MARYLAND STATE DEPARTMENT OF EDUCATION (MSDE)

AGENCY DIRECTIVE (AD)

NUMBER:
AD 21201-002

SUBJECT:
Access Control for Information and Information Systems

EFFECTIVE DATE:
July 6, 2021

APPROVED: _____

Mohammed Choudhury
State Superintendent of Schools
Maryland State Department of Education

Section

1. PURPOSE

a. This Agency Directive (AD) establishes the Maryland State Department of Education (MSDE) policy for implementing, managing, and enforcing logical access to information systems and granting accounts the least privileges necessary to perform assigned duties or actions.

b. It is MSDE policy to comply with Federal and State requirements by establishing, implementing, and enforcing access control policies and procedures.

c. This policy complies with the requirements of the State of Maryland Department of Information Technology (DoIT), *Information Technology Security Manual and* National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*. The Access Control (AC) family of controls in the NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provide the basis for this policy.

d. This policy serves as guidance for agencies to develop and implement access control procedures that comply with State and agency requirements.

2. SPECIAL INSTRUCTION

a. This policy must be approved by the MSDE's designated Senior Executive or Authorizing Official (AO).

b. This policy must be disseminated to all MSDE personnel with IT security responsibilities within the agency.

3. BACKGROUND

a. DoIT's *State of Maryland Information Technology Security Manual* establishes the policies that define the State's IT security practices and requirements for all State of Maryland agencies. Technical Level Controls, *Access Control,* require that agencies ensure the implementation and enforcement of logical access control for all MSDE information systems.

b. To ensure consistent compliance with the DoIT Security Manual and NIST SP 800-53, access rights to all MSDE information and information systems will be based on the functional roles of users of the MSDE IT infrastructure, applications, and data. MSDE will determine an appropriate set of functional roles that adequately define user access. At a minimum, the functional roles must accommodate the following use type:

   I. Non-privileged user accounts
   II. Privileged administrator accounts
   III. Temporary, contractor and external user accounts.

c. MSDE prohibits the use of guest or anonymous accounts.

4. SCOPE

a. This Access Control Policy applies to:

   I. All MSDE employees, contractors, vendors, and partners working for or on behalf of MSDE who require access to MSDE information and/or information systems and components.
   II. All State information, in any form, collected, processed, transmitted, stored, or accessed by, or on behalf of, MSDE.
   III. All information systems or services (including cloud-based services) owned, used, or operated by MSDE, MSDE contractors, or other organizations on behalf of, or funded by, MSDE.
   IV. Interconnections between or among these information systems.

b. This Access Control policy is related to other MSDE policies and procedures, including:

   I. AD 21201-XXX, Identification and Authentication Policy, forthcoming;

II. AD 21201-XXX, Configuration Management, forthcoming; and
III. Electronic Communications and Acceptable Use Policy, August 13, 2020.

5. POLICY

a. MSDE Divisions will develop, implement, and maintain agency processes and procedures aligned with this AD to manage access to MSDE information and information systems, ensuring the procedures:
   I. Grant access only to individuals who have an established need-to-know and who meet the minimum interim or full background investigation requirements consistent with the system and level of access being requested.
   II. Include periodic validation and monitoring of accounts, roles, and privileges.
   III. Specify remedial actions for violations.
   IV. The policy will be reviewed annually and updated, if necessary.
b. Logical access controls:
   I. All MSDE information systems will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
   II. All MSDE information systems will limit access to the types of transactions and functions that authorized users are permitted to execute.
   III. All MSDE information systems will implement logical access control in accordance with State, agency, and, if applicable, Federal policies.
   IV. Restrict access to information and information systems to authorized users or subjects.

6. ACCOUNT MANAGEMENT

a. Agency will:
   I. Identify and document account types (e.g., individual, group, system, application, and temporary) that are permitted for each information system; *NOTE: Guest/Anonymous accounts are not permitted. Access is limited to individuals with a valid business purpose.*
   II. Ensure user accounts issued by MSDE are managed based on user identity and position (e.g., the user role on the information system).
   III. Assign one or more agency personnel to serve as the account manager for information system accounts, with the responsibility for authorizing account actions such creating, modifying, disabling, and deleting accounts.
   IV. Establish conditions for account, role, and group membership for each information system, adhering to the principles of least privilege for each account.
b. Account management processes will ensure that the system owner or designated representative verifies that:
   I. Account access request contains correct and accurate information.
   II. Access requirements to grant the requested access have been met.
   III. Account requests are submitted promptly to:
      1. Create accounts, add group members, and assign access privileges;
      2. Modify user accounts, group memberships, and access privileges when a user's work assignment changes the type of information or information system the user needs to access; or
      3. Disable accounts and remove group memberships when a user transfers or terminates employment, in accordance with agency procedures.
   iv. Verify that individuals have completed security awareness and training for the current fiscal year, and annually thereafter, in accordance with AD 21201-001 *Security Awareness and Training Policy*.

c. Before authorizing the requested access, account managers will:
    I. Validate the required description and justification of each account, role, or group privilege requested.
    II. Verify that individuals have agreed to abide by the system's rules of behavior and terms of use for the current fiscal year, both initially and annually thereafter.
d. Account managers will only authorize requests to create, modify, disable, or delete information system accounts or access privileges following formal authorization by the system owner, employee, or manager.
e. Agency monitoring processes will:
    I. Include audits of all accounts, groups, and roles to ensure account management procedures produce accurate and timely changes.
        a. Validate with the system owner the continued business needs for each user to access active accounts or groups and ensure that accounts and groups are disabled or removed when no longer needed; and
        b. Reconcile active accounts, groups, and roles with account or role requests, and immediately correct or revoke any accounts or privileges not approved through the account management process.
    II. The frequency for audits will be as follows:
        a. Automated mechanisms should be employed to ensure that account creation, modification, disabling, permission changes, and termination actions are audited. Also, as required, appropriate individuals must be notified (system administrators and managers);
        b. Non-privileged and privileged user accounts/groups will be reviewed at least quarterly; and
        c. Any other accounts (e.g., shared, system, service) or groups not included in Sections 6e (II) (b) at least annually.
f. All MSDE information systems will employ an automated mechanism in processes that:
    I. Disable temporary and emergency accounts within 24 hours of when they are no longer in use or when they have expired. The designated temporary access period should not exceed 30 days;
    II. Disable inactive non-privileged and privileged accounts within 60 calendar days;
    III. Disable new accounts that are not used within the first 30 days; and
    IV. Create audit records of account creation, modification, enabling, disabling, and removal actions, and notifies the account manager of these actions.
g. Ensure that user's sessions automatically logout after 15 minutes of inactivity has been reached.
h. Agency procedures will require that the credentials (e.g., password) for shared accounts be changed immediately when a member of the group is removed.

7. ACCESS ENFORCEMENT

MSDE information systems will employ mandatory access enforcement mechanisms to implement access control policies to ensure that:

a. Only authorized subjects may access objects in accordance with information system access control policies.
b. All information systems enforce assigned authorizations for logical access to the information system, that all default manufacturer passwords are changed, and that only authorized personnel are given access to the stored configuration files.
c. User access to a MSDE information system is authenticated.

8. INFORMATION FLOW ENFORCEMENT

Information systems will implement information flow control measures to:

a. Enforce where and how information can travel within an information system and between interconnected information systems;
b. Enforce remote access restrictions;
c. Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems, such as boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content;
    I. MSDE must establish information sharing terms and conditions, consistent with any trust relationships established with other organizations.
    II. MSDE (System Owner and/or Data Owner) must authorize connections from MSDE information systems to other external information systems through the use of applicable agreements such as Interagency Agreement (IA), Interconnection Security Agreements (ISA), Memoranda of Understanding (MOU), or Service Level Agreement (SLA) to document appropriate aspect of interconnections.
d. Encrypt sensitive Controlled Unclassified Information (CUI) such as Personally Identifiable Information (PII), and other protected information from being transmitted as cleartext; and
e. Prevent unauthorized communication between designated sources and destinations (e.g., individuals, devices, networks).
f. Flow control restrictions include, for example:
    I. keeping export-controlled information from being transmitted in the clear to the Internet;
    II. blocking outside traffic that claims to be from within the organization;
    III. Ensure that all device management sessions come from authorized Internet Protocol (IP) addresses / subnets from the internal network; and
    IV. limiting information transfers between organizations based on data structures and content.

9. SEPARATION OF DUTIES

MSDE will implement the following requirements for information system:

a. Define information system access authorizations to support separation of duties;
b. Effectively segregate duties between the administration functions and the auditing functions of database system;
c. Separate duties of individuals as necessary to prevent malevolent activity without collusion;
d. Enforce information system access authorizations to separate duties;
e. Ensure that privileged users permitted to manage access control functions cannot alter audit functions or audit records; and
f. Document separation of duties in the AC procedure.

10. LEAST PRIVILEGE

a. Individuals and system processes will have only the minimum privileges necessary to accomplish their assigned tasks.
b. MSDE information systems will implement the principles of least privilege, ensuring that:
    I. Principles of least privilege are applied throughout the information system lifecycle (e.g., development, implementation, operational, and disposal phases);

II. Privileged users permitted to access security functions in hardware, software, or firmware, and security relevant information will use non-privileged accounts or roles when accessing non-security features;
III. Privileged accounts and groups are only used to perform privileged job functions;
IV. MSDE information systems create audit records when a privileged command is performed, or a privileged account makes a security-related change to a MSDE information system, such as creating an account or group, assigning roles and privileges to an account or group, or changing account or group privileges; and
V. Configuration settings in MSDE information systems prevent non-privileged users and accounts from executing privileged functions, including disabling, circumventing, or altering security safeguards and countermeasures, such as performing system integrity checks or cryptographic key management activities.

11. UNSUCCESSFUL LOGIN ATTEMPTS

a. MSDE information systems will use the most current Security Technical Implementation Guide (STIG) settings to:
   I. Limit the number of unsuccessful login attempts at either the operating system level, the application level, or both;
   II. Enforce a limit of three (3) consecutive invalid login attempts by a user during a 120-minute time period; and.
   III. Automatically lock the account for a minimum of 15 minutes or lock the account/node until released by an administrator or other authorized account management personnel when the maximum number of unsuccessful attempts is exceeded. This control applies regardless of whether the login occurs via a local or network connection.
b. When the maximum number of consecutive unsuccessful login attempts is exceeded during the specified timeframe:
   I. The account, application, or client device will automatically lock and remain locked for the time specified by the STIG setting or until released by an administrator; and
   II. UNIX systems should ensure that the login delay between login prompts after a failed login is set to 4 seconds or greater.
   III. Agency may establish a process to manually unlock accounts prior to the expiration of the lockout period after sufficient user identification has been established.

12. SYSTEM USE NOTIFICATION

All Maryland information systems must:
Display an approved system use notification message or banner before granting access to the system that provides privacy and security notice consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

a. (i) The user is accessing a Maryland state information system, which may contain US government information; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized system use is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.
b. Retain the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.
c. For publicly accessible systems: (i) display the system use information when appropriate, before granting further access; (ii) display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) include a description of the authorized uses of the system in the notice given to the public users of the information system.

Warning banners are displayed when individuals log in to the information system. System use notification is for information system access that includes an interactive login interface with a human user and does not require notification when an interactive interface does not exist. The following is the official DoIT warning banner:

> **"THIS SYSTEM MAY CONTAIN U.S. GOVERNMENT INFORMATION, WHICH IS RESTRICTED TO AUTHORIZED USERS ONLY. UNAUTHORIZED ACCESS, USE, MISUSE, OR MODIFICATION OF THIS COMPUTER SYSTEM OR OF THE DATA CONTAINED HEREIN OR IN TRANSIT TO/FROM THIS SYSTEM CONSTITUTES A VIOLATION OF ARTICLE 27 §§ 45A AND 146 OF THE ANNOTATED codes OF MARYLAND, TITLE 18, USC, § 1030, AND MAY SUBJECT THE INDIVIDUAL TO CRIMINAL AND CIVIL PENALTIES PURSUANT TO TITLE 26, USC, §§ 7213(A), 7213A, AND 7431. THIS SYSTEM AND EQUIPMENT ARE SUBJECT TO MONITORING TO ENSURE PROPER PERFORMANCE OF APPLICABLE SECURITY FEATURES OR PROCEDURES. SUCH MONITORING MAY RESULT IN THE ACQUISITION, RECORDING AND ANALYSIS OF ALL DATA BEING COMMUNICATED, TRANSMITTED, PROCESSED OR STORED IN THIS SYSTEM BY A USER. IF MONITORING REVEALS POSSIBLE EVIDENCE OF CRIMINAL ACTIVITY, SUCH EVIDENCE MAY BE PROVIDED TO LAW ENFORCEMENT PERSONNEL. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING."**

Any deviation from this official banner should be approved by DoIT.

13. CONCURRENT SESSION CONTROL

Maryland information systems must limit the number of concurrent sessions for each system account to a maximum of 5 sessions. Concurrent sessions must be kept to as low as possible based on risk.

14. SESSION LOCK

Information systems typically implement session locks at the operating system level using screen savers; however, applications can also provide session locking capabilities. Users should only use session locks for short periods of inactivity and log off the system for long periods, such as at the end of the workday. Maryland information systems will be configured to ensure that after the DISA STIG specified timeframe of inactivity, an information system or client device automatically initiates a session lock to prevent further access.

a. Maryland information systems must:
   I. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
   II. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
   III. Applications must manually and automatically log the user off.

"Inactivity" is defined as only those actions which would require interaction of a user (e.g., system and application calls are not included).

b. Maryland information systems must conceal, via the session lock, information previously visible on the display with a publicly viewable image.

15. SESSION TERMINATION

Session termination ends all processes associated with a user's logical session except for those processes that the user specifically created to continue after terminating the session. Logical sessions are terminable without terminating the network session.

a. The MSDE information systems will automatically terminate and require re-authentication to re-establish a user-initiated logical session:
   I. After **15 minutes of inactivity**; and

II. After the occurrence of agency-specified conditions or trigger events.

b. COTs or Custom applications are required to terminate network connections at the end of a session or due to inactivity.

NOTE: The System Security Plan (SSP) must address variations from this guideline and applicable mitigation (if appropriate) when there are cases of anonymous access, functional and operational limitations, availability requirements and non-sensitive access.

16. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

a. MSDE will identify systems and system actions that can be performed on the information system without identification and authentication consistent with the Agency mission/business function must be documented. Access to state public information can be accessed without identification or authentication. If an information system requires a system or information to be available without identification and authentication, the information system must provide rationale and seek approval.

b. All information systems with public information must document in the security plan the use of public information.

17. REMOTE ACCESS[1] (MANAGED BY ENTERPRISE)

Remote access encompasses any connection to a MSDE information system or component originating from outside of a MSDE owned and operated network infrastructure, such as accesses for telework and mobile work.

a. Agency will establish usage restrictions, configuration/connection requirements and implementation guidance for each type of allowed remote access method and document them in the SSP.

b. Agency will authorize remote access to information systems prior to allowing such connections.

c. Agency will ensure multi-factor authentication mechanisms are employed for all remote access to the network.

d. Agency will ensure the use of an encrypted Virtual Private Network (VPN) connection is required when administrative actions are performed from external connections.

e. Agencies will ensure that MSDE information systems that allow remote access include automated monitoring capabilities to detect and control access attempts by auditing remote access connection activities on a variety of devices.

f. MSDE will ensure that remote access methods:

I. Employ NIST FIPS PUB 140-2, Security Requirements for Cryptographic Modules certified encryption and mutual authentication;

II. Route all remote access sessions through a limited number of MSDE Trusted Internet Connection network-access control points;

III. Transmit and transfer data via an encrypted VPN; and

IV. Ensure execution of privileged commands and access to security relevant information via remote access must be authorized only for compelling operational needs and the rationale for such access must be documented in the security plans of information systems.

[1] Remote Access is managed by the Department of Information Technology (DoIT), as part of the enterprise solutions.

18. WIRELESS ACCESS

Before allowing wireless connections, each wireless technology used to access a MSDE information system will:

a. Implement wireless connectivity using security algorithms, encryption, and features that are considered generally secure, including:
   I. AES encryption to secure wireless data in transit.
   II. Connectivity to wireless networks must be secured with protocols that support mutual-authentication, such as EAP-TLS.
   III. Management connectivity to the wireless infrastructure should be segregated from user connectivity.
   IV. Physical or logical separation between guest/public networks and employee/secure networks.
   V. Event logging to a centralized log management server.
b. Disable, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
c. Identify and explicitly authorize the users allowed to independently configure wireless networking capabilities.
   Note: This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.
d. Select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of organization- controlled boundaries.
   Note: This enhancement only applies to High categorization systems. If any High systems are introduced in the future this requirement will be further defined.

19. ACCESS CONTROL FOR MOBILE DEVICES AND LAPTOPS

The requirements in this section apply to MSDE-owned or MSDE-controlled client devices issued by agencies. Agency will:

a. Employ full-device encryption (FIPS 140-2) to protect the confidentiality and integrity of information on mobile devices including laptops, tablets, smart phones, etc.
b. Implement anti-malware software and firewalls.
c. Scan for misconfigurations and current and missing software updates and patches.
d. Disable unauthorized or unnecessary mobile capabilities, such as wireless and infrared device capabilities.

20. USE OF EXTERNAL INFORMATION SYSTEMS

External information systems include personally owned devices, such as bring your own device.

a. Divisions that allow bring your own device will adhere to the requirements in MSDE Acceptable Use Policy (AUP), Electronic Communication and Use Policy.
b. The requirements in this section of the policy do not apply to external information systems that access public interfaces to MSDE information systems, including publicly accessible MSDE websites.
c. Information systems managed by other governmental organizations (e.g., federal, state, local) will be considered as external information systems when they do not have an established trust relationship (e.g., memorandum of agreement or interconnection security agreement) with MSDE.
d. All non-Government furnished information systems will be treated as external information systems.

e. MSDE divisions will only permit authorized individuals to access an external information system or to process, store, or transmit organization-controlled information when an approved information system connection or processing agreement has been established with the external information system provider.

21. INFORMATION SHARING

MSDE Security Office, in coordination with System Owners, Information Owners, Business Owners, must:

a. Facilitate information sharing by enabling authorized users to determine whether access authorization assigned to the sharing partner match the access restrictions on sensitive information; and
b. Employ either automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

When it is determined that shared information is sensitive and requires additional security controls, an information sharing or similar agreement documenting security requirements and responsibilities must be signed at a minimum by the sharing partner.

22. PUBLICLY ACCESSIBLE CONTENT

Divisions must:

a. Designate individuals authorized to post information onto a publicly accessible information system.
b. Divisions will develop and implement processes to:
    I. Train authorized users to ensure that publicly accessible information does not contain non-public information;
    II. Review the proposed content of information prior to posting it onto the publicly accessible information system to ensure that non-public information is not included;
    III. Ensure only authorized users post information approved for public release; and
    IV. Review the content on the publicly accessible information system for non-public information at a minimum quarterly and remove such information, if discovered.

23. ROLES AND RESPONSIBILITIES

a. The Chief Information Officer (CIO) shall:
   Hold the agency and staff office responsible for ensuring information system implementation of access control.
b. The Deputy Chief Information Officer (DCIO) shall:
    I. Maintain oversight to ensure the agency and divisions comply with policies, procedure, and access control techniques;
    II. Ensure annual review of the access control policy; and
    III. Provide guidance and enforce the policies, procedures, processes, and checklists developed to comply with this policy.
c. MSDE System Owners[2] will:
    I. Ensure the processes to create, maintain, revoke, and verify access controls and privileges implement the security concepts of need-to-know, least privilege, and separation of duties to produce accurate and desired results, and comply with this policy;

[2] The Information System Owner (also referred to as System Owner) is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The information system owner could be a Program Manager, an Application Manager, an IT Director, or an Engineering Director.

II. Maintain information for all applicable system accounts, and ensure account deactivation when individuals no longer require access;
III. Approve the roles, accounts, groups, and appropriate privileges assigned to each to implement on information systems;
IV. Coordinate with information stewards to decide who has access to the information system and determine the types of privileges and access rights;
V. Establish criteria for authorizing and reviewing account types, privileges, roles, and account and group memberships;
VI. Ensure that MSDE information systems implement appropriate access control mechanisms, including both discretionary and mandatory access controls;
VII. Ensure assignment of, or changes to, user access and privileges to information systems are implemented only with approved authorizations;
VIII. Ensure that privileged accounts are associated with a specific user unless a shared system or service account is required and is specifically authorized;
IX. Ensure assignment of, or changes to, user access and privileges to information systems are implemented only with approved authorizations; and
X. Ensure that privileged accounts are associated with a specific user unless a shared system or service account is required and is specifically authorized.

d. Managers Supervisors will:
I. Request new, modified, or terminated access to information systems for employees and other MSDE personnel; and
II. Apply the security concepts of need-to-know, least privilege, and separation of duties when requesting creation or modification of user account accesses and privileges.
I. Defined and maintain an accurate position description for each contract position;
II. Submit, in advance of contractor work or access, the necessary information to initiate or verify the contractor's background investigation, commensurate with the sensitivity described in the position description and the systems and level of access the contractor will require;
III. Request new, modified, or terminated access for contractor personnel to information systems; and
IV. Apply the security concepts of need-to-know, least privilege, and separation of duties when requesting creation or modification of user account accesses and privileges.

e. Users will:
i. Have and maintain a current, favorably background investigation in accordance with State requirements prior to gaining access to an information system;
ii. Complete monthly securing awareness and training, per AD 21201-001, read and acknowledge acceptable use policy agreement;
iii. Notify their supervisor if an access control vulnerability or policy violation is discovered or suspected;
iv. Report any suspicious or unusual activity to their supervisor as soon as possible; and
v. Conduct remote network access activities securely and in compliance with applicable agency policies and procedures.

24. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

Section GA-8A, MSDE AUP sets forth MSDE policies and procedures on employee responsibilities and conduct regarding the use of computers and electronic communication equipment.

a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action; and

b. Disciplinary or adverse action will be affected in accordance with applicable law and regulations.
c. Staff who commit policy infractions, intentional or unintentional, including misuse of MSDE IT resources, may be subject to disciplinary actions.
These disciplinary actions may include removal. Contractor employees may have their access privileges revoked and the contract could be terminated as a result of an infraction.
In addition to disciplinary action, the staff may have access privileges revoked.
When such actions appear to be criminal in nature, the matter must be referred to the DOIT Service Desk at Service.Desk@maryland.gov, and an incident response ticket will be created.

25. POLICY EXCEPTIONS

All divisions are required to conform to this policy. If a policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the user or system into compliance with policy.

Policy waiver request memorandum will be addressed to the MSDE DCIO and submitted to MSDE.securitytraining@maryland.gov for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

APPENDIX A - DEFINITIONS

Account Types: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

Chief Information Officer (CIO): A chief information officer is the company executive responsible for the management, implementation, and usability of information and computer technologies.

Chief Information Security Officer (CISO): A chief information security officer is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Information System Security Officer (ISSO): The Information System Security Officer serves as the principal advisor to the Information System Owner (SO), Business Process Owner, and the Chief Information Security Officer (CISO)/Deputy CIO on all matters, technical and otherwise, involving the security of an information system.

Logical Access: Logical access control is a restricting virtual access to data; it consists of identification, authentication, and authorization protocols utilized worldwide to protect hardware from unauthorized access, including password programs, smart cards, or tokens to identify and screen users and access levels.

Least Privilege: Individuals and system processes will have only the minimum privileges necessary to accomplish their assigned tasks.

Privileged Account: A privileged account is a user account that has more privileges than ordinary users. Privileged accounts might, for example, be able to install or remove software, upgrade the operating system, or modify system or application configurations.

System Owner (SO): The Information System Owner (also referred to as System Owner) is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The information system owner could be a Program Manager, an Application Manager, an IT Director, or an Engineering Director.

System Use Notification: System Use Notification is an approved system use notification message or banner displayed before granting access to the system that provides privacy and security notice consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states.

APPENDIX B - ACRONYMS AND ABBREVIATIONS

AC	Access Control
AD	Agency Directive
ACL	Access Control List
AUP	Acceptable Use Policy
CIO	Chief Information Officer
COR	Contracting Officer's Representative
CUI	Controlled Unclassified Information
DCIO	Deputy Chief Information Officer
DISA	Defense Information Systems Agency
DoIT	Department of Information Technology
DR	Departmental Regulation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information System Management Act
IP	Internet Protocol
IT	Information Technology
MSDE	Maryland State Department of Education
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TLC	Technical Level Control
VPN	Virtual Private Network

APPENDIX C – AUTHORITY AND REFERENCES

Maryland Department of Education (MSDE), MSDE AUP, *Electronic Communications and Use Policy, Section GA-8A Acceptable*, August 2020

Maryland Department of Education (MSDE), AD 21201-001, *Security Awareness and Training Policy*, March 2021

Maryland Department of Information Technology (DoIT), DoIT Security Manual, *Information Technology Security Manual*, Version 1.2, June 2019

National Institute of Standards and Technology (NIST) Special Publication (SP), NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003

National Institute of Standards and Technology (NIST) Special Publication (SP), NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2021

National Institute of Standards and Technology (NIST) Special Publication (SP), FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, (includes change notices as of December 3, 2002), May 25, 2001

National Institute of Standards and Technology (NIST) Special Publication (SP), FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

National Institute of Standards and Technology (NIST) Special Publication (SP), FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

National Institute of Standards and Technology (NIST) Special Publication (SP), NISTIR 7316, *Assessment of Access Control Systems*, September 2006

National Institute of Standards and Technology (NIST) Special Publication (SP), NISTIR 7874, *Guidelines for Access Control System Evaluation Metrics*, September 2012

National Institute of Standards and Technology (NIST) Special Publication (SP), NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2021

OMB, M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

APPENDIX D – SYSTEM USE NOTIFICATION BANNER EXAMPLE

Notice! Authorized Use Only

"WARNING! WARNING! THIS SYSTEM MAY CONTAIN U.S. GOVERNMENT INFORMATION, WHICH IS RESTRICTED TO AUTHORIZED USERS ONLY.

UNAUTHORIZED ACCESS, USE, MISUSE, OR MODIFICATION OF THIS COMPUTER SYSTEM OR OF THE DATA CONTAINED HEREIN OR IN TRANSIT TO/FROM THIS SYSTEM CONSTITUTES A VIOLATION OF ARTICLE 27 §§ 45A AND 146 OF THE ANNOTATED codes OF MARYLAND, TITLE 18, USC, § 1030, AND MAY SUBJECT THE INDIVIDUAL TO CRIMINAL AND CIVIL PENALTIES PURSUANT TO TITLE 26, USC, §§ 7213(A), 7213A, AND 7431. THIS SYSTEM AND EQUIPMENT ARE SUBJECT TO MONITORING TO ENSURE PROPER PERFORMANCE OF APPLICABLE SECURITY FEATURES OR PROCEDURES.

SUCH MONITORING MAY RESULT IN THE ACQUISITION, RECORDING AND ANALYSIS OF ALL DATA BEING COMMUNICATED, TRANSMITTED, PROCESSED OR STORED IN THIS SYSTEM BY A USER. IF MONITORING REVEALS POSSIBLE EVIDENCE OF CRIMINAL ACTIVITY, SUCH EVIDENCE MAY BE PROVIDED TO LAW ENFORCEMENT PERSONNEL. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING."