPROVED: Karen B. Salmon, Ph.D.
Karen B. Salmon, Ph.D. (Mar 3, 2021 13:52 EST)

Karen B. Salmon, Ph.D.
State Superintendent of Schools
Maryland State Department of Education

Section

1. PURPOSE

I. This publication establishes the policy of the Maryland State Department of Education (MSDE) for meeting the laws, regulations, standards, and best practices of a full security awareness and training program.

II. This policy addresses guidance published or issued by the Maryland Department of Information Technology (DoIT) and the National Institute of Standards and Technology (NIST) requiring an

agency-wide Information Technology (IT) security awareness and training program to be designed, documented, and implemented.

III. It is the goal of MSDE to comply with State requirements to setup, implement, and manage a security awareness training program. The agency confirms its management's commitment to compliance with the State's mandate in establishing and managing security awareness training.

2. SCOPE

This policy applies to all MSDE divisions and staff offices, employees, and contractors working for or on behalf of the MSDE who require access to MSDE information systems or are otherwise directed by State guidance to comply with this training requirement.

3. SPECIAL INSTRUCTION

The security awareness and training policy only applies to the awareness and training aspects of IT.

4. BACKGROUND

I. DoIT's *State of Maryland Information Technology Security Manual* establishes policies that define the State's IT security practices and requirements for all State of Maryland agencies. Operational level controls, a*wareness and training,* require that agencies ensure all information system users and managers are knowledgeable of security awareness material and protocols before authorizing access to systems.

II. MSDE has established an IT security awareness and training program for use throughout MSDE. This Agency Directive (AD) defines the policy and strategy for IT security awareness and training within the Department.

5. POLICY

a. Security Awareness and Training Policy

All MSDE employees and contractors shall routinely and periodically obtain information security awareness information (e.g., training course, training quizzes, security campaign).

b. Annual Computer Based Training

I. The security awareness and training course is mandatory for all MSDE employees and contractors.

II. Security awareness training shall provide the information security training as described in NIST Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

III. New MSDE employees and contractors shall complete security awareness training prior to gaining access to information systems.

c. Role-based Security Awareness training

I. All MSDE employees and contractors who have been identified by their agency or staff office as having significant responsibility for information security (such as those who manage, administer, operate, and design IT systems, and other senior management roles, such as authorizing officials, chief information officers and information security program managers) shall receive formal role-based information security training (also known as specialized training).

d. Training Metrics

I. A system of records shall be maintained for the MSDE security awareness and training course, in the MSDE training system of record (DoIT, Infosec IQ).

II. Reporting and tracking shall be accomplished within the MSDE system of record for security awareness training.

6. ROLES AND RESPONSIBILITIES

a. The MSDE Chief Information Officer (CIO) shall:
   I. Establish the overall strategy for the Agency's security awareness and training program.
   II. Ensure that senior management, executives, system owners, and others understand the security awareness and training program's strategy and concept and are informed of the success of the implementation of the program.
   III. Ensure security awareness and training program is adequately funded.
   IV. Hold agency and staff office responsible for ensuring their personnel enroll and complete required training course.
   V. Ensure that the agency's system of record for tracking and reporting security awareness and training records is in place.
   VI. Assign a security awareness training manager for the agency.

b. The MSDE Deputy Chief Information Officer (DCIO) shall:
   I. Provide oversight of the MSDE security training program.
   II. Ensure annual review of security awareness and training policy.
   III. Ensure MSDE implements, manages, and monitors the MSDE security training program for compliance.

c. The MSDE Security Awareness Training Managers shall:
   I. Ensure all agency employees and contractors have accounts in the official MSDE training system (DoIT's INFOSEC IQ).
   II. Maintain updated employee information to include employee additions, deletions, and other information.
   III. Submit a Comma Separated Value (CSV) file containing all active employee's and contractor's information including first name, last name, email address and Group/Agency before the security awareness training can be configured. File should be submitted depending on frequency of changes. Smaller agencies once a month or as needed. Larger agencies with a lot of turnover may need to submit weekly updates.
   IV. Communicate with Agency employees about the importance of training as discussed in Senate Bill (SB)553. Utilize the DoIT's security awareness training system of record to monitor, track, and report on all security awareness and role-based security training.
   V. Develop and document security awareness and training procedures to ensure agency's employees and contractors receive security awareness and training.
   VI. Ensure that all MSDE staff office employees and contractors have completed the mandatory annual security awareness training course presented in the agency's electronic training system.
   VII. Ensure that MSDE staff office employees and contractors' security awareness and role-based training completions are recorded in the system of records.

d. Agency Administrators for the System of Records shall:
   I. Ensure the number of employees and contractors are updated monthly or whenever there are changes in the system of record.
   II. Ensure training records in the system are accurate.

e. MSDE Division Heads, Managers and Supervisors at all levels shall:
   I. Complete security awareness and training as required by this policy

II. Ensure their employees and contractors complete security awareness and training as required by this policy.
III. Review and be informed of all MSDE information security policies.

f. MSDE employees and contractors shall:
   I. Complete security awareness and training as required by this policy.
   II. Review MSDE Acceptable Use Policy (AUP), Electronic Communication and Use Policy.

7. NON-COMPLIANCE

a. Any user under scope of this policy and procedures must adhere to the stipulated requirements. Any user that is non-compliant and in violation of the parameters of this policy or procedure will be considered a security incident and will require enforcement actions according to the severity and nature of the incident. Users may be considered non-compliant and under incident if:
   I. A user fails to adhere to the required awareness and training.
   II. A user fails periodic assessments.
   III. A user continually fails to carry out expected actions from awareness and training.
   IV. A user continually refuses to take required training course.

b. Any user under scope of this policy who fails to adhere to the policy may be subject to disciplinary action up to and including employment termination. Violation of any of the constraints of these policies or procedures will be considered a security breach and, depending on the nature of the violation, various sanctions will be taken:
   I. A minor breach will result in written reprimand.
   II. Multiple minor breaches or a major breach will result in suspension.
   III. Multiple major breaches will result in termination and potential legal action according to applicable laws and contractual agreements.

APPENDIX A

ACRONYMS AND ABBREVIATIONS

AD	Agency Directive
AUP	Acceptable Use Policy
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoIT	Department of Information Technology
DR	Departmental Regulation
FISMA	Federal Information System Management Act
IT	Information Technology
NIST	National Institute of Standards and Technology
MSDE	Maryland State Department of Education

APPENDIX B

Maryland Department of Information Technology, *Information Technology Security Manual*, Version 1.2, June 2019.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015.

National Institute of Standards and Technology (NIST) Special Publication (SP), Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011.

National Institute of Standards and Technology (NIST) Special Publication (SP), Building an Information Technology Security Awareness and Training Program, October 2003.

Signature: James Dale Cornelius

Email: dale.cornelius@maryland.gov

Signature: Jennifer Judkins

Email: jennifer.judkins@maryland.gov

Signature: Carol Williamson
Carol Williamson (Mar 3, 2021 11:45 EST)

Email: carol.williamson@maryland.gov