Information Resources Policy & Procedures

Table of Contents

Policy Standards 1
Scope 1
Audience 1
Application of Policy Standards 1
Violations 1
Disciplinary Actions 2
Key Roles and Responsibilities 3
Information Resources Manager (IRM) 3
Information Security Officer (ISO) 3
Custodian 3
User 3
Information Resources (IR) 3
Internal Auditor 3
Security Policy Development and Maintenance 4
Introduction 4
Changing Environment 4
Technology Neutral 4
Ownership 4
Change Drivers 4
Change Process 4
Change Distribution and Notification 5
Exceptions 5
Acceptable Use 6
Introduction 6
Audience 6
Ownership of Electronic Files 6
Privacy 6
Information Resource Acceptable Use Policy 6
Incidental Use of Information Resources 7
Account Management 8
Introduction 8
Purpose 8
Audience 8
Account Management Policy 8
Administrative Access 9
Introduction 9
Purpose 9
Audience 9
Administrative/ Special Access Policy 9
Change Management 10
Introduction 10
Purpose 10
Audience 10
Policy 10
Data Backup 11
Introduction 11
Purpose 11
Audience 11
Backup Policy 11

Table of Contents

Electronic Mail (email) 12
Introduction 12
Purpose 12
Policy 12
General Guidelines 12
Other Email Rules 13
Maintenance of Email 13
Disposition of Email 13
User Responsibilities 14
Retention Requirements 14
Administrative Correspondence 14
General Correspondence 14
Transitory Information 15
Policy for TVC Email Records 15
Restrictions 15
Incident Management 16
Introduction 16
Purpose 16
Audience 16
Incident Management Practice Standard 16
Internet Use 17
Introduction 17
Audience 17
Ownership 17
Privacy 17
Internet and Intranet Usage Policy 17
Incidental Use 19
Intrusion Detection 20
Introduction 20
Purpose 20
Audience 20
Intrusion Detection Policy 20
Information Resource Privacy Policy 21
Introduction 21
Purpose 21
Audience 21
Ownership 21
Policy 21
Public Access Privacy Policy 21
Information Resource Security Policy 22
Introduction 22
Purpose 22
Audience 22
Security Standards Policy 22
Information Security Officer (ISO) 23
Security Risk Management 23
Physical Security 24
Removal of Data from Information Resources 24
Accessibility Policy 25

Table of Contents

Access by Employees with Disabilities 25
TVC Website Accessibility 25
Business Continuity Plan 26
Network Access Security 27
Introduction 27
Purpose 27
Audience 27
Policy 27
Network Configuration Policy 28
Introduction 28
Purpose 28
Audience 28
Policy 28
Password Policy 29
Introduction 29
Purpose 29
Audience 29
Policy 29
Enforced ISeC Policies 29
Physical Access 30
Introduction 30
Purpose 30
Audience 30
Physical Access Policy Checklist 30
Portable Computing 31
Introduction 31
Purpose 31
Audience 31
Security Monitoring 32
Introduction 32
Purpose 32
Audience 32
Policy 32
Security Training 33
Introduction 33
Purpose 33
Audience 33
Policy 33
Server Hardening 34
Introduction 34
Purpose 34
Audience 34
Policy 34
IR Procurement and Asset Management Policy 35
Introduction 35
Purpose 35
Audience 35
Policy 35
Software Licensing 36

Table of Contents

Introduction 36
Purpose 36
Audience 36
Policy 36
Viruses and Threats 37
Introduction 37
Purpose 37
Audience 37
Virus Detection Policy 37
Technology Lease vs. Purchase Policy 38
DIR Policy Standard Reference Table 40
TVC Information Systems Security Agreement 44

Policy Standards

Scope

The Information Resources (IR) Security Policy Standards apply to all information obtained, created, or maintained by the TVC's automated Information Resources. These Policy Standards are based on the interpretation of TAC 202 and other reference material and apply equally to all levels of management and to the personnel they supervise. Further, these Policy Standards apply to all information generated by the TVC's Information Resources functions, through the time of its transfer to ownership external to the TVC or its proper disposal/destruction.

Audience

These Policy Standards apply equally to all personnel including, but not limited to, the TVC's employees, agents, consultants, volunteers, and all other authorized users granted access to Information Resources.

Application of Policy Standards

TVC will protect the Information Resources assets of the state of Texas in accordance with the state of Texas Department of Information Resources' (DIR) Information Resources Security and Risk Management Policy, Standards and Guidelines as published in the Texas Administrative Code, Chapter 202, and as authorized by the Information Resources Management Act (Chapter 2054, Texas Government Code Annotated).

Specifically, the TVC will apply policies, procedures, practice standards, and guidelines to protect its IR functions from internal data or programming errors and from misuse by individuals within or outside the TVC. This is to protect the TVC from the risk of compromising the integrity of state programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

All TVC Information Resources security programs will be responsive and adaptable to changing technologies affecting Information Resources.

Violations

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of IR constitutes a breach of security and confidentiality. Violations may include, but are not limited to any act that:

- exposes TVC to actual or potential monetary loss through the compromise of Information Resources security,
- involves the disclosure of sensitive or confidential information or the unauthorized use of TVC data or resources, and
- involves the use of Information Resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the TVC.

Policy Standards

Disciplinary Actions

Violation of these Policy Standards may result in immediate disciplinary action that may include, but may not be limited to:

- formal reprimand,
- suspended or restricted access to TVC Information Resources,
- restitution or reimbursement for any damage or misappropriation of any TVC property,
- suspension without pay,
- termination of employment,
- termination of contract,
- civil prosecution, state and/or federal criminal prosecution

Key Roles and Responsibilities

Information Resources Manager (IRM)

Responsible to the State of Texas for management of the TVC's information resources. The designation of an TVC information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state TVC's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the TVC. If the TVC does not designate an IRM, the title defaults to the TVC's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO)

Responsible to the IRM for administering the information security function within the TVC. The ISO is the TVC's internal and external point of contact for all information security matters.

Custodian

Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications, Information Resources is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User

The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security and has the responsibility to:

- Use the resource only for the purpose specified by the owner,
- Comply with controls established by the owner, and
- Prevent disclosure of confidential or sensitive information.

Information Resources (IR)

The name of the TVC function responsible for computers, networking, and data management.

Internal Auditor

Ensures that the TVC's information resources are being adequately secured, based on risk management, as directed by the IRM acting on delegated authority for risk management decisions.

Security Policy Development and Maintenance

Introduction

The TVC Information Security Policy Standards are the foundation for the Information Security Program. These standards have been developed by interpreting HIPAA, TAC 202 and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment.

Changing Environment

The business, technical, cultural, and legal environment of TVC, as it relates to information resources use and security, is constantly changing. The Security Policy Standards are revised as required to comply with changes in law or administrative rules or to enhance its effectiveness.

Technology Neutral

These Policy Standards are technology neutral and apply to all aspects of information technology. It is possible however, that emerging technologies or new legislation could affect these standards in the future.

Ownership

The TVC Information Resources Manager (IRM) owns the Security Policy Standards.

Change Drivers

A number of factors could result in the need or desire to change the Security Policy standards. These factors include, but are not limited to:

- Review schedule
- New legislation
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Change Process

Updates to the TVC Information Security Policy Standards, which include establishing new policy standards, modifying existing policy standards, or removing policy standards, can result from two different processes:

- Biannual review corresponding with the end of a legislative session. The IRM, or designate, will review the Policy Standards for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

Security Policy Development and Maintenance

- Any User may propose the establishment, revision, or deletion of any policy principle at any time. Proposals are directed to the IRM.

Change Distribution and Notification

Once a change to the Security Policy Standards has been approved by the IRM the following steps must be taken to properly document and communicate the change:

- The appropriate TVC web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change
- The changes will be communicated using standard TVC communications methods.

Exceptions

The TVC Security Policy Standards set the security strategy for TVC at a very high level and are technology neutral. As such, there is no need for an exception process for the Security Policy Standards.

Acceptable Use

Introduction

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Audience

The TVC Acceptable Use policy applies equally to all individuals granted access privileges to any TVC Information Resources.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of TVC are the property of TVC.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of TVC are not private and may be accessed by TVC IR employees at any time without knowledge of the Information Resources user or owner. Appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards, may access electronic file content.

Information Resource Acceptable Use Policy

- Users must report any weaknesses in TVC computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on TVC systems for which they do not have authorization or explicit consent.
- Users must not share their TVC account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Users must not make unauthorized copies of copyrighted software.
- Users must not use non-standard shareware or freeware software without TVC Information Resources management approval unless it is on the TVC standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized TVC user access to a TVC resource; obtain extra resources beyond those allocated; circumvent TVC computer security measures.

Acceptable Use

- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, TVC users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on TVC Information Resources.
- TVC Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material that TVC may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the TVC official processes for dealing with academic ethical issues).
- Access to the Internet from a TVC owned, home based computer must adhere to all the same policies that apply to use from within TVC facilities. Employees must not allow family members or other non-employees to access TVC computer systems.
- Users must not otherwise engage in acts against the aims and purposes of TVC as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use of Information Resources

As a convenience to the Texas Veterans Commission user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Texas Veterans Commission approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Texas Veterans Commission.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, the Texas Veterans Commission.
- Storage of personal email messages, voice messages, files and documents within Texas Veterans Commission's Information Resources must be nominal.

Account Management

Introduction

Computer accounts are the means used to grant access to TVC Information Resources. These accounts provide a means of providing accountability, a key to any computer security program for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of the TVC Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience

The TVC Account Management Security Policy applies equally to all individuals with authorized access to any TVC Information Resources.

Account Management Policy

- All users must sign the ***TVC Information Systems Security Agreement*** before receiving a computer account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the TVC Password Policy.
- All accounts must have a password expiration that complies with the TVC Password Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- Information Resources document requests for account activation and termination in the *Employee Account Activation-Termination Request Log*.
- The TVC Information Security Officer (ISO) reconciles both network and email accounts against actual employee status on an annual basis and takes appropriate action when needed.
- System Administrators or other designated staff are responsible for:
  - Removing the accounts of individuals that change roles within TVC or are separated from their relationship with TVC.
  - Modifying user accounts to accommodate situations such as name changes, accounting changes and permission changes.

Administrative Access

Introduction

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

Purpose

The purpose of the Administrative Access Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

Audience

The TVC Administrative/Special Access Practice Standard applies equally to all individuals that have, or may require, special access privilege to any TVC Information Resources.

Administrative/ Special Access Policy

- All users must sign the ***TVC Information Systems Security Agreement*** before access is given to an account.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the ISO.
- Each account used for administrative/special access must meet the TVC Password Policy.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
  - must be authorized,
  - must be created with a specific expiration date, and
  - must be removed when work is complete.

Change Management

Introduction

The Information Resources infrastructure at TVC is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time, each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure

Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

Audience

The TVC Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

Policy

- Every change to a TVC Information Resources resource such as operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.
- Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
  - Date of change,
  - Nature of the change,
  - Indication of success or failure, and
  - All TVC information systems must comply with an Information Resources change management process that meets the standards outlined above.

Data Backup

Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

Purpose

The purpose of the TVC Backup/DRP Policy is to establish the rules for the backup and storage of electronic TVC information.

Audience

The TVC Backup/DRP Policy applies to all individuals within the TVC enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security, and data owners.

Backup Policy

TVC servers are located at the Austin Data Center which is managed by IBM.

Server (network) backups are addressed as follows:

- A complete server backup is performed at the beginning of each month. This monthly backup is stored offsite and retained for 1 year. The backup is performed on all physical and logical disk drives.
- A partial server (network) backup of all new or modified files is performed each night. The most recent 60 versions of a file are retained.
- **Desktop and laptop computers are not backed up.**
- All work related files must be saved to network drives. Network drives are drives G:\ and greater.

Server backups are tested at quarterly. A successful restore of a ‘production user file restore request’ can represent a successful quarterly backup test.

Electronic Mail (email)

Introduction

This policy applies to email used within the agency and email used conjointly with the internet, and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. Generally, email should be used only for legitimate state business; however, brief and occasional email messages of a personal nature may be sent and received if the following conditions are met.

Purpose

The purpose of the Electronic Records Management policy is to instruct users of electronic resources on the appropriate use of email and the retention of electronic records.

Policy

It is the policy of the Texas Veterans Commission to provide efficient, economical and effective management of email records in accordance with Texas Administrative Code (TAC), Chapter 13, Sections 6.91-6.97 (State Agency Bulletin Number One, Electronic Records Standards and Procedures). TAC Chapter 13, Section 6.92(c), provides that the agency head or designated records management officer must administer a program for the management of records created, received, retained, used, or disposed on electronic media.

The Texas Veterans Commission desires to adopt a policy for that purpose and to prescribe guidelines and procedures for the management of email consistent with Electronic Records Standards and Procedures and in the interest of cost-effective and efficient recordkeeping, including long-term records retention for the Archives of the State.

This policy applies to any email messages created, received, retained, used, or disposed of using TVC email system.

General Guidelines

Personal use of email is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. Employees need to keep in mind that all email is recorded and stored along with the source and destination. Management has the ability and right to view employee email. Recorded email messages are the property of the agency and therefore the taxpayers of the State of Texas. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to State records retention. Employees should be aware that when sending an email message of a personal nature, there is always the danger of the employees' words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal email, especially if the content of the email could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message:

Electronic Mail

"This email contains the thoughts and opinions of (employee name) and does not represent official TVC policy."

If the content of the email contains sensitive or confidential information, the employee may use the following message at the end of the message:

"This message contains information which may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply email and delete the message."

Other Email Rules

- Do not provide a work email address to non-work related Internet sites, surveys or list-servers.
- Do not forward work email to a personal mail account.
- Discourage others from sending non-business email.
- Ensure that personal email does not interfere with TVC's mission or operation.
- All TVC email messages are the property of TVC and are subject to the Public Information Act, Texas Government Code, Chapter 552.
- Do not use email for sending or forwarding chain letters.
- Do not use email to send, receive or forward sexually oriented or pornographic materials.
- Do not use email to send, receive or forward objectionable language.
- Do not use email to solicit for outside or commercial ventures, religious or political causes, outside organizations or organizations that are not job related.
- Do not use email for any personal monetary interests or gain

Maintenance of Email

Records created using an email system may be saved for their approved retention period by one of the following:

- Print message and file in appropriate hard copy file
- Place in folders and save on personal network drive

Whichever method is chosen, the record must be readable and/or in a format that does not require the use of email software.

Disposition of Email

The process for the legal disposition of state records (including email) is subject to the same documentation requirements as any other format or medium. This usually requires agency permission and some type of disposition log to adequately document disposition and destruction of electronic records. Section 6.95 of the Electronic Records Standards and Procedures (relating to the Final Disposition of Electronic State Records) states that:

Electronic Mail

An electronic state record that is an archival record must be maintained by the agency through hardware and software migrations and upgrades as authentic evidence of the state's business in accessible and searchable form, except as otherwise determined by the state archivist.

A state agency must establish and implement procedures that address the disposition of an electronic mail record by staff in accordance with its approved records retention schedule and, specifically, must establish guidelines to enable staff to determine if an electronic mail record falls under transitory information (records series item number 1.1.057) on the agency's approved records retention schedule in order to encourage its prompt disposal after the purpose of the record has been fulfilled.

User Responsibilities

It is the responsibility of the user of the email system to manage email messages according to the agency's retention schedule.

It is the responsibility of the sender of email messages within the agency's email system and recipients of messages from outside the agency to retain the messages for the approved retention period.

Names of sender, recipient, date/time of the message, as well as any attachments must be retained with the message. Except for listserv mailing services, distribution lists must be able to identify the sender and recipient of the message.

Retention Requirements

The TVC approved retention schedule lists the record series that are created and the retention period for each series. It is the content and function of an email message that determines the retention period for that message. All email sent or received by an agency is considered a state record. Therefore, all email messages must be retained or disposed of according to the agency's retention schedule. Email systems must meet the retention requirements found in TAC 6.94(e).

Email generally, but not always, falls into several the following series categories. These are:

Administrative Correspondence
Incoming/outgoing and internal correspondence, in any format, pertaining to the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services, or projects of an agency and the administrative regulations, policies and procedures that govern them. Subject to Archival review. Retention: 2 years.

General Correspondence
Non-administrative incoming/outgoing and internal correspondence, in any media, pertaining to or arising from the routine operations of the policies, programs, services, or projects of an agency. Retention: 2 years.

Electronic Mail

Transitory Information
Records of temporary usefulness that are not an integral part of a records series of TVC; that are not regularly filed within TVC's recordkeeping system; and that are required only for a limited time for the completion of an action by an official or employee of the agency or in the preparation of an on-going records series. Transitory records are not essential to the fulfillment of statutory obligations or to the documentation of agency functions. Examples of transitory information are routine messages (can be recorded on any medium, such as hard copy message slips or in an electronic format on email and voice mail). Retention: Purpose of record fulfilled.

The vast majority of email messages sent and received by TVC employees are transitory information. When the purpose of a transitory email record is fulfilled, the user must delete the email from both Sent and Received Outlook folders. The Outlook user should also “Purge All Messages Marked for Deletion” on at least a monthly basis. Information Resources will assist employees as needed.

Policy for TVC Email Records

The TVC email system is not to be used as a filing or storage system for documents that are an integral part of a TVC record series. Users are responsible for determining what documents meet this criteria and saving those documents in another form (described in ‘Maintenance of Email’) outside the email system.

Restrictions

Personal email should not impede the conduct of state business. Racist, sexist, threatening, or otherwise objectionable language is strictly prohibited. Email should not be used for any personal monetary interests or gain. Employees should not subscribe to mailing lists or mail services strictly for personal use. Personal email should not cause the state to incur a direct cost in addition to the general overhead of email.

Incident Management

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

Audience

The TVC Incident Management Policy applies equally to all individuals that use any TVC Information Resources.

Incident Management Practice Standard

- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The ISO will take appropriate action to block email, internet access, and/or network access to reduce the spread of an incident.
- The ISO will determine if a widespread TVC communication is required, the content of the communication, and how best to distribute the communication.
- The TVC ISO is responsible for reporting the incident to the:
  - Department of Information Resources as outlined in TAC 202
  - Local, state or federal law officials as required by applicable statutes and/or regulations
- The IRM is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the Executive Director.
- In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and TVC.

Internet Use

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.
- To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

Audience

The TVC Internet Use Policy applies equally to all individuals granted access to any TVC Information Resource with the capacity to access the internet, the intranet, or both.

Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered or otherwise under the custody and control of TVC are the property of TVC.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of TVC are not private and may be accessed by TVC IR employees at any time without knowledge of the Information Resources user or owner. Appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards, may access electronic file content.

Internet and Intranet Usage Policy

- Software for browsing the Internet is provided to authorized users for business and research use only.
- All software used to access the Internet must be part of the TVC standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.
- All files downloaded from the Internet must be scanned for viruses using the approved IR distributed software suite and current virus detection software.
- All sites accessed must comply with the TVC Acceptable Use Policies.
- All user activity on TVC Information Resources assets is subject to logging and review.
- Content on all TVC Web sites must comply with the TVC Acceptable Use Policies.
- No offensive or harassing material may be made available via TVC Web sites.
- Business related purchases are subject to TVC procurement rules.
- No personal or commercial advertising may be made available via TVC Web sites.
- TVC internet access may not be used for personal gain or non-TVC personal solicitations.

Internet Use

- No TVC data will be made available via TVC Web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive TVC material transmitted over external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.
- All authorized users of state networks or systems must use the Internet facilities in ways that do not disable, impair, or overload performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another user.
- Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.
- Written permission is required from the employee's supervisor and must be approved by the TVC IRM to act outside of the normal Internet Use Policy. Access is limited to provide for professional activities and career development over the internet and the activities should be included in the employee's job description.
- Written specific authorization from the employee's immediate supervisor is required before the employee represents the TVC in news groups or chat rooms on the state network, state network users may participate in news groups or chat rooms in the course of business when relevant to their duties, but they should do so as individuals speaking for themselves and must include a disclaimer in their comments similar to the following: This message contains the thoughts and opinions of [employee name] and does not represent official TVC policy.
- Users of state computers or networks shall not download/install or use any peer-to-peer software on state computers, networks, or mobile computing device (PDA) without specific authorization in writing from the TVC IRM.
- State employees, contractors, and network users must not send, forward, store, or receive confidential agency information on unapproved mobile devices, such as two-way pagers, personal digital assistants (PDAs), or cell phones. State agency-approved mobile devices may receive and store confidential information in encrypted, password-protected form.
- Email that contains an individual's name along with any restricted personal information (e.g., Social Security number) will be encrypted for transmission and storage.
- All users of state networks and systems should be aware that when sending an email message or other electronic transmission of a personal nature, there is the danger of the employee's words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal email, especially if the content of the email could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message: "This email contains the thoughts and opinions of [employee name] and does not represent official TVC policy.

Internet Use

- Do not use Instant Messaging (IM) to conduct any state business that would require the content to be saved as a state record. IM may not be used to document a statutory obligation or agency decision, and IM should not be used when the resulting record would normally be retained for recordkeeping purposes.
- If any copied or transferred data or information from a peer-to-peer network is licensed or copyrighted, the authorized network user shall ensure that all notifications and costs are documented and approved.

Incidental Use

TVC allows limited personal use of the internet. However, it is limited to the employee's non-work time, it must not interfere with the agency's mission or operation and it cannot violate standards of ethical conduct. Access to the Internet is a privilege that may be revoked at any time for inappropriate use or conduct including use that violates other applicable agency policies. Inappropriate use or conduct includes but is not limited to:

- Use of the Internet for unlawful or malicious activities;
- Misrepresenting a personal communication as a communication in the employee's official capacity;
- For viewing or printing offensive, sexually oriented or pornographic materials;
- Soliciting for outside or commercial ventures, religious or political causes, outside organizations, or other organizations that are not job related;
- Activity which causes congestion and disruption of networks and systems is prohibited.

Intrusion Detection

Intrusion Detection

Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Audience

The TVC Intrusion Detection Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resources Security.

Intrusion Detection Policy

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be enabled.
- Audit logs from the perimeter access control systems must be monitored or reviewed by the ISO.
- System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
- Audit logs for servers and hosts on the internal, protected, network must be reviewed on a routine basis by the ISO.
- Host based intrusion tools will be checked on a routine basis.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy.
- Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the ISO.

Information Resource Privacy Policy

Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of TVC Information Resources. Internal users should have no expectation of privacy with respect to Information Resources. External users should have the expectation of complete privacy, except in the case of suspected wrongdoing, with respect to Information Resources.

Purpose

The purpose of the TVC Information Resources Privacy Policy is to communicate the TVC Information Resources Privacy expectations to Information Resources users.

Audience

The TVC Information Resources Privacy Policy applies equally to all individuals who use any TVC Information Resource.

Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered or otherwise under the custody and control of TVC are the property of TVC.

Policy

- Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of TVC are not private and may be accessed by TVC IR employees at any time without knowledge of the IR user or owner.
- To manage systems and enforce security, TVC may log, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these purposes, TVC may also capture User activity such as telephone numbers dialed and web sites visited.
- A wide variety of third parties have entrusted their information to TVC for business purposes, and all workers at TVC must do their best to safeguard the privacy and security of this information.
- Users must report any weaknesses in TVC computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on TVC systems for which they do not have authorization or explicit consent.

Public Access Privacy Policy

TVC web sites available to the public must contain a Privacy Statement.

Information Resource Security Policy

Introduction

Security policies establish the requirements for protection of the information assets in custody of the TVC.

Purpose

The purpose of the TVC Information Resources Security Policies is to clearly communicate the TVC Information Resources Security expectations to Information Resources users.

Audience

The TVC Information Resources Security Policy applies to all individuals who use any TVC Information Resource.

Security Standards Policy

Information resources residing in The Texas Veterans Commission (TVC) are strategic and vital assets belonging to the people of Texas. These assets must be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to TVC information resources must be appropriately managed.

The TVC is required to have an information resources security program consistent with these standards:

- The Executive Director is responsible for the protection of information resources.
- All individuals are accountable for their actions relating to information resources.
- Information resources shall be used only for intended purposes as defined by the TVC and consistent with applicable laws.
- Risks to information resources must be managed.
- The expense of security safeguards must be commensurate with the value of the assets being protected.
- The integrity of data, its source, its destination, and processes applied to it must be assured.
- Changes to data must be made only in an authorized manner.
- Information resources must be available when needed.
- Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.
- Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

The TVC must ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

Information Resource Security Policy

Information Security Officer (ISO)

The TVC Executive Director or his designated representative shall designate an Information Security Officer (ISO) to administer the TVC information security program. The ISO shall report to executive level management.

It shall be the duty and responsibility of this individual to develop and recommend policies and establish procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction, or disclosure.

The ISO shall document and maintain an up-to-date information security program. The information security program must be approved by the TVC Executive Director or his or her designated representative(s).

The Information Security Officer is responsible for monitoring the effectiveness of defined controls for mission critical information.

The Information Security Officer shall report, at least annually, to the TVC Executive Director or his or her designated representative(s) the status and effectiveness of information resources security controls.

A review of the TVC's information security program for compliance with these standards will be performed at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the TVC Executive Director or his or her designated representative(s).

Security Risk Management

The TVC IRM will perform a risk analysis per the following schedule.

The inherent risk and frequency of the security risk analysis will be ranked, at a minimum, as either "High," "Medium," or "Low," based primarily on the following criteria:

High Risk (Annual assessment)-Information resources that;

A. Involve large dollar amounts or significantly important transactions, such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately, or
B. Contain confidential or sensitive data such that unauthorized disclosure would cause real damage to the parties involved, or
C. Impact a large number of people or interconnected systems.

Medium Risk-biennial assessment--Information resources that;

A. Transact or control a moderate or low dollar value, or
B. Data items that could potentially embarrass or create problems for the parties involved if released, or
C. Impact a moderate proportion of the customer base.

Low Risk-biennial assessment--Information resources that;

A. Publish generally available public information, or
B. Result in a relatively small impact on the population.

Security risk assessment results, vulnerability reports, and similar information shall be

documented and presented to the TVC Executive Director or his or her designated representative. The TVC Executive Director or his or her designated representative(s) shall make the final security risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The TVC Executive Director or his or her designated representative(s) must approve the security risk management plan. This information may be exempt from disclosure under §2054.77(c), Government Code

Physical Security

Physical access to mission critical information resources facilities shall be managed and documented by the TVC Information Security Officer (ISO).

The ISO shall review physical security measures for information resources annually and report the results to the TVC IRM.

Mission critical information resources shall be protected from environmental hazards to the extent financial resources allow. The ISO shall monitor environmental control procedures and equipment and shall be trained in the desired response in case of emergencies or equipment problems.

Written emergency procedures shall be developed, updated, and tested at least annually. The TVC will refer to the State Office of Risk Management for applicable rules and guidelines

Removal of Data from Information Resources

TVC complies with the requirements and procedures addressing the sale or transfer of data processing equipment in §403.278, Government Code (between institutions of higher education or state agencies) or Chapter 2175, Government Code (for all other transactions).

Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, the TVC Information Security Officer (ISO) shall assess whether to remove data from any associated storage device.

Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the TVC shall retain a hard copy or other electronic copy of the record for the required retention period.

If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are provided in the "Sale or Transfer of Computers and Software" guidelines available at http://www.dir.state.tx.us.

The TVC ISO shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:

1. date
2. description of the item
3. serial number
4. inventory number
5. the process and sanitization tools used to remove the data or method of destruction
6. the name and address of the organization receiving the equipment.

Accessibility Policy

Access by Employees with Disabilities

The TVC shall take all reasonable steps to ensure that agency employees with disabilities have comparable access to information technology as employees without disabilities.

The Executive Director shall have authority to determine what constitutes “reasonable steps” on a case-by-case basis.

TVC Website Accessibility

The TVC shall take all reasonable steps to ensure that members of the public with disabilities have comparable access to agency information located on the World Wide Web as people without disabilities.

The Executive Director shall have authority to 1) determine what constitutes “reasonable steps” on a case-by-case basis, and 2) grant exceptions to this policy as allowed by Govt. Code Section 2054.460.

Business Continuity Plan

The TVC has developed a Business Continuity Plan for all agency operations. Included in that plan are procedures applicable to information resources.

Elements of the Plan for information resources include:
1) Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis address' maximum tolerable downtime for time-critical support services and resources including:

- Personnel;
- Facilities;
- Technology platforms (all computer systems);
- Software;
- Information resources security utilities;
- Data networks and equipment;
- Vital electronic records and/or data.

2) Security Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

3) Recovery Strategy to appraise recovery alternatives and alternative cost-estimates, which are presented to management.

4) Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the Plan.

5) Disaster Recovery Plan—the TVC maintains a written disaster recovery plan for information resources. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan.

The disaster recovery plan:

- Contain measures that address the impact and magnitude of loss or harm that will result from an interruption;
- Identify recovery resources and a source for each;
- Contain systematic instructions for implementing the Plan;
- Be maintained to ensure currency; and
- Be tested either formally or informally at least annually.

Mission critical data shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized TVC representatives.

Network Access Security

Introduction

The TVC network infrastructure is provided as a central utility for all users of TVC Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet TVC demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the TVC Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of TVC information.

Audience

The TVC Network Access Policy applies equally to all individuals with access to any TVC Information Resource.

Policy

- Users are permitted to use only those network addresses issued to them by TVC IR.
- Remote users may connect to TVC Information Resources only through an ISP and using protocols approved by TVC.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the TVC network without TVC IR approval.
- Users must not install network hardware or software that provides network services without TVC IR approval.
- Non-TVC computer systems that require network connectivity must conform to TVC IR Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, TVC users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the TVC network infrastructure.
- Users are not permitted to alter network hardware in any way.

Network Configuration Policy

Introduction

The TVC network infrastructure provides a central utility for all users of TVC Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continue to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the TVC Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of TVC information.

Audience

The TVC Network Configuration Policy applies equally to all individuals with access to any TVC Information Resource.

Policy

- TVC Information Resources owns and is responsible for the TVC network infrastructure and manages further developments and enhancements to this infrastructure
- To provide a consistent TVC network infrastructure capable of exploiting new networking developments, all cabling must be installed by TVC IR or an approved contractor.
- All network-connected equipment must be configured to a specification approved by TVC IR.
- All hardware connected to the TVC network is subject to TVC IR management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of TVC IR.
- The TVC network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by TVC IR.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by TVC IR.
- The use of departmental firewalls is not permitted without the written authorization from TVC IR.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the TVC network without TVC IR approval.
- Users must not install network hardware or software that provides network services without TVC IR approval.
- Users are not permitted to alter network hardware in any way.

Password Policy

Introduction

User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to TVC.

Purpose

The purpose of the TVC Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the TVC user authentication mechanisms.

Audience

The TVC Password Policy applies equally to all individuals who use any TVC information resource.

Policy

- TVC passwords are governed by Information Security Controls (ISeC) established by the Department of Information Resources (DIR) and controlled by Windows Active Directory (AD) Group Policy.
- User account passwords must not be divulged to anyone. TVC IR and IR contractors will not ask for user account passwords.
- If the security of a password is in doubt, the password must be changed immediately.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the TVC ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the passwords and protect them.
  - Report the discovery to the TVC IRM.
  - Transfer the passwords to an authorized person as directed by the TVC ISO

Enforced ISeC Policies

- Passwords must be changed at least every 90 days and cannot be changed for 7 days after a password change.
- Passwords must have a minimum length of 8 characters and contain at least 3 of the following: lower case letter, upper case letter, number, or special character.
- A password history of 8 passwords is maintained preventing password reuse.
- A password protected screen saver executes after 30 minutes of computer inactivity.

Physical Access

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.

Purpose

The purpose of the TVC Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The TVC Physical Access Policy applies to all individuals within the TVC enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security and data owners

Physical Access Policy Checklist

- All physical security systems must comply with applicable all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Resources restricted facilities must be documented and managed.
- All IR facilities must be physically protected in proportion to the criticality or importance of their function at TVC.
- Access to Information Resources facilities must be granted only to TVC support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.
- Requests for access must come from the applicable TVC data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.
- The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within TVC or are separated from their relationship with TVC.
- Visitors are escorted in card access controlled areas of Information Resources facilities.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location must be displayed.

Portable Computing

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices

Purpose

The purpose of the TVC Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of TVC information.

Audience

The TVC Portable Computing Security Policy applies equally to all individuals that utilize Portable Computing devices and access TVC Information Resources

Policy

- Only TVC approved portable computing devices may be used to access TVC Information Resources.
- Administrative access to portable computing devices must be password protected.
- Confidential, proprietary, or sensitive TVC data shall not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive TVC data must be encrypted using IR approved encryption techniques.
- TVC data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- Non-TVC computer systems that require network connectivity must conform to TVC IR Standards and cannot access TVC Local Area Networks (LAN).
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Security Monitoring

Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files

Purpose

The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning.

Audience

The TVC Security Monitoring Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

Policy

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible tools will report exceptions. These tools could be deployed to monitor:
  - Internet traffic
  - LAN traffic, protocols, and device inventory
  - Operating system security parameters
- The following files may be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
  - Automated intrusion detection system logs
  - Firewall logs
  - User account logs
  - Network scanning logs
  - System error logs
- The following checks may be performed as needed:
  - Unauthorized network devices
  - Unauthorized personal web servers
  - Unsecured sharing of devices
  - Operating System and Software Licenses

Any security issues discovered will be reported to the ISO for follow-up investigation.

Security Training

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific, and training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Training Policy is to describe the requirements for ensure each user of TVC Information Resources is receives adequate training on computer security issues.

Audience

The TVC Security Training Policy applies equally to all individuals that use any TVC Information Resources.

Policy

- The TVC Executive Director delegates his authority to the IRM to review and approve ownership of information resources and their associated responsibilities.
- All users must sign the TVC Information Security Acknowledgement and understand TVC requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect TVC information resources.
- IR will communicate new computer security program information, security bulletin information, and security items of interest as they become available and applicable.
- ISO will present security training at the TVC fall or spring conference on an annual basis.

Server Hardening

Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service

Purpose

The purpose of the TVC Server Hardening Policy document is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

Audience

The TVC Server Hardening Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security

Policy

- A server must not be connected to the TVC network until it is in a TVC IR accredited secure state and the network connection is approved by TVC IR.
- The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for TVC IR accreditation. Some of the general steps included in the Server Hardening Procedure include:
  - Installing the operating system from an IR approved source
  - Applying vendor supplied patches
  - Removing unnecessary software, system services, and drivers
  - Setting security parameters, file protections, and enabling audit logging
  - Disabling or changing the password of default accounts
- TVC IR will monitor security issues, both internal to TVC and externally, and will manage the release of security patches on behalf of TVC.
- TVC IR will test security patches against IR core resources before release where practical.
- TVC IR may make hardware resources available for testing security patches in the case of special applications.
- Security patches must be implemented within the specified timeframe of notification from TVC IR.

IR Procurement and Asset Management Policy

Introduction

The procurement and tracking of all information resource assets such as computers, software, and services is the responsibility of the TVC IRM.

Purpose

The IR Procurement and Asset Management Policy establishes a standard approach for purchasing and tracking IR assets. The policy allows the IRM and the TVC Property Manager to capture fixed asset information for assets shipped to Austin HQ and assets shipped directly to field office locations.

Audience

The IR Procurement and Asset Management Policy applies equally to all individuals that use TVC Information Resources.

Policy

- The TVC IRM will initiate and approve all requisitions for information resource hardware, software, and services.

- The IRM's approval (signature) is required on all IR purchase requisitions.

- The Finance Division will forward scanned or paper copies of the all IR invoices to the TVC IRM upon receipt. The IRM will log pertinent information from the invoice into the Information Resource Asset Database and forward them to the TVC Property Manager.

- Finance will forward a scanned or paper copy of all IR purchase orders to the IRM as they are processed. IR will update the Information Resource Asset Database and forward them to the TVC Property Manager for entry into the Statewide Property System (SPA).

- The TVC Property Manager will update inventory number, location, and employee data on the Information Resource Asset Database to reflect the SPA database.

Software Licensing

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on TVC Information Resources.

Audience

The TVC Software Licensing Policy applies equally to all individuals that use any TVC Information Resources.

Policy

Only properly licensed software may be used on TVC computers.

Any use of software on TVC computers must be in accordance with the applicable software license agreement and all applicable TVC policies and procedures.

Unauthorized copies of copyrighted software are prohibited.

Using, installing, loading, downloading or operating any copyrighted or non-copyrighted software without approval by TVC IR Department is prohibited.

Unauthorized use of shareware or freeware without TVC IR Department approval is prohibited.

Unauthorized download, installation or execution of programs that reveal or exploit weaknesses in the security of a system is prohibited.

Viruses and Threats

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Computer Virus and Threat Detection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

Audience

The TVC Computer Virus and Threat Detection Policy applies equally to all individuals that use any TVC Information Resources.

Virus Detection Policy

- All workstations whether connected to the TVC network, or standalone, must use the TVC IS approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each Email gateway must utilize TVC IS approved email virus protection software and must adhere to the IS rules for the setup and use of this software.
- Every virus or threat that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the ISO immediately.
- All TVC servers must comply with the statewide data center virus protection and prevention policies.

Technology Lease vs. Purchase Policy

The TVC Information Resources Manager reviewed the Department of Information Resources (DIR) Guidelines for leasing, purchasing, and lease-purchasing of information technologies. Based on the criteria established by DIR, TVC determined that it is in the best interest of TVC to purchase computers.

The following conclusions were reached in the analysis:

- Computer equipment is retained for longer than 3 years.
- Purchasing equipment eliminates the need to dedicate resources needed to develop, implement, and manage lease agreements.
- It is not feasible to manage lease agreements in field offices that receive IT support from Workforce Development Areas and the Department of Veterans Affairs, and
- The TVC makes its older computers available to Veterans County Services Offices throughout the state.

While desktop and laptop computers will be purchased by TVC, all purpose copiers will be leased when purchasing feels it is appropriate.

Criteria Considered for Lease vs. Purchase of Information Technology
Business Value
These questions examine the need for new equipment for end users, and the agency's ability to manage a leasing contract:

Does your agency/university have a formal replacement plan? If so, leasing is feasible. If replacement is done on an as-needed basis, the controls may be lacking to manage a lease.
TVC has a formal replacement plan for Claims computer. Central Administration, Employment, and Education replace computers as funding permit.

Does your agency/university currently lease any type of equipment? If so, this can provide useful expertise at identifying the usefulness, benefits, and drawbacks of leasing in your agency.
All purpose copiers (copy, print, scan, and fax) are usually leased by TVC.

Does your agency/university have a business need to replace PCs more often than is currently done? If so, what is the largest obstacle to more frequent replacement?
No.

Equipment Life Cycle
Identifying current agency practices helps to determine if leasing would or would not be useful to the agency. Long-term use of equipment indicates that the costs of leasing would most likely outweigh its benefits.
What is the average age of PCs before they are replaced in your agency/university?

Technology Lease vs. Purchase Policy

Over 4 years.

How long are servers used?
N/A. Servers are managed at the state data center.
Is data center software upgraded on a regular basis?
N/A

Asset Management
The ability to know where all of the IT equipment is at a given point in time is crucial to lease management. Tracking only at aggregate levels does not allow the agency to meet leasing terms when the time comes to identify and return the leased equipment. Penalties for lost/stolen equipment can add significantly to the cost of a leasing engagement.

Does your agency/university have IT tracking mechanisms in place?
Yes.
Does your agency/university have a problem with lost or stolen IT equipment? If so, is this a small, medium, or large problem?
No.

Contract Management
Effective leasing depends on the ability of the agency or university to set up the lease properly at the outset, and then to manage the entire life of the leasing contract. Uncertain funding makes leasing much less feasible.

Does your agency/university have the time to select a vendor?
No.

Does your agency/university have the time to develop a good leasing contract?
No.

Does your agency/university have the time and staff to manage the contract throughout the life cycle of the equipment?
No.

What is the stability of the primary source of funding for your IT equipment?
Funding is dependent upon State revenue. TVC had to reduce its capital budget.

DIR Policy Standard Reference Table

DIR Policy Standard	Detail based on TAC 202 and Best Practices
1	IR Security controls must not be bypassed or disabled. **TAC 202.2 – (1)**
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated. **TAC 202.8 – (d), (e)**
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management. **TAC 202.2 – (3); TAC 202.3 – (c) (3)**
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management. **TAC 202.2- (3); TAC 202.3 – (c) (3)**
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as a transfer, promotion, demotion, or termination of service. **TAC 202.3 - (c) (1)(A),(H); TAC 202.7 – (c) (2)**
6	The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management. **TAC 202.2 – (3); TAC 202.7 – (h) (O), (j)**

7	The user must keep any data used in an IR system confidential and secure. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured. **TAC 202.2 – (1); TAC 202.3 – (c) (3); TAC 202.7 – (b)**
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property. **TAC 202.2 – (1)**
9	On termination of the relationship with the TVC, users must surrender all property and IR managed by the TVC. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship. **TAC 202.7 – (c) (2)**
10	The owner must engage the IRM, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. Appropriate management must authorize the costs of acquisitions, development and operation of computer hardware and applications. Management and the requesting department must act within their delegated approval limits in accordance with the TVC authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published. **Industry Best Practices**
11	The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian. **TAC 202.3 – (c) (1)**
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure. **Industry Best Practices**
13	The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all TVC legal and fiscal policies and procedures. **Industry Best Practices**

14	The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data. **TAC 202.3 – (2), TAC 202.7 – (g) (1)**
15	All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.**TAC 202.3 – (c) (1)**
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled. **TAC 202.3 – (c) (2)**
17	All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the TVC is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements. **TAC 202.2 – (1); TAC 202.2 – (5); TAC 202.4 (a); TAC 202.6 (a) (5), (b); TAC 202.7 – (h) (D), (I), (P); 202.7 – (i) (1)**
18	All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized TVC officer and must contain terms approved as to form by the Legal Department, advising vendors of the TVC's IR retained proprietary rights and acquired rights with respect to its information systems, programs, and data requirements for computer systems security, including data maintenance and return. **Industry Best Practices**
19	IR computer systems and/or associated equipment used for TVC business that is conducted and managed outside of TVC control must meet contractual requirements and be subject to monitoring. **TAC 202.3 – (c) (2)**
20	External access to and from IR must meet appropriate published TVC security guidelines. **Industry Best Practices**

DIR Policy Standard Reference Table

21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system. **TAC 202.7 – (h) (S); Section 117 of the Copyright Act**
22	The IRM through IS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware. **TAC 202.7 – (h) (S); Industry Best Practices**
23	Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory. **Industry Best Practices**

TVC Information Systems Security Agreement

Read the following agreement carefully and completely before signing:

Purpose: The purpose of this document is to inform you of your responsibilities concerning the use of the Information Resources owned or held in trust by the Texas Veterans Commission (TVC). This agreement applies to all employees of the Texas Veterans Commission and other entities having a need for access to these Information Systems/Resources or any state-owned, federally-owned or controlled Information Resources while making use of TVC owned or operated networks or connections. This also applies to TVC employees using Information Resources and equipment supplied by other state and federal agencies and/or workforce boards.

Authorized Use:
I understand, acknowledge, and agree that:

- Information Resources are to be used for official state-approved business.
- Information Resources are not for personal use.
- There may be specific limited use exceptions outlined in other policies and procedures of TVC.
- TVC has a duty to protect its Information Resources.
- TVC has the right to monitor the use of Information Resources under its authority.
- TVC retains the right to restrict or limit access to or use of any Information Resources by any individual(s).
- Users of TVC Information Resources have no right to expect privacy in their use of Information Resources or in the content of their communication sent or stored in TVC owned or operated Information Resources.

Policy Adherence:
I understand, acknowledge and agree that:

- It is a violation of FLSA policy for a non-exempt TVC employee to access and/or use TVC Information Resources outside of assigned work hours without prior TVC supervisory approval.
- Access to the Internet from a Texas Veterans Commission owned, home based computer must adhere to all the same policies that apply to use from within Texas Veterans Commission facilities. Employees must not allow family members or other non-employees to access Texas Veterans Commission computer systems.

Personal Security Identification Codes:
I understand, acknowledge and agree that:

- I will receive and will be required to use one or more personal security identification codes (user account(s), passwords, Personal Identification Numbers (PIN), Security Tokens, etc.) to gain access to and to use Information Resources.
- My Security Identification codes are security controls and must be used only by me.
- I will be held personally responsible for any actions taken, or for any harm, loss or adverse consequences arising from the use of my personal security codes, including any unauthorized use by a third party if such party gains access to my security access codes due to my negligence or misconduct.
- Transactions initiated under my security identification codes will be considered as having been authorized and electronically signed by me.

Software:
I understand, acknowledge and agree that:

- Only properly licensed software may be used on TVC computers.
- Any use of software on TVC computers must be in accordance with the applicable software license agreement and all applicable TVC policies and procedures.
- Unauthorized copies of copyrighted software are prohibited.

TVC Information Systems Security Agreement

- Using, installing, loading, downloading or operating any copyrighted or non-copyrighted software without approval by TVC IT Department is prohibited.
- Unauthorized use of shareware or freeware without TVC IT Department approval is prohibited.
- Unauthorized download, installation or execution of programs that reveal or exploit weaknesses in the security of a system is prohibited.

Access to Data:
I understand, acknowledge and agree that:

- Proper authorization is required for access to all data owned or held in trust by TVC except for data that is maintained for public access. Additional Information Usage Agreements may be required in order to gain access to such data. Each TVC Division will furnish appropriate agreements to their respective employees.
- Any data considered to be, or designated as, confidential and/or sensitive shall have the full protection of all codes, laws, rules, standards and guidelines appropriate to those data and the particulars of their use.
- Information collected, stored and maintained in Agency data bases is considered confidential and disclosure of such information to unauthorized personnel is subject to disciplinary action up to and including termination.

Security of Equipment:
I understand, acknowledge and agree that:

- Information resources ***cannot*** be removed physically, electronically or through any other means from TVC property without written authorization and prior approval of my supervisor.
- Any questions or concerns about the security of Information Resources will be addressed to my supervisor or the IT Department at Headquarters.

General Rules of Behavior:

- **Incidental Use of Information Resources**
  - As a convenience to the Texas Veterans Commission user community, incidental use of Information Resources is permitted. The following restrictions apply:
  - Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Texas Veterans Commission approved users; it does not extend to family members or other acquaintances.
  - Incidental use must not result in direct costs to Texas Veterans Commission.
  - Incidental use must not interfere with the normal performance of an employee's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, the Texas Veterans Commission.
  - Storage of personal email messages, voice messages, files and documents within Texas Veterans Commission's Information Resources must be nominal.

  All messages, files and documents – including personal messages, files and documents – located on Texas Veterans Commission Information Resources are owned by Texas Veterans Commission, may be subject to open records requests, and may be accessed in accordance with this policy.

- **Emails:**
  - Do not provide a work email address to non-work related Internet sites, surveys or list-servers.
  - Do not forward work email to a personal mail account.
  - Discourage others from sending non-business email.
  - Ensure that personal email does not interfere with TVC's mission or operation.
  - ***All TVC*** email messages are the property of TVC and are subject to the Open Records Act.

- Do not use email for sending or forwarding chain letters.
- Do not use email to send, receive or forward sexually oriented or pornographic materials.
- Do not use email to send, receive or forward objectionable language.
- Do not use email to solicit for outside or commercial ventures, religious or political causes, outside organizations or organizations that are not job related.
- Do not use email for any personal monetary interests or gain.

- **Internet:**
  - TVC allows limited personal use of the internet.
  - However, it is limited to the employee's non-work time, it must not interfere with the agency's mission or operation and it cannot violate standards of ethical conduct.
  - Access to the Internet is a privilege that may be revoked at any time for inappropriate use or conduct including use that violates other applicable agency policies. Inappropriate use or conduct includes but is not limited to:
    - Use of the Internet for unlawful or malicious activities;
    - Misrepresenting a personal communication as a communication in the employee's official capacity;
    - For viewing or printing offensive, sexually oriented or pornographic materials;
    - Soliciting for outside or commercial ventures, religious or political causes, outside organizations, or other organizations that are not job related;
    - Activity which causes congestion and disruption of networks and systems is prohibited.

- **Professional Behavior:**
  - Avoid any appearance of impropriety. Do not complete, update or key any information (i.e. a claim, WIT application for employment, referral, etc.) for yourself, a relative, a friend or a coworker without the review and approval of a supervisor.
  - Do not access or monitor any records or information except those that are absolutely necessary to complete assigned job duties.
  - Do not attempt to access any data or programs used by the Texas Veterans Commission systems for which you do not have authorization or explicit consent.
  - Do not purposely engage in activity that may:
    - harass, threaten or abuse others;
    - degrade the performance of Information Resources;
    - deprive an authorized Texas Veterans Commission user access to a Texas Veterans Commission resource; obtain extra resources beyond those allocated; or
    - circumvent Texas Veterans Commission computer security measures.
  - Do not intentionally access, create, store or transmit material which Texas Veterans Commission may deem to be offensive, indecent or obscene.
  - You must report any weaknesses in Texas Veterans Commission computer security, any incidents of possible misuse or violation of this agreement to your direct supervisor.
  - Do not engage in acts against the aims and purposes of Texas Veterans Commission as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
  - Use of Agency Information Resources for excessive personal use or any personal gain is strictly prohibited and subject to disciplinary action up to and including termination.

I understand that any violation of these policies and procedures could result in disciplinary action up to and including termination of my employment and/or prosecution under one or more applicable statutes.

TVC Information Systems Security Agreement

Note: "Information Resources means the procedures, equipment and software that are employed, designed, built, operated and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel including consultants and contractors."
TX. Govt. Code 2054.003(7).

Information Resources also includes Information Resources Technologies which are defined as data processing and telecommunication hardware, software, services, supplies, personnel, facility resources, maintenance and training. TX Govt. Code 2054.003(8).