



**Policy: Payment Card Industry
Security Policy**

Date: 10-20-09

Rev Date:

Overview

This document summarizes The Wellness Community of Central New Jersey's comprehensive written Information Security Policy mandated by the PCI DSS Security Compliance Program. In particular, this document describes the Security Policy elements pursuant to which TWC-CNJ intends to (i) ensure the security and confidentiality of card holder data, (ii) protect against any anticipated threats or hazards to the security of such data, and (iii) protect against the unauthorized access or use of such card holder data records or information in ways that could result in substantial harm or inconvenience to customers. The Security Policy incorporates by reference TWC-CNJ's policies and procedures enumerated below and are in addition to any TWC-CNJ policies and procedures that may be required pursuant to other federal and state laws and regulations.

Designation of Representatives

TWC-CNJ's Executive Director is designated as the Security Officer who shall be responsible for coordinating and overseeing the Security Policy. The Security Officer may designate other representatives of TWC-CNJ to oversee and coordinate particular elements of the Security Policy. Any questions regarding the implementation of the Security Policy or the interpretation of this document should be directed to the Security Officer or his or her designees.

Scope of Security Policy

The Security Policy applies to all types of sensitive information including any record containing sensitive and confidential information about a employee or card holder or a customer who has a relationship with TWC-CNJ, whether in paper, electronic or other form that is handled or maintained by or on behalf of TWC-CNJ or its affiliates. In addition, if needed, the Security Officer will work with the legal department to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards to comply with the Payment Card Industry Standard.

Important Note:

For these purposes, the term card holder information includes any information

- (i) Provided by the card holder in conjunction with a transaction to purchase or obtain a product or service from TWC-CNJ,*
- (ii) Elements of the card holder data includes cardholder name, primary account number (PAN), Service Code, Expiration date*
- (iii) Sensitive Authentication data such as Full Magnetic Stripe, CVC2/CVW2/CID, PIN/PIN Block.*

Elements of the Security Policy

1. Risk Identification and Assessment. TWC-CNJ intends, as part of the Security Policy, to undertake a review on an annual basis to identify and assess external and internal risks to the security, confidentiality, and integrity of information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Security Policy, the Security Officer will establish procedures for identifying and assessing such risks in each relevant area of TWC-CNJ's operations, including:

Employee training and management. The Security Officer will coordinate with key employees to evaluate the effectiveness of the Company's procedures and practices relating to access to and use of card holder data. This evaluation will include assessing the effectiveness of TWC-CNJ's current policies and procedures in this area.

Information Systems and Information Processing and Disposal. The Security Officer will coordinate with individuals responsible for the IT matters to assess the risks associated with TWC-CNJ's information systems, including network and software design, information processing, and the storage, transmission and disposal of card holder data and information. This evaluation will include assessing TWC-CNJ's current policies and procedures relating to document retention and destruction. The Security Officer will also coordinate with individuals responsible for the IT matters to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

Detecting, Preventing and Responding to Attacks. The Security Officer will with individuals responsible for the IT matters to evaluate procedures for and methods of detecting, preventing and responding to attacks

or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Security Officer may elect to delegate to another employee the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by TWC-CNJ.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of sensitive information such as card holder data, whether in electronic, paper or other form. The Security Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The Security Officer shall coordinate with those responsible for the third party service procurement to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for protecting card holder data and other third parties to which they will have access. In addition, the Security Officer will work with the legal department to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards to comply with the PCI DSS requirements. Any deviation from these standard provisions will require the approval of the legal department. These standards shall apply to all existing and future contracts entered into with such third party service providers.

4. Incident Management Policy. TWC-CNJ's Information Technology Resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. All information security incidents must be reported in accordance with the policies and procedures provided below regardless of whether or not damage appears to have been incurred. The incident management process is the responsibility of the Executive Director.

5. Adjustments to Security Policy. The Security Officer is responsible for evaluating and adjusting the Security Policy based on the risk identification and assessment activities undertaken pursuant to the Security Policy, as well as any material changes to TWC-CNJ's operations or other circumstances that may have a material impact on the Security Policy.

Terminology

Security Officer - A person responsible within TWC-CNJ for coordinating and overseeing this Security Policy. The Security Officer may designate other representatives of TWC-CNJ to oversee and coordinate particular elements of the Security Policy.

Information Technology Resources (ITR) - Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from TWC-CNJ campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on TWC-CNJ premises may be appropriate.

Vendor: A third party who provides one or more services that includes software, hardware, or other type of service to TWC-CNJ.

Connected Entity: Any foreign entity that is connected to the cardholder environment. In most instances a connected entity will be a connected third party, but this will vary depending on how TWC-CNJ has segmented their environment. In most cases the reference is to third-parties such as VPN connections to acquirers/processors, network connection to vendor or client, external dedicated network connections (i.e. VPN, frame-relay, etc.)

Internet Use Policy

Introduction - 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 employees, contractors and third parties who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

Audience - The Internet Use Policy applies equally to all employees, contractors and third parties granted access to any 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 company are the property of TWC-CNJ.

Privacy - Electronic files created, sent, received, or stored on Information Technology Resources owned, leased, administered, or otherwise under the custody and control of company are not private and may be accessed by company administrators at any time without knowledge of the Information Technology Resources user or owner.

Internet Use Policy

- Software for browsing the Internet is provided to authorized users for business use only.
- All software used to access the Internet must be part of TWC-CNJ standard software suite or approved by the Security Officer. This software must incorporate all vendor provided security patches.
- All files downloaded from the Internet must be scanned for viruses using the approved IT distributed software suite and current virus detection software.
- All software used to access the Internet shall be configured to use the firewall http proxy.
- All sites accessed must comply with TWC-CNJ Acceptable Use Policies.
- All user activity on Company Information Technology Resources assets is subject to logging and review.
- Content on all Company Web sites must comply with TWC-CNJ Acceptable Use Policies.
- No offensive or harassing material may be made available via Company Web sites.
- Non-business related purchases made over the internet are prohibited. Business related purchases are subject to Company procurement rules.
- No personal commercial advertising may be made available via Company Web sites.
- Company internet access may not be used for personal gain or non-Company personal solicitations. No Company data will be made available via Company Web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive Company 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.

Permitted Use

- Incidental personal use of Internet access is restricted to TWC-CNJ approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to TWC-CNJ.
- 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 liability for, or embarrassment to TWC-CNJ.
- Storage of personal files and documents within TWC-CNJ's Information Technology Resources should be nominal.
- All files and documents – including personal files and documents – are owned by TWC-CNJ, may be subject to open records requests, and may be accessed in accordance with this policy.

Disciplinary Actions for Violation

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Email Policy

Introduction

This policy is established to achieve the following:

1. ... To ensure compliance with applicable statutes, regulations, and contractual mandates regarding the management of information resources.
2. ... To establish prudent and acceptable practices regarding the use of email.
3. ... To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of TWC-CNJ Email Policy is to establish the rules for the use of TWC-CNJ email for the sending, receiving, or storing of electronic mail.

Audience

TWC-CNJ Email Policy applies equally to all individuals granted access privileges to any TWC-CNJ information resource with the capacity to send, receive, or store electronic mail.

Email Policy

- The following activities are prohibited by policy:
 - § Sending email with any type sensitive information such as Credit card data or personally identifiable information (PII).
 - § Sending email that is intimidating or harassing.
 - § Using email for conducting personal business.
 - § Using email for purposes of political lobbying or campaigning.
 - § Violating copyright laws by inappropriately distributing protected works.
 - § Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - § The use of unauthorized e-mail software.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - § Sending or forwarding chain letters.
 - § Sending unsolicited messages to large groups except as required to conduct agency business.
 - § Sending excessively large messages.
 - § Sending or forwarding email that is likely to contain computer viruses.
- All user activity on TWC-CNJ Information Technology Resources assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of TWC-CNJ or any unit of TWC-CNJ unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing TWC-CNJ. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."
- Individuals must not send, forward or receive confidential or sensitive TWC-CNJ information through email accounts.
- Individuals must not send, forward, receive or store confidential or sensitive TWC-CNJ information utilizing non-TWC-CNJ accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers, Blackberry's and cellular telephones.

Disciplinary Actions for Violations - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Account Management Security Policy

Introduction - Computer accounts are the means used to grant access to 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 Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience - The Account Management Security Policy applies to all individuals within TWC-CNJ enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Technology Resources Security, and data owners.

Account Management Security Policy

- All accounts created must have an associated request and approval that is appropriate for the system or service.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with TWC-CNJ Password Policy.
- All accounts must have a password expiration that complies with TWC-CNJ 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.
- System Administrators or other designated staff are responsible for removing the accounts of individuals that change roles within company or are separated from their relationship with company.
- System Administrators or other designated staff are responsible must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
- System Administrators or other designated staff must have a documented process for periodically reviewing existing accounts for validity.
- System Administrators or other designated staff are subject to independent audit review.
- System Administrators or other designated staff must provide a list of accounts for the systems they administer when requested by authorized management.

Disciplinary Actions for Violations - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Physical Access Policy

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 Technology Resources facilities is extremely important to an overall security program.

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

Audience - TWC-CNJ Physical Access Policy applies to all individuals within TWC-CNJ enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Technology Resources Security, and data owners.

Physical Access Policy

- 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 Technology Resources restricted facilities must be documented and managed.
- All ITR facilities must be physically protected in proportion to the criticality or importance of their function at TWC-CNJ.
- Access to Information Technology Resources facilities must be granted only to TWC-CNJ support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to Information Technology Resources facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an Information Technology Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable TWC-CNJ 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 Technology 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 Technology Resources facility.
- Cards and/or keys must not have identifying information other than a return mail address.
- All Information Technology Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for Information Technology Resources facilities must be kept for routine review based upon the criticality of the Information Technology Resources being protected.
- The person responsible for the Information Technology Resources facility must remove the card and/or key access rights of individuals that change roles within TWC-CNJ or are separated from their relationship with TWC-CNJ.
- Visitors must be escorted in card access controlled areas of Information Technology Resources facilities.
- The person responsible for the Information Technology Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the Information Technology Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Disciplinary Actions for Violations - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Incident Management Policy

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 section 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 Technology Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

Audience - TWC-CNJ Incident Management Policy applies equally to all individuals that use any Company Information Resources.

Incident Management Practice Standard

- Company Incident Management Team (CIMT) members have pre-defined roles and responsibilities which can take priority over normal duties.
- 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 Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIMT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The Security Officer, working with the Incident Management Manager (IMM), will determine if a widespread Company communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIMT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIMT.
- TWC-CNJ Security Officer is responsible for reporting the incident to the:
 - § Local, state or federal law officials as required by applicable statutes and/or regulations
- The Security Officer is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the Security Officer will recommend disciplinary actions.
- In the case where law enforcement is involved, the Security Officer will act as the liaison between law enforcement and Company.

Disciplinary Actions for Violations - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Network Access Policy

Introduction - TWC-CNJ network infrastructure is provided as a central utility for all users of TWC-CNJ Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet TWC-CNJ 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 TWC-CNJ 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 TWC-CNJ information.

Audience - TWC-CNJ Network Access Policy applies equally to all individuals with access to any TWC-CNJ Information Resource.

Network Access Policy

- Users are permitted to use only those network addresses issued to them by TWC-CNJ's Information Technology team.
- All remote access (dial in services) to TWC-CNJ will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to TWC-CNJ Information Technology Resources only through an ISP and using protocols approved by Company.
- Users inside TWC-CNJ firewall may not be connected to TWC-CNJ network at the same time a modem is being used to connect to an external network.
- 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 TWC-CNJ network without TWC-CNJ IT approval.
- Users must not install network hardware or software that provides network services without TWC-CNJ IT approval.
- Non TWC-CNJ computer systems that require network connectivity must conform to TWC-CNJ IT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, TWC-CNJ users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to TWC-CNJ network infrastructure.
- Users are not permitted to alter network hardware in any way.

Disciplinary Actions for Violations - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of TWC-CNJ Information Technology Resources access privileges, civil, and criminal prosecution.

Backup & Disaster Recovery Policy

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 TWC-CNJ Backup/DRP Policy is to establish the rules for the backup and storage of electronic TWC-CNJ information.

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

Backup & Disaster Recovery Policy

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- TWC-CNJ Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for TWC-CNJ must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest TWC-CNJ sensitivity level of information stored.
- A process must be implemented to verify the success of TWC-CNJ electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s) for access to TWC-CNJ backup media must be reviewed annually or when an authorized individual leaves TWC-CNJ.
- Procedures between TWC-CNJ and the offsite backup storage vendor(s) must be reviewed at least annually. (Please refer to Managing Third Party Vendors Policy for more details)
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
 - § System name
 - § Creation Date
 - § Sensitivity Classification
 - § TWC-CNJ

Disciplinary Actions - Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TWC-CNJ Information Resources access privileges, civil, and criminal prosecution.

Employee Screening Policy

Introduction - Hiring employees with integrity is important to TWC-CNJ. Screening of employees allows verifying the credentials provided by them. This policy also allows TWC-CNJ complies with various federal, state and contractual mandates.

Purpose - The purpose of the Policy is to establish the rules for the screening of the employee during their hiring process.

Audience - TWC-CNJ Employee Screening Policy applies to all individuals within TWC-CNJ enterprise who is considering employment with TWC-CNJ.

Employee Screening Policy

- All applicants for employment with TWC-CNJ are asked to sign a release form authorizing the appropriate background checks. Any applicant who refuses to sign a release form is no longer considered eligible for employment.
- Applicants also are expected to provide references from their former employers as well as educational reference information that can be used to verify academic accomplishments and records. The background check will include verification of information provided on the completed application for employment, the applicant's resume or on other forms used in the hiring process.
- Information to be verified includes, but is not limited to, social security number and previous addresses. TWC-CNJ will also conduct a reference check and verification of the applicant's education and employment background as stated on the employment application or other documents listed above. The background check may also include criminal court record searches. If a conviction is discovered, a determination will be made whether the conviction is related to the position for which the individual is applying or presents safety or security risks before an employment decision is made.
- Additional checks such as a driving record or credit record may be made on applicants for particular job categories if appropriate and job related. If an applicant is denied employment in whole or in part because of information obtained in his/her background check, the applicant will be informed of this and given the name, address and phone number of the screening provider to contact if s/he has specific questions about the result of the check or wants to dispute its accuracy.

Disciplinary Actions for Violations - Any applicant who provides misleading, erroneous or willfully deceptive information to TWC-CNJ on an employment form or resume or in a selection interview is immediately eliminated from further consideration for employment with TWC-CNJ.

Awareness & Training

Introduction - Effective information security requires a high level of participation from all employees of TWC-CNJ. Ensuring all individuals understand the security needs of protecting TWC-CNJ data is important to comply with federal, state or other contractual mandates.

Purpose - This policy defines responsibilities and roles for instilling information security awareness among all information resource owners, managers, service providers and users.

Audience - TWC-CNJ Awareness & Training applies to all individuals within TWC-CNJ enterprise.

Awareness & Training Policy

- All must be well informed of their responsibilities as Information Owners, Managers, Users, and Service Providers.
- In cooperation with the training office, TWC-CNJ Information Security Officer is responsible for managing a training and awareness program for all individuals of TWC-CNJ and for consulting with members of TWC-CNJ on information security issues.
- Training classes and materials will be offered to instill the importance of appropriate information handling and to explain the implications of this Policy.
- Training will offered at least annually to all employees using various means online, classroom, posters, direct communication.
- Training should include specific information on the use of security precautions such as encryption, anti-viral tools, backup procedures, physical security and awareness of social engineering tactics.
- TWC-CNJ Security Officer is responsible for maintaining the security program, which makes the information resources described in this Policy available to TWC-CNJ individuals.
- Managers and responsible for seeing that their employees take advantage of available security awareness resources.
- Information Owners and Vendors must become familiar with standard information security principles and procedures as they apply to the information resources under their care.

Disciplinary Actions for Violations - Any applicant who provides misleading, erroneous or willfully deceptive information to TWC-CNJ on an employment form or resume or in a selection interview is immediately eliminated from further consideration for employment with TWC-CNJ.

List of Connected Entities

Name of Entity	Description
VPN	Employees for remote work access

Employee Acknowledgement

(This acknowledgement must be signed at least once a year by the employee after reading the policy document)

The employee security policy manual described above is important information about TWC-CNJ. I understand that I should consult my immediate supervisor or Security Officer, if I have any questions that are not answered in the handbook.

I understand and acknowledge that there may be changes to the information, policies, and benefits in the handbook. I understand that TWC-CNJ may add new policies to the handbook as well as replace, change, or cancel existing policies. I understand that I will be told about any handbook changes and I understand that handbook changes can only authorized by the Security Officer or delegated of TWC-CNJ.

I understand and acknowledge that this handbook is not a contract of employment or a legal document. I have received the handbook and I understand that it is my responsibility to read and follow the policies contained in this handbook and any changes made to it.

EMPLOYEE'S NAME (printed):

EMPLOYEE'S SIGNATURE:

DATE: _____