29.01.03.B1.01 Information Security Procedures

Approved October 1, 2020
Revised February 1, 2022
Next Scheduled Review: February 1, 2027

Standard Administrative Procedure Summary

- The Technology Services department of the Texas Division of Emergency Management, working in partnership and strategic alignment with the Chief Information Security Officer and Security Operations Center of the Texas A&M University System, manages and protects the Division's information resources and systems in accordance with the policies set forth herein. These policies are based on requirements contained in the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202 and other reference materials. These policies apply equally to all personnel including, but not limited to, Division employees, agents, consultants, contractors, and any third-party authorized users granted access to the Division's information resources and systems.

- The objectives of Cyber Security policies are the continuous availability and integrity of the Division's systems and information. Cyber Security policies are evolving in nature, which may be continually updated to adapt with evolving threats, exploits, emerging technologies, and business requirements, and serve to inform all Division users of their responsibility to safeguard Division resources.

- Violation of these policies may result in disciplinary action up to and including termination of employees, contractors, consultants, or vendor contract relationships. Additionally, individuals may be subject to loss of access to the Division's information resources and systems, as well as civil and criminal prosecution.

Definitions

Public Data - Information that is collected and maintained by the Division and is made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required. However, Division personnel must review public data thoroughly before its release to ensure Confidential Data is not included.

Internal Use Data - Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws.

Confidential Data - Information as defined in Title 1 Texas Administration Code § 202.1 (5) that is collected and maintained by the Division that must be protected against unauthorized disclosure or public release based on state or federal law or other legal agreement.

Procedure

1) Responsibilities

    a. Technology Services Department - responsible for developing and maintaining information technology security and compliance programs and procedures, including:
        i. Developing and maintaining information security compliance documentation;
        ii. Aligning with TAMUS cyber security standards and training programs;
        iii. 3. Ensuring a highly available technology infrastructure that enables the ongoing achievement of the Division mission;
        iv. Monitoring Division network and information system activity to ensure continuous security controls and compliance;
        v. Leading and performing cyber security incident response efforts;
        vi. Analyzing and preparing for emerging cyber security threats;
        vii. Leading Division cyber security assessments and risk-reduction efforts;
        viii. Assisting Division information owners to vet third-party solutions and data sharing agreements; and
        ix. Guiding Division information owners in classifying, managing, and securing Division data

    b. Division Business Owners and Users - for adhering to Division cyber security standards and guidance, including:
        i. Authorizing user access to Division systems and data as necessary;
        ii. Notifying Technology Services of necessary changes in user access to Division systems and data;
        iii. Approving release of Division data;
        iv. Determining corrective actions resulting from system risk reduction efforts;
        v. Ensuring the overall data quality and accuracy of Division data; and
        vi. Ensuring that system and data users are informed of Division cyber security policies and data protection requirements

2) Information Security Plan

    a. Purpose - The Division CIO and Information Security Officer develop and implement a security plan that provides an overview of the security requirements and a description of the security controls in place or planned for meeting those requirements.

    b. Scope - This policy is intended to apply to the agency as a whole with the *Department of Information Resources*' "Agency Security Plan" being the "plan" indicated in this Control. (The template for this Plan is provided by the Texas

Department of *Information Resources* (DIR) in *SPECTRIM*). The Division's Chief Information Officer has the primary responsibility for the implementation of this policy.

c. Implementation – The Chief Information Security Officer shall:
    i. Develop a security plan for information systems that is consistent with the Division's enterprise architecture and defines the scope and boundaries of the Division systems infrastructure; and that describes the operational environment for the information systems;
    ii. Make the security plan available to agency staff and communicate changes to the plan as appropriate;
    iii. Review the security plan for the information systems biennially and submit report to DIR;
    iv. Update the plan to address changes to the information system, environment of operation, or issues identified during plan implementation or security control assessments; and
    v. Protect the security plan from unauthorized disclosure and modification.

3) Data Classification Procedures

a. Purpose - The purpose of the Data Classification policy is to establish a framework for properly classifying and managing data assets in accordance with TAC 202.74(b) (1) and the Texas A&M University System Data Classification Standard [Security Control RA-2]. The Division values data and is committed to protecting citizen privacy. Classifying data into organized categories ensures effective, efficient, and secure usage. Data Classification establishes the official policy and standards for classifying, managing, and securing the Division's data assets.

b. Scope - The Data Classification policy applies to all Division-owned data, personnel employed or contracted by the Division, and entities accessing Division owned data. All users must comply with this policy. This policy does not designate what data can or must be released in response to a request under the Public Information Act, subpoena, court order, discovery, or other legal processes regarding the release of Division data.

c. The following actions must be taken based upon the defined data categories:

    i. Public data must be thoroughly reviewed before its release to ensure Confidential Data is not included.
    ii. Internal Use data records and information may be considered "public" under State and Federal regulations; however, a higher level of protection and review is needed to ensure Confidential Data is not included.
    iii. Confidential data **r**equires the Division to implement specific privacy and security safeguards.

d. Data controls must ensure data assets remain protected throughout its lifecycle. Data Classification standards determine the requirements for data marking, handling, duplication, mailing, disposal, and storage.

e. Access Controls - Information owners must approve all access rights to personnel. Information owners must approve the external release of Internal Use or Confidential Data unless the release is required by law. Third parties and data sharing agreements accessing Data must be verified and compliant with Department Data Classification requirements.

4) Password Procedures

a. Purpose - User authentication is a means to control who has access to Division information resources. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This, in turn, may result in negative impacts such as loss of revenue, liability, loss of trust, or embarrassment to the agency. This policy establishes procedures for the creation, distribution, safeguarding and termination of Division user password authentication mechanisms.
b. Scope - The intended audiences are Division employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and, those individuals who need to be aware of and abide by the procedures, including all staff, contractors, consultants and vendors who may be authorized access to Division systems.

c. Passwords must be treated as Confidential information.

d. Passwords must follow these requirements:
    i. If the confidentiality of a password is in doubt, the password shall be changed immediately;
    ii. Users must change default or assigned passwords where possible;
    iii. Passwords shall be protected both in storage and in transit;
    iv. When passwords are stored, they shall be encrypted using current FIPS-validated cryptography;
    v. Passwords that must be transmitted shall be encrypted;
    vi. Temporary passwords that are transmitted for the sole purpose of establishing a new password or changing a password can be excepted from the requirement to encrypt provided it is a one-time transmission and the user must also change the password upon first logon;
    vii. Whenever possible, passwords should be stored as hashes instead of plain text passwords. Hashes should use current FIPS-approved hashing functions, be salted, and each salt should be varying across the account population; and
    viii. Forgotten passwords shall not be reissued, but rather replaced with a new password.

e. When automated password generation programs are utilized:
    i. Non-predictable methods of generation must be employed;

ii. Systems that auto-generate passwords for initial account establishment must, where possible, force a password change upon entry into the system; and
iii. Wherever possible, password management and automated password generation systems must have the capability to maintain auditable transaction logs containing information such as:
    1. Time and date of password change, expiration, and administrative reset
    2. Type of action performed; and
    3. Source system (e.g. IP and/or MAC address) that originated the change request.

f. If a password has been compromised, the event shall be reported as a security incident to IT leadership.

g. Complexity for passwords used for authentication must meet at least one of the following requirements:

i. Be at least eight characters in length;
ii. Contain the following four groups of characters: lower case letters, upper case letters, symbols or numbers;
iii. May not contain anything that can be easily associated with the account owner, such as: username, SSN, UIN, given names or nicknames, birth date, telephone number, etc.;
iv. May not be a single dictionary word or an acronym regardless of language of origin; and
v. May not be a repetitive sequence.

5) Incident Response Plan

a. Division IT will follow the TAMUS cyber security incident response process and procedures. This standard outlines the procedures that will be taken in response to incidents involving data security throughout the Division environment, including:
    i. Incident reporting
    ii. Containment
    iii. Notification
    iv. Investigation
    v. Final report/recommendations/RCA

b. Incidents involving data and/or resources classified as “Internal Use” or higher will be communicated to the Division CIO, ISO and A&M System CISO immediately upon discovery.

c. The Division and the TAMUS SOC will keep track of results and effectiveness of Division responses to security incidents in order to incorporate lessons learned, and to enhance incident response procedures.

6) Security Training

a. All Division employees and contractors must be aware of, have access to, and comply with Division information technology security policies, standards, and procedures. All new Division employees are required to participate in the course *Information Security Awareness* training. In addition, all Division employees are required to attend annual refresher information security awareness training.

7) Access Control Procedures

a. Purpose - Access to the Division's information resources is commonly controlled by a logon ID associated with an authorized account. Proper administration of these access controls is important to ensure the integrity of the Division's information and the normal business operation of agency managed and administered information resources.

b. Scope - The IT team and system business owners are responsible for ensuring that the control measures described in this policy are implemented. The intended audience for this policy includes all information resources owners and IT staff.

c. Implementation

i. An approval process is required prior to granting access authorization for an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use (Information Resource related Rules, SAPs and Texas A&M University System Cybersecurity Control Standards and the granting of authorization by IT or a specific solution's Division business owner.
ii. Each person is to have a unique logon ID and associated account
iii. Access authorization controls are to be modified appropriately as an account holder's employment or job responsibilities change.
iv. Individuals shall only have the ability to access those transactions and functions for which they are authorized.
v. Processes are required to disable logon IDs that are associated with individuals who are no longer employed by or associated with the Division. In the event that the access privilege is to remain active, Deputy Chief approval is required.
vi. All new logon IDs that have not been accessed within a reasonable period of time from the date of creation will be disabled.
vii. All network logon IDs that have not been used/accessed within a period of three months shall be disabled, and can be reenabled upon request to IT.
viii. Division solution business owners should periodically review existing accounts for compliance and remove access for users that is no longer required.
ix. Division IT should periodically review network accounts and deprovision latent accounts.
x. All Division user endpoints, including mobile devices, should be centrally managed by Division IT to ensure security and compliance.

8) User Access Review

   a. Division domain user accounts are audited by Division IT on a monthly basis. Any Division user domain account that has not logged into the Division domain in the last 90 calendar days is disabled.

Related Statutes, Policies, or Requirements

- Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202
- Texas A&M University System Policy 29.01
- Texas A&M University System Regulation 29.01.01
- Texas A&M University System Regulation 29.01.03
- Texas Division of Emergency Management Rule 29.99.01.B1

Contact Office

Texas Division of Emergency Management Office of the Chief Operating Officer
(512) 424-5353

Texas A&M University System Chief Information Security Officer
(979) 458-6433