

# **TEXAS WORKFORCE COMMISSION**

## **Enterprise Information Security**

### **Standards and Guidelines**

**It is the policy of the Texas Workforce Commission that the Commission and its employees will protect the Information Resources (IR) of the Commission in accordance with the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202 Information Security Standards and the Information Resources Management Act (Texas Government Code Chapter 2054). The Commission will also protect the IR of the Commission in accordance with other applicable state and federal laws.**

## Information Security Standards and Guidelines

- SG1.0 [Acceptable Use](#)
- SG2.0 [Account Management](#)
- SG3.0 [Administrative/Special Access](#)
- SG4.0 [Anti-Spam](#)
- SG5.0 [Back-up/Disaster Recovery](#)
- SG6.0 [Change/Patch Management](#)
- SG7.0 [Contingency Planning](#)
- SG8.0 [E-Mail Use](#)
- SG9.0 [Imaging Devices](#)
- SG10.0 [Incident Management](#)
- SG11.0 [Incidental Use/Limited Use](#)
- SH12.0 [Instant Messaging \(IM\)](#)
- SG13.0 [Internet/Intranet/Extranet Use](#)
- SG14.0 [Intrusion Detection](#)
- SG15.0 [Malicious Code](#)
- SG16.0 [Media Disposal](#)
- SG17.0 [Network Access](#)
- SG18.0 [Network Configuration](#)
- SG19.0 [Operating Systems](#)
- SG20.0 [Passwords](#)
- SG21.0 [Peer-to-Peer \(P2P\)](#)
- SG22.0 [Physical Access](#)
- SG23.0 [Portable/Remote Computing](#)
- SG24.0 [Privacy Policies](#)
- SG25.0 [Removable Media](#)
- SG26.0 [Security Monitoring](#)
- SG27.0 [Security Training](#)
- SG28.0 [Server Hardening](#)
- SG29.0 [Systems Development](#)
- SG30.0 [Vendor Access](#)
- SG31.0 [VPN – Virtual Private Network](#)
- SG32.0 [Wireless Computing](#)

## **SG1.0 Acceptable Use**

Computer data, hardware, and software are state property. All information passing through the TWC network, which has not been specifically identified as the property of other parties, will be treated as a TWC asset. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information is prohibited.

Every information system privilege that has not been explicitly authorized is prohibited. Information entrusted to TWC will be protected in a manner consistent with its confidentiality and in accordance with all applicable standards, agreements, and laws.

All TWC employees, Local Workforce Development Board staff, volunteers, private providers of services, contractors, vendors, representatives of other agencies of state government, and any other person or entity granted access to TWC information resources must comply with the following standards set forth below and elsewhere in the TWC Information Security Standards and Guidelines as they are updated:

- SG1.1** All User activity on TWC information resources is subject to logging and review.
- SG1.2** Software installed or executed within the TWC systems and/or networks must be approved by the Custodian responsible for that area and be on the agency software list.
- SG1.3** Users leaving their computers unattended must either lock access to their workstation or logoff.
- SG1.4** Users must not share their passwords, Personal Identification Numbers (PIN), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authentication purposes.
- SG1.5** Users must not operate a public peer-to-peer file sharing system to transfer files.
- SG1.6** Any TWC IR User who becomes aware of a weakness, incident, misuse or violation of any policy related to the security and protection of those resources must report such to IT Security and their area's management as soon as possible.
- SG1.7** Users may not attempt to access any data, program, or system for which they do not have approved authorization or explicit consent.
- SG1.8** Users of TWC IR must protect all account information that may allow access to any system under the authority of TWC. This includes account identifiers, passwords, personal identification numbers, access tokens or any other information, or device used for User identification and/or authorization.
- SG1.9** The use of any unapproved, unlicensed or otherwise unauthorized software is prohibited. This includes any activity that adversely affects the functionality of a User's workstation or violates software license requirements.
- SG 1.10** Users must not intentionally access, create, store, or transmit any material that may be offensive, indecent, or obscene unless such action is specifically within the scope of job duties for their position.
- SG1.11** Any activity which may harass, threaten or abuse others, degrade the performance of information resources, deprive or reduce an authorized User's access to resources or otherwise circumvent any security measure or policy is prohibited.
- SG1.12** Users must not purposely engage in unauthorized activity that may circumvent the department computer security measures.
- SG1.13** The unauthorized copying of otherwise legal and licensed software is prohibited. Unauthorized duplication of software may be a violation of copyright laws.

- SG1.14** A User shall not use any TWC information resource in such a manner that they may gain personal benefit.
- SG1.15** Users must use appropriate safeguards to protect state-owned software and hardware from damage, loss, or theft.
- SG1.16** If a User is in possession of a department owned or leased computer that is used off-site, at the User's home, or at any location not under the authority of TWC, that User must follow the same policies, standards and guidelines established for use of such equipment located at or in any TWC location.
- SG1.17** Any User of TWC owned or leased equipment used in an environment out of the authority of TWC must protect that equipment from use and abuse by non-TWC approved Users. Users of such equipment must not allow the use of such equipment by any family member or other non-employee or unauthorized User.
- SG1.18** Users of TWC information resources must not engage in any act that would violate the purposes and goals of TWC as specified in its governing documents, rules, regulations, and procedures.
- SG1.19** Users must not divulge modem phone numbers to anyone unless doing so is a function of their responsibilities.
- SG1.20** Users must not divulge IP addresses of internal TWC systems to anyone without prior consent of the Director, Information Resources or their designee.
- SG1.21** Users must not intentionally store or transmit any materials for which they or TWC does not hold copyright permission. This includes, but is not limited to, audio, video, software, data or any other digital information.

## SG2.0 Account Management

Account Management establishes the standards for the creation, monitoring, control, and removal of User accounts. The Account Management standard shall apply equally to all User accounts without regard to their status or category.

User accounts are the means by which access is granted to TWC information resources. Accounts are granted to employees, Board staff, volunteers, vendors, contractors, students and others determined to have a need. These accounts assist in establishing accountability for systems use and are a key component in the protection of data; its confidentiality and integrity.

- SG2.1** All Users must sign the TWC Information Resources Usage Agreement (IRUA or P-41) before access is given to an account. Additional documentation may also be required.
- SG2.2** Users of TWC systems must have on file a signed TWC IRUA/P-41 and such agreement shall be reaffirmed annually.
- SG2.3** All accounts must be identifiable using a unique User ID.
- SG2.4** Accounts, other than service/maintenance accounts, must uniquely identify a specific User.
- SG2.5** Account access levels will be reviewed, at a minimum, every twelve (12) months for appropriateness. Appropriateness shall be reviewed and affirmed by the appropriate user supervisor and/or application Owner.
- SG2.6** Unsuccessful account access attempts must be monitored and accounts locked after no more than three (3) failed attempts or as determined by a documented risk assessment. Unlocking accounts must require human intervention unless documented risk analysis determines otherwise.
- SG2.7** All new User accounts that have not been accessed within thirty (30) days of creation will be disabled. (NOTE: See 8b below for possible exceptions to this standard.)
- SG2.8** Any User of TWC IR that shall be absent from the work place and will not be working remotely for a period in excess of thirty (30) days must notify the Custodian responsible for that area (in lieu of the user ,the user's supervisor may provide notice). The User's account will be disabled during their absence and reactivated upon notification of their return. Exceptions to this include:
  - SG2.8.1** Certain accounts held in indefinite suspense for the purpose of application maintenance.
  - SG2.8.2** Accounts established for the purpose of quarterly, semiannual or annual usage
- SG2.9** Custodians or other designated staff are:
  - SG2.9.1** Responsible for modifying, disabling or deleting the accounts of individuals who change roles within TWC or are separated from their relationship with TWC, and
  - SG2.9.2** Must have a documented process to modify a User account to accommodate situations such as name changes, accounting changes and permission changes, and
  - SG2.9.3** Must have a documented process for periodically reviewing existing accounts for approved access, and
  - SG2.9.4** Must provide a list of accounts for the systems they administer when requested by authorized TWC IT management, and
  - SG2.9.5** Must cooperate with authorized TWC IT management investigating security incidents.
  - SG2.9.6** Special processes have been established to manage accounts in the event of termination of employment or change in job status necessitating the termination of a User's access.

- SG2.9.7** All access accounts established for contractors, consultants, vendors and/or maintenance accounts must be deleted immediately upon termination or completion of the contract period. Any extension of access periods for these accounts must be reflected in appropriate contract changes.
  
- SG2.9.8** All non-TWC Users of non-public TWC IR shall be required to sign an agreement establishing the requirement for notification of User changes brought about by an employee termination or transfer. These accounts shall be deleted, removed or reassigned in compliance with application specific requirements.

### **SG3.0 Administrative and/or Special Access**

On occasion certain staff and/or consulting personnel may be granted levels of access to TWC systems that exceed the account privileges granted to a regular User. Typically, these are positions providing technical support and administrative functions. The nature of these accounts requires a higher level of control and monitoring on the part of security administrators throughout the TWC system.

Administrative and/or Special Access accounts shall not be granted universally throughout the TWC user community. Instead these access levels shall be granted only on a role-based need with full knowledge and approval of the user's supervisor and/or other management level staff. The Administrative and/or Special Access policy establishes those parameters to which the User granted this access must adhere in order to adequately protect the information resources of TWC.

- SG3.1** TWC department heads must submit to the IRM, or designee, a listing of administrative contacts or other staff using these accounts for their systems that are connected to the TWC network.
- SG3.2** Users of TWC systems must sign the TWC Information Resource Usage Agreement (IRUA) and any other security and/or privacy agreements appropriate to their status, prior to any access being granted.
- SG3.3** Users with Administrative/Special Access accounts must refrain from abusing the elevated level of access they are granted and must only perform specialized and/or non-standard functions granted by those rights within the framework of their positions.
- SG3.4** Users with Administrative/Special Access must use the account privileges most appropriate to the work they are performing. For example, they will not make use of their administrator account to perform work more appropriately performed while using their standard User account.
- SG3.5** Users with Administrative/Special Access will maintain a password for that account in compliance with the TWC Password standard.
- SG3.6** Any password used in relation with a "shared" Administrator Special Access account must be changed when any individual with knowledge of that password leaves the department or TWC. This shall apply to TWC employees as well as any employee of another entity or organization with the "shared" access. Any user of an Administrator account must participate in a password escrow procedure so that another approved User, other than the original administrator, may access that account in the event of an emergency.
- SG3.7** Any Special Access account created on behalf of specialized research projects, internal or external audit needs and requirements, software installation or development projects, or any other defined needs must:
  - SG3.7.1** Be authorized by the appropriate TWC staff position or administrator,
  - SG3.7.2** Be established with a specific and defined date of expiration, and
  - SG3.7.3** Be removed when the work is completed or the expiration date is reached.
- SG3.8** Changes and amendments to these accounts must be clearly documented in advance of the change. Personnel changes, including reduction or increase in account privileges, must be communicated to the IRM or designee.

## **SG4.0 Anti-Spam**

As E-Mail has become an integral part of the business process its abuse has also grown. These abuses often is manifested as “spam” or “junk” E-Mail which has the potential, beyond its annoying nature, to slow-down and/or clog the infrastructures required to process electronic messages. In addition, “spam” is often used as a transmission vehicle in the migration of virus, worm, Trojan and other malicious-code infections.

In order to protect the electronic messaging environments under the authority of TWC the following anti-spam standard is provided:

- SG4.1** TWC IT management, in consultation with other TWC management, reserves the right to filter and/or block any E-Mail item, inbound or outbound, which is determined to place TWC, its systems and/or networks at an unacceptable level of risk.
- SG4.2** TWC IT retains the right to examine any non-encrypted E-Mail item for subject and/or content to determine E-Mail abuse.
- SG4.3** TWC IT shall, in consultation and aligned with industry best practices, filter and/or block any attachment or enclosure to any E-Mail that places the TWC systems and/or networks at an unacceptable level of risk.
- SG4.4** TWC IT may identify a listing of key words and phrases that are common to “spam” and shall filter those E-Mail words and phrases on all inbound E-Mail items in order to prevent those items from entering the TWC systems and/or networks.
- SG4.5** All Users of TWC E-Mail systems shall refrain from forwarding multiple copies of received E-Mail items that are not directly connected to the TWC business process without the explicit consent of the recipient
- SG4.6** All Users of TWC E-Mail systems shall use caution in selecting the “Reply to All” function of the TWC E-Mail client application.
- SG4.7** All users of TWC E-Mail systems shall refrain from signing up for “mailing lists” or registering for non-agency related events or websites using their TWC E-Mail address. Users shall also refrain from posting to public newsgroups or “web boards”, blogs, etc. using their TWC E-Mail address.
- SG4.8** All users of TWC E-Mail systems shall not publish their TWC E-Mail address on any internet website outside the authority of TWC.

## **SG5.0 Back-up and Disaster Recovery**

Back-ups of data and applications are a business requirement established to enable the recovery of data and applications in the event of loss or damage due to natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors or systems operator errors. The standard includes:

- SG5.1** The frequency and extent of backups must be sufficient to support documented business continuity and disaster recovery plans. Frequency and extent may vary, depending on data classification and Owner requirements. The IRM or designee must approve back-up and recovery plans and procedures.
- SG5.2** Any TWC information resources back-up and recovery process for any TWC system must be documented and periodically reviewed.
- SG5.3** Any provider of offsite storage for TWC must be determined by means of certifications and/or verifiable adherence to industry standards as able to provide protection for the highest risk level of information being stored.
- SG5.4** Physical access controls in use at any offsite storage location must meet or exceed the physical access controls defined for the source systems.
- SG5.5** Media used in the provision of backup storage must be protected in accordance with the highest level of sensitivity of that information being stored.
- SG5.6** A success-verification process shall be used for all electronic information back-ups.
- SG5.7** Electronic information back-ups must be periodically tested to assure recoverability.
- SG5.8** Identification data used in granting access to and/or in directing the recall or transfer of media stored in the offsite storage facility must be reviewed on a regular basis and changed or updated to reflect changes brought about by changes in authorized access personnel.
- SG5.9** Stored data must be labeled in such a way to facilitate the recovery and protection of the stored data
- SG5.10** Offsite storage facilities must be geographically located away from the primary physical location of the TWC information resource so that a single disaster should not destroy the data at both sites.

## **SG6.0 Change/Patch Management**

The TWC Change/Patch Management Standard establishes a set of rules and administrative guidelines used to manage changes in a rational and predictable manner as well as provide for the necessary documentation of changes made to reduce any negative impact to the community of Users of TWC systems. Changes include, but are not limited to implementation of new functionality, interruption of services, maintenance activity and repair of existing functionality and/or removal of existing functionality. Standards include but are not limited to:

- SG6.1** Change/Patch management will be required based on Department risk assessment to TWC information resources (including operating systems, computing hardware, networks, and applications).
- SG6.2** Any change affecting computing environmental facilities (HVAC, water, plumbing, alarms, etc.) must be coordinated with the appropriate IT staff to assure compliance with the change management process.
- SG6.3** Changes must be documented by the appropriate application Custodian.
- SG6.4** Scheduled changes must be submitted to the appropriate staff for review to determine the appropriateness of the change and to permit advance determination as to allowing or delaying the change.
- SG6.5** Scheduled changes must be reviewed by the appropriate IT staff and data Owner(s) prior to the change. These review staff may deny or delay the change if it is determined that the change has not been adequately planned for, suffers from inadequate backup planning, will negatively impact a key business process or adequate resources cannot be made available to support the change.
- SG6.6** User notification, as appropriate to the specifics of the change, must be performed for each scheduled change.
- SG6.7** A change review process must follow all scheduled, unscheduled or emergency changes.
- SG6.8** A change management log must be maintained for all changes.

## SG7.0 Contingency Planning

Contingency Planning provides the best possible opportunity for preserving and recovering key computing components and the critical information that resides on those components. This standard establishes the requirement that each department owning a critical system or system that contains critical information is responsible for providing (or participating in the provision of) a contingency plan for system and data recovery.

**All systems that support a critical function and/or that contain critical information are covered by this standard.**

In addition, departments are encouraged to prepare contingency plans for non-critical systems.

**NOTE:** For the purpose of this standard a contingency plan is defined by NIST 800-34 Appendix C. "An IT Contingency Plan is the same as the Continuity of Support Plan required by Office of Management and Budget (OMB) Circular A-130, Appendix III. Both plans provide the recovery and resumption procedures for an IT system. This type of plan is broader in scope than a Disaster Recovery Plan because it includes procedures for recovering a system resulting from minor disruptions that do not necessarily require relocation to an alternate site."

Each individual system covered under this standard must have an individual contingency plan included within the "master" plan document. The individual plan must, at a minimum, contain the following elements:

- Name of System
- System Description
- Critical System (T or F)
- Critical Data (T or F)
- Primary Staff
- Backup Staff
- Key Users
- Dependencies (other systems dependent on)
- Facility/Location
- Vendor Contact (if applicable)
- Maintenance (contract and expiration date)
- Backup Frequency
- Backup Location
- Emergency Mode Operations (how to provide equivalent services until restored)
- Normalization Procedures
- Lost or Damaged Data Recovery Procedures

The Contingency Plan may be a component part of an overall Business Continuity and Disaster Recovery Plan.

Prior to any new critical system or system containing critical data being placed into production, a contingency plan must be documented and submitted to the appropriate IT Director or designee for approval and inclusion into the TWC Business Continuity and Disaster Recovery Plan.

This standard shall apply to all individuals who are responsible for purchase, development, installation, implementation or maintenance of key/critical data, key/critical systems, hardware and the facility that houses such equipment, hardware, systems or data.

## **SG8.0 E-Mail Use**

The growth of use and the increase in vulnerabilities related to electronic communications has seen a corresponding increase in the need for policies governing the use of, and protections directed to, those communications. The e-mail standards include:

- SG8.1** The following activities are prohibited:
  - SG8.1.1** Sending e-mail that is intimidating or harassing,
  - SG8.1.2** Using e-mail for conducting personal business,
  - SG8.1.3** Using e-mail for purposes of political lobbying or campaigning,
  - SG8.1.4** Violating copyright laws by distributing protected works,
  - SG8.1.5** Posing as anyone other than oneself when sending e-mail, except when authorized to send messages for another when serving in an administrative support role, as a delegate, or when using a "pool" account,
  - SG8.1.6** Using unauthorized e-mail software,
  - SG8.1.7** Sending or forwarding chain letters,
  - SG8.1.8** Sending unsolicited messages to large groups except as required in conducting department business,
  - SG8.1.9** Sending excessively large messages or enclosures, and
  - SG8.1.10** Sending or forwarding e-mail that is likely to contain malicious code
- SG8.2** Confidential TWC material transmitted over external network connections must be encrypted or otherwise protected as required by rule or law.
- SG8.3** All User activity on TWC information resources assets is subject to logging and review.
- SG8.4** E-Mail Users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of TWC or any unit of TWC unless authorized (explicitly or implicitly) to do so.
- SG8.5** Individuals must not send, forward or receive confidential TWC information through non-TWC approved e-mail accounts.
- SG8.6** Individuals must not send, forward or store confidential TWC electronic information utilizing non-TWC owned mobile devices such as, but not limited to, laptop/notebook computers, personal data assistants or other hand-held devices, two-way pagers or digital/cellular telephones without written permission.
- SG8.7** Individuals have no right to privacy with regard to E-Mail. Management has the ability and right to view employees' E-Mail. Recorded E-Mail messages are the property of TWC. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

## **SG9.0 Imaging Devices**

The TWC Imaging Devices Security Standard establishes those rules necessary to mitigate risks associated with the increased use of devices that have the capability to capture images for storage and/or transmission. Such devices include, but are not limited to, Cellular Telephones with camera capabilities (built-in or attached), Personal Digital Assistants (PDA) with camera capabilities (built-in or attached), Laptop/Notebook Computers with camera capabilities (built-in or attached) and/or Digital cameras, digital video recording devices of any sort.

- SG9.1** The use of such devices is allowed to the extent that there is a TWC business reason. In any case, the Owner is responsible for the protection of all sensitive, confidential or private information to which employees, contractors, vendors, visitors or others may have access either as a granted right or by accidental exposure.
- SG9.2** Any device that has the capability to capture, store and/or transmit an image of any document, person or environment (still or in motion) under the authority of this standard shall have the image capturing function disabled while in restricted TWC environments.
- SG9.3** Exemptions to this policy include dedicated document scanning devices and other equipment designed specifically to capture document images for archival storage.
- SG9.4** Requests for any other exemption to this policy must be approved in writing prior to use of the device. The exemption approval authority shall be one or more of the following:
  - SG9.4.1** Information Resources Manager (IRM)
  - SG9.4.2** Chief Information Security Officer (CISO)
  - SG9.4.3** Director, Information Technology
  - SG9.4.4** Director, Data Processing/Distributed Systems

## **SG10.0 Incident Management**

The TWC Incident Management Standard establishes requirements for dealing with computer security events. These security events include, but are not limited to, virus, worm and Trojan detection, unauthorized use of computer accounts and systems as well as improper use of resources as outlined in those standards related to e-mail, Internet/Intranet/Extranet and Acceptable Use.

- SG10.1** A Computer Incident Response Team (CIRT) shall exist with membership having pre-defined roles and responsibilities which can take priority over their normal functions.
- SG10.2** The Incident Management procedure must be followed whenever a security incident is suspected or confirmed.
- SG10.3** The Chief Information Security Officer, or designee, is responsible for notifying the IRM, the Director of Data Processing, the CIRT, the Department of Information Resources (DIR), and applications Owner(s) as appropriate and shall initiate the appropriate incident management action(s).
- SG10.4** CIRT will manage the monitoring and analyzing of any damage and shall oversee its repair or mitigation and that the area of vulnerability is eliminated or minimized as appropriate.
- SG10.5** The Chief Information Security Officer, working with the IRM, shall determine if a widespread communication related to the incident is required and shall determine the content and how best to distribute the communication.
- SG10.6** The appropriate technical personnel from the CIRT are responsible for communicating issues or vulnerabilities to any vendor involved and for working with the vendor to eliminate or mitigate the vulnerability.
- SG10.7** The Chief Information Security Officer, or designee, is responsible for initiating, completing, and documenting the incident investigation with the assistance from the CIRT and shall report the incident to the appropriate management at DIR and TWC as outlined in the requirements of TAC 202 and other entities as appropriate.

### **SG11.0 Incidental Use/Limited Use**

Incidental and Limited personal use of TWC information resources by Users is permitted. Such use must adhere to the following standards:

- SG11.1** Limited personal use of e-mail and Internet access is allowed for employees, vendors and other approved Users only. This use does not extend to visiting friends or relatives of the approved User.
- SG11.2** Limited use must not result in any additional direct costs to TWC such as printer toner or paper.
- SG11.3** Limited use must not interfere with the normal performance of the Users' duties or any TWC resource.
- SG11.4** No file, document or other item may be sent or intentionally received that may provoke legal action against, or embarrassment to, TWC.
- SG11.5** Storage of personal e-mail, voice-mail, files, and/or any other document by the approved User must be kept to a minimum.
- SG11.6** All messages, files and/or documents (including any personal messages, files and/or documents) located on or in any TWC information resource are owned by TWC and may be accessed by TWC IT and supervisory staff without notice to the User. Such documents may be subject to open records requests.
- SG11.7** The use of "social networking" Internet sites by TWC network users during work-hours is prohibited.
- SG11.8** Limited personal use does not extend to the streaming of audio and/or video content across the Internet except as it is directly related to the functions of the user's position.

## **SG12.0 Instant Messaging**

Instant messaging (IM) is a tool that allows a form of text-based communication from a person or persons to another/others. IM works on a real-time basis, meaning that as long as the required parties are connected to an IM server, each party is able to see the connection status of the other and communicate with them almost instantly. Like a telephone, IM allows for back-and-forth conversations.

The Texas Workforce Commission (TWC) supports the use of IM for job-related activities. The need of IM should be communicated through approved software requests procedures. If approved, the IM software will be installed or passed to the user for installation. Users of TWC information technology resources may not install IM software, or any other software, without authorization.

This standard applies to Instant Messaging (IM) software used within the Texas Workforce Commission (TWC) and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. In all cases users of TWC information resources shall comply with all Information Security Standards and Guidelines as they apply to a particular circumstance with special consideration for requirements related to Acceptable Use and the Information Security Program statements on Responsibilities and Rules of Behavior.

- SG12.1** IM usage within TWC must be authorized in writing by the Information Resources Manager (IRM), Director of Information Technology, Director of Data Processing or their designee(s).
- SG12.2** IM usage within TWC or its Information Technology environments will be only for legitimate state business. Users of TWC computers or networks that are authorized to use IM software will use only those instant messaging applications approved and provided by TWC.
- SG12.3** All policies and guidelines pertaining to standards of conduct and user rules of behavior apply to IM, including, but not limited to, rules regarding solicitation, obscenity, harassment, pornography, sensitive information and malware.
- SG12.4** If the IM software provided allows for the user to create a unique user name it shall be appropriate for a professional environment and selected in good taste.
- SG12.5** If authorized for use IM may be used for any routine official business. "Conversations" conducted in the IM environment are subject to agency records retention rules, State of Texas Open Record rules, and any other state or federal rule regarding the availability of government documents.
- SG12.6** Users of TWC Computers or networks will not download/install or use any IM software or participate in any IM network on TWC computers, networks or mobile computing devices (laptops, PDAs, cell phones) without the specific written authorization to do so.
- SG12.7** Users of TWC computers and networks should always keep in mind that all IM traffic may be recorded and stored. Employees have no expectation of privacy with regard to IM "conversations". Management has the ability and right to view users' IM "conversations" on TWC systems and networks.
- SG12.8** IM "conversations" recorded on TWC systems are the property of the State of Texas held in trust by TWC and may be subject to requirement of the Texas Public Information Act and rules related to retention of State of Texas records.
- SG12.9** Personal use of IM on TWC networks shall be limited to brief "conversations" of a personal nature within the managed constraints of the IM software or network. A user may not modify configurations of the IM software in any way to expand its personal use capabilities.
- SG12.10** IM software shall not impede the conduct of other state/TWC business.

- SG12.11** Many IM applications allow peer-to-peer (P2P) file sharing. Using IM-P2P to access, view, download, upload, forward, print, copy, post or share in any way racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable materials (visual, textual or auditory) is strictly prohibited. Such usage will be reported to the appropriate authorities by TWC.
- SG12.12** Using IM-P2P to transmit or receive copyrighted materials of any nature (audio, video, still picture, etc.) for which the copyright is not owned by TWC and/or the State of Texas is prohibited at all times.

### **SG13.0 Internet/Intranet/Extranet Use**

For the purpose of this standard, the term Internet shall include Intranet and/or Extranet. This standard includes:

- SG13.1** Software for browsing the Internet is provided to Users for business, research and allowed incidental/limited personal use only.
- SG13.2** All software used to access the Internet must be part of the TWC standard software suite or approved for use by the appropriate TWC authority.
- SG13.3** All software used to access the Internet must incorporate vendor provided security patches.
- SG13.4** All files downloaded from the Internet must be scanned for viruses using the approved IT distributed software suite and current virus detection software.
- SG13.5** All software used to access the Internet shall be configured to provide the highest level of protection possible to TWC systems and networks.
- SG13.6** All sites accessed on the Internet must comply with the TWC Acceptable Use Standard.
- SG13.7** All content on TWC Internet sites must comply with the TWC Acceptable Use Standard and other guidelines and standards developed for the management of Internet content.
- SG13.8** No offensive or harassing materials may be made available via any TWC Internet site.
- SG13.9** No personal commercial advertising may be made available via any TWC Internet site.
- SG13.10** Internet access provided by TWC may not be used for personal gain or non-TWC personal solicitations.
- SG13.11** Confidential TWC material transmitted over external network connections must be encrypted.
- SG13.12** Users may not install or use encryption software on the TWC computer resources that has not been reviewed and approved for use by TWC Enterprise Security. Users may not use encryption keys that are unknown to their supervisor.
- SG13.13** All electronic files are subject to the same records retention rules that apply to the same document in non-electronic formats.
- SG13.14** Incidental personal use of Internet access is permitted but must not inhibit the use of network resources for business purposes.
- SG13.15** Incidental personal use of Internet access is restricted to TWC approved Users; it does not extend to family members or other acquaintances or visitors to any TWC office.
- SG13.16** Incidental use must not interfere with the functionality of any TWC system or network or the normal performance of an employee's work duties.
- SG13.17** Incidental use must not result in any direct costs to TWC.

## **SG14.0 Intrusion Detection**

The Intrusion Detection Standard includes:

- SG14.1** Operating system, user accounting, and application software audit logging processes must be enabled on all systems as appropriate to the risks determined for that system.
- SG14.2** Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled as appropriate to the risks determined for that system.
- SG14.3** Audit logging of any firewalls and other network perimeter access control systems must be enabled as appropriate to the risks determined for that system.
- SG14.4** System integrity checks of firewalls and other network perimeter access control systems must be performed on a routine basis.
- SG14.5** Audit logs for servers and hosts must be reviewed on a routine basis as established by ongoing risk assessment and analysis.
- SG14.6** Host based intrusion tools will be reviewed on a routine basis as established by ongoing risk assessment and analysis.
- SG14.7** All trouble reports should be reviewed for symptoms indicating intrusive activities.
- SG14.8** All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to Enterprise Security according to the Incident Management Standard.
- SG14.9** Users shall be trained to recognize and report any anomalies and signs of wrongdoing according to the Incident Management Standard.

## **SG15.0 Malicious Code**

The purpose of the TWC Malicious Code Standard is to describe requirement for dealing with digital infections (including virus, worm, Trojan and other malware), their prevention, detection and cleanup. This standard includes:

- SG15.1** All workstations (desktop, notebook, laptop or other device capable of digital interaction with TWC networks, systems and/or applications) whether connected to the TWC network, used remotely or stand-alone, must use TWC IT approved virus protection software and configurations or a certifiably comparable product.
- SG15.2** Virus protection software must not be disabled or bypassed without the approval and involvement of TWC IT staff.
- SG15.3** Settings for virus protection software must not be altered in any manner that will reduce the effectiveness of the software.
- SG15.4** Any automatic update frequency of the virus protection software designed into the software or established as a batch process within the network must not be altered to reduce the frequency of the updates.
- SG15.5** Each file server attached to the TWC network(s) must utilize TWC IT approved virus protection software and setup to detect and clean viruses that may infect file shares.
- SG15.6** Each e-mail gateway must use TWC IT approved e-mail virus protection software.
- SG15.7** Any virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the appropriate TWC authority.

## **SG16.0 Media Disposal**

*This section is currently under revision.*

## **SG17.0 Network Access**

The TWC Network Access Standard establishes security rules for the access and use of the network infrastructure.

- SG17.1** Users are permitted to use only those network addresses and access points authorized by TWC IT.
- SG17.2** Remote Users may connect to TWC information resources using only those protocols approved by TWC IT.
- SG17.3** Users must not extend or re-transmit network services in any way.
- SG17.4** Users must not install network hardware or software that provides network services without TWC IT approval including wireless.
- SG17.5** Non-TWC systems that require network connectivity must conform to TWC Standards and Guidelines.
- SG17.6** Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system except as part of the official systems security management process.
- SG17.7** The use of unapproved tools such as password cracking programs, packet sniffers, network-mapping tools, or port scanners are prohibited except as part of the official systems security management process.
- SG17.8** Users are not permitted to alter network hardware or bypass any network security tools, monitoring systems or other configurations in any way.
- SG17.9** All user accounts shall be reviewed as part of routine supervisory responsibilities and as part of an annual RACF security assessment. (06-12-2008)

## **SG18.0 Network Configuration**

The TWC Network Configuration Standard establishes the rules necessary for the maintenance, expansion, and use of the TWC network infrastructure.

- SG18.1** TWC IT owns and is responsible for the network infrastructure including management, development and enhancement.
- SG18.2** Networking development (including cabling) must be installed by TWC IT or an approved contractor.
- SG18.3** Equipment connected to the TWC network must be configured to specifications approved by TWC IT.
- SG18.4** Any hardware connected to the TWC network infrastructure is subject to the management and standards of TWC IT.
- SG18.5** Changes to the configurations of any active network management device must not be made without the approval of TWC IT.
- SG18.6** TWC IT must approve any use of non-sanctioned protocols.
- SG18.7** All network addresses for protocols supported by TWC are allocated, registered and managed by TWC IT.
- SG18.8** Any connection to the TWC network infrastructure by third party networks (including telecommunications) is the responsibility of TWC IT.
- SG18.9** The use of departmental firewalls or other non-standard tools is not permitted without the written authorization of TWC IT.
- SG18.10** Users must not extend or re-transmit network services in any way.
- SG18.11** Users must not install network hardware or software intended to provide network services without the approval of TWC IT including wireless.
- SG18.12** Users must not alter network hardware in any way or bypass any network security tools, monitoring or configurations.

## **SG19.0 Operating Systems**

- SG19.1** Installation of operating system software shall be documented and reviewed.
- SG19.2** All operating system software shall be stable with appropriate patches and have corresponding and complete documentation.
- SG19.3** Operating system software changes shall be authorized, tested and approved in accordance with TWC change management processes before being implemented.
- SG19.4** Operating system software will be installed with the minimum number of services required to fulfill the designated function.
- SG19.5** Security-related operating system or software application patches must be reviewed and installed periodically consistent with the criticality and vulnerability of the resource.
- SG19.6** Operating systems software will provide application software environments for all non-OS activities, which are rigorously separated from the operating system environment.
- SG19.7** The direct use of host hardware environments shall be controlled by an operating system function(s).
- SG19.8** Application software use of the host hardware environment is through the OS environment through specifically defined interfaces for those purposes.
- SG19.9** Use of OS functions and functionality by application software will be through specifically defined interfaces for those purposes.
- SG19.10** Application software, as distinguished from Operating Systems software, will be unable to assume access privileges normally reserved to the operating system.
- SG19.11** Separate application environments/software will be partitioned in a rigorous well-defined fashion, with the only interaction between separate application environments/software being under operating system software control.
- SG19.12** Any use of host operating systems and application environments which does not conform to this standard will be phased out as soon as possible.
- SG19.13** Changes to Operating Systems and application software by TWC IT to strengthen system integrity and increase security may be undertaken as needed.

## **SG20.0 Passwords**

The TWC Password Standard establishes rules related to the User authentication process, including the creation, distribution, safeguarding, termination and reclamation of those mechanisms. Exceptions to this policy may be allowed temporarily for certain legacy systems.

- SG20.1** All passwords must comply with the TWC Password Standard in force at the time of creation.
- SG20.2** User chosen passwords must adhere to a minimum length and format as defined by current password guidelines:
  - SG20.2.1** Contain at least one each of upper and lower case letters and least one number
  - SG20.2.2** Are at least six characters in length (8 characters are encouraged)
  - SG20.2.3** Passwords should not have consecutive duplicate characters such as 99 or BB
  - SG20.2.4** Passwords should not have consecutive-count numbers or letters such as 1234 or ABCD
  - SG20.2.5** Passwords are not words in any dictionary including, slang, dialect, jargon, etc.
  - SG20.2.6** Passwords are not based on personal information such as names, birthdates, etc.
  - SG20.2.7** Passwords should be easily remembered
  - SG20.2.8** Passwords should never be the same as the User ID
- SG20.3** Users must not write down passwords and store them near their computer.
- SG20.4** Users must not share their passwords.
- SG20.5** If a password's security is in doubt, it must be changed immediately.
- SG20.6** If a User suspects his/her password has been compromised it must be changed immediately and their supervisor and/or Help Desk notified of the suspected compromise.
- SG20.7** New or temporary passwords issued to a User must be changed upon User's receipt or creation of permanent password.
- SG20.8** All passwords must have an expiration period not to exceed 180 days or as defined by the most current Passwords Standards.
- SG20.9** Stored passwords must be encrypted.
- SG20.10** User account passwords must not be divulged to anyone. TWC IT staff or its contractors/representatives will not ask for User account passwords except as allowed by law.
- SG20.11** TWC network administrators will not circumvent the password policy for the sake of expediency.
- SG20.12** Users may not circumvent password entry with auto-logon, application remembering, embedded scripts or hard coded passwords in client software. (NOTE: Exceptions may be made for specific applications with the approval of the TWC IT management. All exceptions must include a procedure to change the password if necessary.)
- SG20.13** If an agency staff member needs temporary access to another staff member's files, the staff member's supervisor must send this request to TWC IT in writing.

## SG21.0 Peer-to-Peer

Peer-to-Peer software is defined by Governors Executive Order as “computer software, other than computer and network operating systems that has as its primary function the capability of allowing the computer on which the software is used to designate files available for transmission to another computer using the software to transmit files directly to another computer using the software and to request transmission of files from another computer using the software.”

Peer-to-Peer networks rely primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. Such networks are used for sharing content files containing audio, video, data or anything in digital format as well as real-time data such as telephony traffic.

This standard applies to Peer-to-Peer (P2P) used within the Texas Workforce Commission (TWC) and P2P 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. In all cases users of TWC information resources shall comply with all Information Security Standards and Guidelines as they apply to a particular circumstance and with special consideration for requirements related to Acceptable Use and the Information Security Program statement on Responsibilities and Rules of Behavior.

- SG21.1** P2P usage within TWC must be authorized in writing by the Information Resources Manager (IRM), Director of Information Technology, Director of Data Processing or their designee(s).
- SG21.2** P2P usage within TWC environments will be only for legitimate state business. Users of TWC computers or networks that are authorized to use P2P technologies will not download any illegal and/or unauthorized copyrighted content. If authorized for use P2P may be used for any routine official business that is not normally filed for recordkeeping.
- SG21.3** No state business that is filed for record keeping (records retention) shall be conducted making use of P2P.
- SG21.4** P2P applications that permit the sharing of files across or within the TWC network make it easy to share music, videos, movies, software, or text and/or picture files. Often times these are copyrighted files where the copyright is owned by an individual or entity other than the individual sharing the file. Sharing these files without the explicit permission of the copyright owner may be a violation of federal copyright law.
- SG21.5** **The Texas Workforce Commission cannot protect you from a copyright complaint.** In fact, TWC may be legally required to assist a complainant in pursuing action against you in the event of copyright violation. Penalties for copyright violations can range from loss of network access privileges on TWC networks to civil and/or criminal prosecution. You are not protected simply because you may have received these materials at no cost or that you are sharing them at no cost. **Your only protection is to not possess or distribute any unlicensed copyrighted materials.**
- SG21.6** Users of TWC Computers or networks will not download/install or use any P2P software or participate in any P2P network on TWC computers, networks or mobile computing devices (laptops, PDAs) without the specific written authorization to do.
- SG21.7** Users of TWC computers and networks should always keep in mind that all P2P traffic may be recorded and stored along with the source and destination. Employees have no expectation of privacy with regard to P2P transactions. Management has the ability and right to view users' P2P transactions on TWC systems and networks.
- SG21.8** P2P transactions on TWC systems are the property of the State of Texas held in trust by TWC and may be subject to requirement of the Texas Public Information Act and rules related to the retention of State of Texas records.
- SG21.9** There is no provision for personal use of P2P on TWC networks. Personal use of P2P software or networks is prohibited in all circumstances.

- SG21.10** P2P shall not impede the conduct of other state/TWC business.
- SG21.11** Using P2P to access, view, download, upload, forward, print, copy, post or share in any way racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable materials (visual, textual or auditory) is strictly prohibited. Such usage will be reported to the appropriate authorities by TWC.
- SG21.12** Using P2P to transmit or receive copyrighted materials of any nature (audio, video, still picture, etc.) for which the copyright is not owned by TWC and/or the State of Texas is prohibited at all times.

## **SG22.0 Physical Access**

The Physical Access Standard establishes rules for granting, controlling, monitoring and removing physical access to TWC Information Resource facilities. Each Building, Department or Secured Room must have a documented Facility Security Plan.

- SG22.1** Physical security systems must comply with applicable regulations such as building codes and fire regulations.
- SG22.2** Physical access to all restricted facilities or areas must be documented and managed.
- SG22.3** Information Resource facilities must be physically protected in proportion to the importance of their function within TWC.
- SG22.4** Access to Information Resource facilities must be granted only to Users whose job responsibilities require routine and on-going access. Exceptions to apply to those facilities shared in common with other state agencies.
- SG22.5** The process for granting access, via key-card or otherwise, to information resource facilities must include the approval of the designated office or staff person responsible for the facility.
- SG22.6** Each User granted access to information resource secured facilities must sign the appropriate access and non-disclosure agreements.
- SG22.7** The User's Supervisor must initiate requests for access to Information Services secured facilities.
- SG22.8** Access to secured facilities and/or key-cards must not be shared or loaned.
- SG22.9** Access materials and/or key-cards that are no longer required must be returned to the appropriate TWC representative. Under no circumstances is a "retired" card to be passed directly to another User.
- SG22.10** Lost or stolen access key-cards must be reported to the appropriate TWC representative immediately upon the User becoming aware of the loss.
- SG22.11** Any TWC secured facility that allows access to visitors will track visitors' access with a sign in/out log.
- SG22.12** Visitors to controlled facilities must be escorted at all times.
- SG22.13** Access records, entry and exit logs, and visitor logs must be kept based on records retention or other state or federal requirements.
- SG22.14** Functional capabilities for an access key-card must be inactivated upon termination of need or following 60 days of non-use.
- SG22.15** Signs posted to inform of the restricted access to certain rooms or buildings must be posted in a manner that serves their purpose without drawing attention to the secured nature of the site.
- SG22.16** "Piggybacking" – the act of following an authorized staff person into a secured area is strictly prohibited except when visitors are being escorted by authorized staff.

### **SG23.0 Portable/Remote Computing**

The TWC Portable Computing Security Standard establishes rules necessary to mitigate risks associated with the use of mobile computing devices and their connection to the TWC network(s).

- SG23.1** Portable computing devices may be used to access TWC information resources based on prior approval by the IRM or designee.
- SG23.2** TWC owned/leased portable computing devices must be password protected or use a mechanism to encrypt electronic protected data of a confidential and/or sensitive nature.
- SG23.3** Remote access to TWC information resources by means of non-TWC owned/leased computing devices must provide User authentication including at a minimum a unique User identifier and a password.
- SG23.4** TWC data should not be stored on portable computing devices. In the event there is no alternative to local storage all confidential and/or sensitive TWC data must be encrypted and/or all access to the computing capabilities of the device must require an authenticated login.
- SG23.5** In the case of remote access from approved home-based computing devices approved and up-to-date firewall and antivirus protection must be installed and maintained by the remote User.
- SG23.6** Non-TWC systems that require network connectivity must conform to TWC standards and guidelines and must be approved by TWC IT.
- SG23.7** Unattended portable computing devices must be physically secured by locking devices and/or locked storage.
- SG23.8** Portable computing devices must maintain active antivirus protection and appropriate security patch levels equivalent to those applied to any other TWC computing device.
- SG23.9** All TWC security policies, standards, guidelines and procedures must be followed when using remote access. Additionally, remote access requires security measures beyond those used in TWC office facilities. These extra measures include:
  - SG23.9.1** Prohibition against password storage on the remote system
  - SG24.9.2** Prohibition against automatic sign-on scripts containing a User's password.
- SG23.10** Loss or theft of portable computing devices must be reported immediately upon discovery.

## **SG24.0 Privacy Policies**

The purpose of the TWC Privacy Standard is to clearly communicate the TWC Information Services Privacy expectations to Users of TWC information Resources. The standard includes:

- SG24.1** Internal Users of TWC information resources should have no expectation of privacy with respect to the use of those resources.
- SG24.2** External Users of TWC information resources should have the expectation of privacy, except in the case of suspected wrongdoing, with respect to TWC information resources. However, aggregate information from the analysis of logs may be used without compromising individual privacy.
- SG24.3** Electronic files created, sent, received, or stored on TWC owned, leased, administered information resources, or otherwise under the custody and control of TWC are not private and may be accessed by TWC IT employees at any time without knowledge of the resource User or Owner.
- SG24.4** To enforce security, TWC IT may log, review, and otherwise utilize any information stored on or passing through TWC information resources in accordance with provisions and safeguards provided by Title 1, Texas Administrative Code, Chapter 202.
- SG24.5** To enforce security, TWC IT may capture User activity such as telephone numbers dialed or web sites visited, in accordance with provisions and safeguards provided by Title 1, Texas Administrative Code, Chapter 202.
- SG24.6** To assure the protection of private, confidential and/or sensitive data stored on TWC information resources, prior to media or equipment re-use or disposal, a data sanitization guideline in compliance with TAC 202.28 must be followed.

## **SG25.0 Removable Media**

The TWC Removable Media Security Standard establishes those rules necessary to protect the data and the networks of TWC and satisfies compliance requirements of state and federal rule and law with regard to disposal and reuse of media that contain protected, confidential and/or sensitive information. These devices include, but are not limited to:

- Diskettes, tapes and/or compact disks
- Memory cards/sticks used in various portable digital devices
- Firewire/USB "Flash"/Key/Pen/Thumb drive memory devices
- Portable mass storage devices
- Personal audio/video players

**SG25.1** The use of personally owned removable media is prohibited without specific exemption granted by the IRM or designee.

**SG25.2** Sensitive TWC data stored on removable media must be encrypted.

**SG25.3** In the event of loss or theft of the removable media, the description of the data and index or table of contents must be provided with the report of loss or theft.

**SG25.4** All removable media must be scanned for malicious code content prior to use in TWC systems and/or networks.

**SG25.5** Reuse or disposal of removable media will follow a data sanitization guideline in compliance with TAC 202.28, to assure removal of any electronic protected, confidential and/or sensitive information

## **SG26.0 Security Monitoring**

The purpose of the Security Monitoring Standard is to ensure adequate controls are in place, are followed, and are effective.

**SG26.1** Automated monitoring tools provide real-time notification of suspected or actual wrongdoing and vulnerabilities. Where possible security baselines should be developed and the appropriate monitoring tools used to report exceptions.

**SG26.2** Files may be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by their define level of risk. Such files include but are not limited to:

**SG26.2.1** Automated intrusion detection logs

**SG26.2.2** Firewall logs

**SG26.2.3** User account logs

**SG26.2.4** Network scanning logs

**SG26.2.5** System logs

**SG26.2.6** Application logs

**SG26.2.7** Backup and recovery logs

**SG26.2.8** Network printer and network fax logs

**SG26.2.9** E-mail logs (6-24-2008)

**SG26.3** The following areas will be reviewed periodically to assure compliance:

**SG26.3.1** Appropriate use of passwords

**SG26.3.2** Unauthorized network connected devices

**SG26.3.3** Unauthorized personal servers (web, email, ftp, etc.)

**SG26.3.4** Unsecured sharing of network connected devices

**SG26.3.5** Unauthorized modem use

**SG26.3.6** Operating system and software licenses

## **SG27.0 Security Training**

The purpose of the Security Training Standard is to ensure Users are aware of and adhere to security requirements.

- SG27.1** New Users must complete an approved security awareness training program prior to, or within thirty days of being granted access to any TWC information resource.
- SG27.2** Users must sign the Information Resources Usage Agreement/P-41 stating they have read and understand TWC requirements regarding computer security policies and procedures prior to accessing any information resources.
- SG27.3** Users must be provided with sufficient training and support reference materials to allow them to properly protect TWC information resources.
- SG27.4** TWC IT must ensure that copies of the Information Security Program, Information Security Policy and Information Security Standards and Guidelines are available to Users.
- SG27.5** Users must reaffirm their commitment to the protection of TWC Information Resources by completing an annual security awareness training program.
- SG27.6** TWC IT must maintain a process enabling the communication of new computer security program information, security bulletin information and security items of interest.

## **SG28.0 Server Hardening**

The Server Hardening Standard is created to ensure that TWC servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in services provided.

- SG28.1** A server may not be connected to the TWC network until it is in a TWC IT accredited secure state and the network connection is reviewed and approved by TWC Information Services and Enterprise Security.
- SG28.2** The TWC server hardening procedure shall include, but is not limited to:
  - SG28.2.1** Operating systems may only be installed from TWC IT approved sources.
  - SG28.2.2** Vendor supplied patches shall be applied.
  - SG28.2.3** Unnecessary software, system services and drivers shall be removed
  - SG28.2.4** Appropriate security parameters, field protections and audit-logging capabilities shall be set.
  - SG28.2.5** Default account passwords shall be disabled or changed as appropriate.
  - SG28.2.6** Vulnerability assessment will be run against the server before being placed into production.
- SG28.3** TWC IT will monitor security issues and will manage the release of security patches on behalf of TWC.
- SG28.4** TWC IT will test security patches, as appropriate, against core resources prior to their release. Where practical staff will test patches on non-production systems before deployment.
- SG28.5** TWC IT may make hardware resources available for testing of security patches in the case of special applications.
- SG28.6** Security patches must be implemented within the specified timeframe after notification by TWC IT.

## **SG29.0 Systems Development**

The purpose of the Systems Development Standard is to ensure the development and implementation of new software meets the requirements necessary to assure the security of TWC network(s) and systems.

- SG29.1** Systems development projects shall adhere to a Software Development Life Cycle (SDLC) approved by the IRM or designee.
- SG29.2** Production systems must have a designated Owner and Custodian.
- SG29.3** Production systems must have an access control system to restrict access to the system as well as restrict the privileges available to Users.
- SG29.4** Confidential data must be protected during SDLC phases.
- SG29.5** Application program-based access paths, other than the formal User access paths, must be deleted or disabled prior to the software being moved into production.
- SG29.6** Procedures must be established to restrict access to systems and software for purposes of testing and revision to only authorized personnel.
- SG29.7** No alternate entry points (aka back-doors) may be installed or coded into any system that would bypass TWC user controls and security implementations.
- SG29.8** Testing and development environments shall be physically or logically separated from production resources.
- SG29.9** Test and development data shall be sanitized of any private or confidential information. Alternately, all individuals having access to that data shall have the proper clearances for the data.

### **SG30.0 Vendor Access**

The TWC Vendor Access Standard is intended to assure the security of TWC information resource assets when vendor interaction is involved. The TWC Vendor Access Standard shall apply to any contractor as well.

- SG30.1** Vendors must comply with all applicable TWC policies, practices, standards, guidelines and agreements, including acceptable use, auditing, safety, security, licensing, passwords and privacy.
- SG30.2** Vendor agreements must specify the TWC information to which the vendor should have access.
- SG30.3** Vendor agreements must specify how the TWC information is to be protected by the vendor. These protections must meet or exceed the existing protections within the TWC networks for that information.
- SG30.4** Vendor agreements must specify that upon the departure of a vendor employee all TWC materials will be collected and returned to TWC or destroyed, as appropriate, and that the vendor will return or destroy all TWC information and provide written assurance of that destruction upon termination of the agreement or at the request of TWC.
- SG30.5** Vendor agreements must specify that TWC information will be used only for the purpose of the terms of the business agreement.
- SG30.6** Vendor agreements must specify that any additional TWC information encountered during the fulfillment of the agreement cannot be used for the vendor's own purposes or disclosed to others.
- SG30.7** TWC will provide an IT contact for the vendor. This individual shall work with the vendor to ensure compliance with applicable TWC requirements.
- SG30.8** Vendors must provide TWC IT with a list of all employees of the vendor who will be performing work on the contract/agreement. This list must be updated within 24 hours of any change.
- SG30.9** Vendor employees must report all security incidents directly to the appropriate TWC staff.
- SG30.10** Vendors must follow all applicable TWC change control processes and procedures.
- SG30.11** Any vendor owned information resources equipment and/or maintenance equipment connected to the TWC network with the intent of additional connection outside the TWC network via the network, telephone lines, leased lines or any other method will remain disabled except when in use for the purpose of authorized maintenance functions or other functions clearly defined in the terms of the vendor agreement.
- SG30.12** Vendors must comply with all State and TWC auditing requirements, including the auditing of the vendor's work.
- SG30.13** All software used by the vendor in the provision of services to TWC must be properly inventoried and licensed.

### **SG31.0 VPN – Virtual Private Network**

The TWC VPN Security Policy establishes those rules necessary to mitigate risks associated with remote connections to the TWC network(s) made by means of an approved VPN connection.

- SG31.1** Approved Users may utilize the benefits of VPN. VPN access, granted by request to TWC, is a “User managed” service. In all events, the User is responsible for the selection of a provider of service, coordinating installation, installing any required software, and paying required fees.
- SG31.2** VPN connected equipment is subject to the same rules, policies and regulations that apply to any TWC owned equipment.
- SG31.3** It is the User’s responsibility, when connected to TWC networks, to assure that unauthorized Users are not allowed access to the TWC networks.
- SG31.4** The use of VPN access to TWC networks must be controlled by using password authentication, token devices, or public/private key systems incorporating a strong pass phrase.
- SG31.5** VPN connections to TWC networks must force all traffic over the VPN tunnel: all other traffic will be dropped.
- SG31.6** Any computing device connected to TWC networks or any other TWC technology must be protected by the use of a firewall that satisfies the standards of TWC.
- SG31.7** Any computing device connected to TWC networks or any other TWC technology must use anti-virus software and configurations approved by TWC IT. Configuration will include real time as well as passive scanning and maintain current virus definitions.
- SG31.8** VPN connections will be automatically disconnected after a period of non-use or inactivity. In such an event, the User must log in again.
- SG31.9** The use of any technology to maintain an inactive connection (ping, stay-connect, etc.) is prohibited and can result in termination of the VPN account.
- SG31.10** Only computing devices with a TWC inventory tag, complying with TWC standards and security polices will be authorized to have the TWC VPN client installed.
- SG31.11** The use of any VPN client other than the one provided by TWC or its service provider is prohibited.
- SG31.12** The VPN User must monitor and report intrusion or incidents to TWC as set forth in the TWC Information Security Standards and Guidelines.
- SG31.13** The VPN User is subject to audit (internal or external) to insure compliance with this VPN standard and TWC policies, standards and guidelines.

### **SG32.0 Wireless Computing**

The TWC Wireless Computing Standard establishes those rules necessary to mitigate risks associated with the use of devices that have the capability to connect to networks without the use of wires or cables, such as but not limited to:

- Wireless base and/or access points (built-in or free-standing)
- Personal Digital Assistants (PDA) or cellular/digital PDA-based telecommunication devices (smart phones or PC phones) with wireless connectivity capabilities (built-in or free-standing)
- Laptop/Notebook computers with wireless connectivity capabilities (built-in or free-standing)
- Wireless transmitting and/or receiving devices used to transfer audio, video, image or data of any sort.

- SG32.1** The User is responsible for the protection of all sensitive, confidential or private information to which they may have access either as a granted right or by accidental exposure.
- SG32.2** All employees, providers, and vendors are prohibited from using or installing any device which functions in wireless mode in order to access data, transfer data or connect in any manner to TWC networks or systems without the approval and assistance of TWC IT staff.
- SG32.3** The only exemptions shall be for equipment specifically tested, installed and maintained with configurations that protect all TWC data and resources in accord with other sections of this document and requirements of state and federal rule and law.
- SG32.4** The exemption approval authority shall be the IRM or designee.