

Texas Veterans Commission

Information Security Charter

I. Purpose

The mission of the Texas Veterans Commission (TVC) is to advocate for and provide services that will significantly improve the quality of life for Texas veterans, their families, and survivors. During carrying out of its mission the TVC collect many different types of information, including financial, medical, human resources and other personal information. The TVC values the ability to communicate and share information appropriately. Such information is an important resource of the TVC and any person who uses information collected by the TVC has a responsibility to maintain and protect this resource. Federal and state laws and regulations, as well as industry standards, also impose obligations on the TVC to protect information relating to veterans, its associates and its own staff. In addition, terms of certain contracts and TVC policy require appropriate safeguarding of information.

This Charter and the information security policies adopted by the TVC hereunder (collectively, the "Information Security Policies") define the principles and terms of the TVC's Information Security Management Program (the "Information Security Program") and the responsibilities of the members of the TVC organization in carrying out the Information Security Program. The Information Security Policies are listed in Appendix C as regularly updated.

II. Scope

The resources included in the scope of the Information Security Policies are:

- Information (as defined in Appendix A) items regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
- Information Resources (as defined in Appendix A) under the direct management control of TVC.
- The people associated with the TVC that produce and consume Information.

The Information Security Policies are TVC-wide policies that apply to all individuals who access, use or control Information and Information Resources at the TVC, including the Commissioners, the Executive Management, employees, as well as contractors, consultants and other agents of the TVC and/or individuals authorized to access Data by affiliated institutions and organizations.

III. Charter Text

The mission of the Information Security Program is to protect the confidentiality, integrity and availability of Information. Confidentiality means that Information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of Information

Texas Veterans Commission

Information Security Charter

and processing methods. Availability means ensuring that authorized users have access to Information and associated Information Resources when required.

This Charter establishes the various functions within the Information Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies. The functions are:

A. Executive Management

Executive Managers are TVC officials that include the Executive Director, Deputy Executive Director, General Counsel, Program Operations Director and the Resource Management Director and are responsible for overseeing information security for their respective areas of responsibility and ensuring compliance with all Information Security Policies. Such responsibilities include, but are not limited to:

- Ensuring that each Information Owner in their respective areas of responsibility appropriately identify and classify Data in accordance with the Data Classification Policy;
- Ensuring that each such Information Owner receives training on how to handle Data per its classification; and
- Ensuring that each Information Custodian in his/her area of responsibility provides periodic reports with respect to the inventory of Information and Information Resources used in such area to the Information Security Officer.
- Ensuring the effectiveness of the Information Security Program both by leadership support and by the appropriate allocation of resources.
- Ensuring acceptable Residual Risk levels for their respective areas of responsibility.

B. Security Management

Information Security Officer (ISO) is the officer designated by the Executive Director with the authority and the duty to administer information security requirements. Among the responsibilities of the ISO are:

- Developing and maintaining an agency-wide information security plan;
- developing and maintaining information security policies and procedures that address the agency's information security risks;
- working with Information Owners and Information Resources Owners to ensure that controls are utilized to address agency's information security risks;
- providing for training and direction of personnel with significant responsibilities for information security with respect to such responsibilities;

Texas Veterans Commission

Information Security Charter

- providing guidance and assistance to Executive Managers, Information Owners, Information Custodians, and end users concerning their responsibilities under the Information Security Program;
- ensuring that annual information security risk assessments are performed and documented by Information Owners;
- reviewing the agency's inventory of Information and Information Resources and related ownership and responsibilities;
- developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, Information Owners and Custodians, necessary to ensure the security of Information and Information Resources against unauthorized or accidental modification, destruction, or disclosure;
- coordinating the review of data security requirements, specifications, and, if applicable, third-party risk assessment of any new Information Resource or services that receive, maintain, and/or share confidential Information;
- verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data;
- reporting, at least annually, to the Executive Director the status and effectiveness of security controls; and
- informing Executive Management in the event of noncompliance the agency's Information Security Policies.

In addition to the responsibilities listed above, the Executive Managers have granted the authority to the ISO to conduct the following activities:

- Monitoring use of Information on TVC Information Resources for compliance with Information Security Policies;
- conducting vulnerability scanning of any Information Resources;
- conducting security assessments of Information Resources;
- disconnecting Information Resources that present a security risk;
- documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
- erasing all Information stored on personal Endpoints previously used for TVC business, as requested or required; and
- leading and managing the TVC Response Team in connection with any breach or compromise of Information, to the extent provided for in the TVC Information Security Breach Reporting and Response Policy.

Texas Veterans Commission

Information Security Charter

Information Owners are TVC officials that have statutory or operational authority for specified Information or Information Resources. Generally, these include TVC Program Directors and among their responsibilities are:

- Classifying Information and Information Resources under their authority in accordance with the Data Classification Policy;
- maintaining an inventory of Information and Information Resources;
- approving access to Information and Information Resources and periodically review access lists based on documented risk management decisions;
- formally assigning custody of Information or an Information Resource;
- coordinating data security control requirements with the ISO;
- conveying data security control requirements to Information Custodians;
- providing authority to Information Custodians to implement security controls and procedures;
- justifying, documenting, and being accountable for exceptions to security controls.
- The Information Owner shall coordinate and obtain approval for exceptions to security controls with the Information Security Officer; and
- participating in risk assessments.

Information Custodians are TVC personnel or third-party service provider overseen by the Information Resources Manager and responsible for implementing the Information Owner defined controls and access to Information or Information Resources. Such responsibilities include, but are not limited to:

- Implement controls required to protect Information and Information Resources based on the classification and risks specified by the Information Owner(s) or as specified by the Information Security Policies;
- provide Information Owners with information to evaluate the cost-effectiveness of controls and monitoring;
- adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;
- provide information necessary for appropriate information security training to employees; and
- ensure information is recoverable in accordance with risk management decisions.
- Maintaining an inventory of Information Resources used in their respective areas of responsibility;
- performing self-audits and reporting metrics to the ISO and monitoring assessments and appropriate corrective actions; and
- ensuring that the TVC Sanitization and Disposal of Information Resources Policy is followed.

Texas Veterans Commission

Information Security Charter

User is an individual, process, or automated application authorized to access an information resource in accordance with federal and state law, and the Information Security Policies. Among their responsibilities are:

- Use Information and Information Resources only for the purpose specified by the Information Owner and Information Security Policies;
- comply with information security controls and Information Security Policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
- formally acknowledge that they will comply with the Information Security Policies and procedures in a method determined by the Information Security Program.

IV. Compliance


Violations of the Information Security Policies shall be determined by the Information Security Officer. Violations will be reported by the ISO to the Executive Director and to the appropriate Executive Manager for corrective actions which may include: (a) the immediate suspension of computer accounts and network access; (b) mandatory attendance at additional training; (c) a letter to the individual's personnel file; (d) administrative leave without pay; (e) termination of employment; (f) civil or criminal prosecution; or (g) other actions consistent with TVC policy.

V. Version History

1.0 May 15, 2017 – Adoption

VI. Approval and Adoption

The Texas Veterans Commission Information Security Charter was approved and adopted by the Executive Director per the signature and date below. This policy is subject to periodic review and may change to supersede existing policies.



Thomas Palladino
Executive Director

5/15/2017
Date

DEFINITIONS

As used in the Information Security Program, the following terms are defined as follows unless the context clearly indicates otherwise:

Access: The physical or logical capability to view, interact with, or otherwise make use of information resources.

AES: the Advanced Encryption Standard adopted by the U.S. government.

Availability: The security objective of ensuring timely and reliable access to and use of information.

Cloud Computing: Has the same meaning as "Advanced Internet-Based Computing Service" as defined in §2157.007(a), Texas Government Code.

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Confidentiality: The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Control: A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Control Standards Catalog: The document that provides state agencies and higher education institutions state specific implementation guidance for alignment with the National Institute of Standards and Technology (NIST) SP (Special Publication) 800-53 security controls.

Covered Entity: as defined in the HIPAA Rules at 45 CFR 160.103.

Data: all items of information that are created, used, stored or transmitted and in the execution of TVC's mission and required business functions. Term is often interchangeable with Information.

Destruction: The result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

DEFINITIONS

DHCP: Dynamic Host Configuration Protocol, which is a Network protocol that enables a Server to automatically assign an IP address to a Network enabled device from a defined range of numbers (i.e., a scope) configured for a given Network.

DNS: Domain Name System, which is a protocol within the set of standards for the exchange of Data on the Internet or on a private Network. The Domain Name System translates a user-friendly domain name such as <https://www.tvc.texas.gov> into an IP address such as "168.44.248.93" that is used to identify computers on a Network.

Electronic Communication: A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (email), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the TVC wireless or wired Network, access TVC email from any local or remote location or access any institutional System either owned by the TVC or by an individual and used for TVC purposes.

EPHI: Electronic Protected Health Information.

FERPA: The Family Educational Rights and Privacy Act.

Guideline: Recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

High Impact Information Resources: Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

HIPAA: The Health Insurance Portability and Accountability Act, as amended from time to time.

HIPAA Rules: the HIPAA Privacy, Security and Breach Notifications and Enforcement Rules (45 CFR Parts 160 and 164), as amended from time to time.

HITECH: The Health Information Technology for Economic and Clinical Health Act, as amended from time to time.

Information: data items as processed, stored, or transmitted by a computer. Term often interchangeable with Data.

DEFINITIONS

Information Custodian: as defined in Section III(B) of this Charter.

Information Owner: as defined in Section III(B) of this Charter.

Information Resources: computing hardware and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit Data. As defined in §2054.003(7), Texas Government Code.

Information Resources Manager: As defined in §2054.071, Texas Government Code.

Information Security Policies: as defined in Section I of this Charter.

Information Security Program: as defined in Section I of this Charter.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications and people.

Integrity: The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

IP: Internet Protocol.

Low Impact Information Resources: Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Mobile Device: a smart/cell phone (i.e., iPhone, Blackberry, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab and other Android based tablet) or USB/removable drive.

Moderate Impact Information Resources: Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Network: electronic Information Resources that are implemented to permit the transport of Data between interconnected Endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.

DEFINITIONS

Network Security Operations Center (NSOC): As defined in §2059.001(1), Texas Government Code.

OHCA: an Organized Health Care Arrangement, which is an arrangement or relationship, recognized in the HIPAA Rules that allows two or more Covered Entities that hold themselves out to the public as participating in a joint arrangement and participate in certain joint activities to share PHI for joint health care operations purposes.

Personal Identifying Information (PII): A category of personal identity information as defined by §521.002(a)(1), Business and Commerce Code.

Procedure: Instructions to assist information security staff, custodians, and users in implementing policies, standards and guidelines.

Removable Media: CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

Residual Risk: The risk that remains after security controls have been applied.

Risk: The effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact. Risk outcomes are a consequence of Impact levels defined in this section.

Risk Assessment: The process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Risk Management: The process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures.

Risk Management Program: the combined processes of Risk Assessment, Risk Remediation and Risk Monitoring.

Risk Monitoring: the process of maintaining ongoing awareness of an organization's information security risks via the risk management program.

DEFINITIONS

Risk Remediation: the process of prioritizing, evaluating and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management process. “Risk Mitigation” or “Corrective Action Planning” is synonymous with “Risk Remediation”.

RSA: the Rivest-Shamir-Adleman Internet encryption and authentication system.

Security Incident: An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of Information or Information Resources.

Sensitive Personal Information: A category of personal identity information as defined by §521.002(a)(2), Business and Commerce Code.

Server: any computing device that provides computing services to Endpoints over a Network.

SSL: the Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.

Standards: Specific mandatory controls that help enforce and support the information security policy.

System: Server or Endpoint based software that resides on a single Server/Endpoint or multiple Servers/Endpoint and is used for TVC purposes. “Application” or “Information System” is synonymous with “System”.

System Administrator: a person who is responsible for the configuration, operation and maintenance of a System.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

User: as defined in Section III(B) of this Charter.

User ID: a User Identifier.

VPN: Virtual Private Network.

DEFINITIONS

Vulnerability Assessment: A documented evaluation containing information described in §2054.077(b), Texas Government Code which includes the susceptibility of a system to a specific attack.

APPLICABLE LAWS, REGULATIONS AND INDUSTRY STANDARDS

The federal and Texas State laws and regulations and industry standards that are applicable to TVC Information Security Program are (not an exhaustive list):

Federal

Computer Fraud and Abuse Act

<http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf>

The Digital Millennium Copyright Act

<http://www.copyright.gov/legislation/dmca.pdf>

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

The Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Information Technology for Economic and Clinical Health Act (HITECH)

<http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>

Texas State

State of Texas Executive Order RP58

Texas Administration Code (TAC) Title 1, Chapter 202

Texas Business and Commerce Code, Chapters 48 and 521

Texas Government Code, Chapters 441, 552, and 2054

Texas Penal Code, Title 7, Chapter 33 and 33A

Texas Public Information Act

Industry Standards

Payment Card Industry/Data Security Standard

<https://www.pcisecuritystandards.org/tech/>

TEXAS VETERANS COMMISSION INFORMATION SECURITY POLICIES

- Information Security Charter