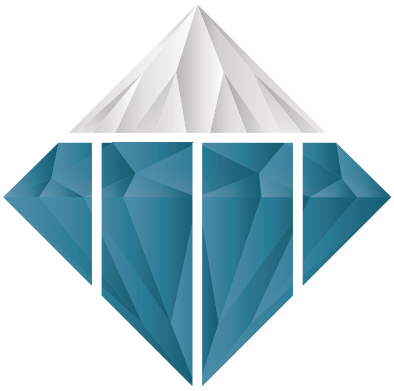

TTI
SUCCESS
INSIGHTS®

TTI SI INFORMATION SECURITY POLICY

CONFIDENTIAL

INFORMATION SECURITY POLICY MANAGER

Brent Rowland
Chief Technology Officer

TTI Success Insights
17785 North Pacesetter Way, Scottsdale, AZ 85255
480.443.1077 or 800.869.6908

TABLE OF CONTENTS

TTI SI INFORMATION SECURITY POLICY

1.0 PURPOSE OF THE INFORMATION SECURITY POLICY

The purpose of this Information Security Policy (the "Policy") is to create an all-encompassing security policy based on Target Training International, Ltd., TTI Success Insights, Inc., and TTI Success Insights North America, Inc.'s (collectively "TTI SI") existing security policy framework and industry best practices for implementation and guidance across TTI SI networks and systems.

2.0 SCOPE OF THE INFORMATION SECURITY POLICY

This Policy applies to employees, contractors, consultants, and other workers at TTI SI, including all individuals affiliated with third parties.

This Policy applies to all physical and network infrastructure that are owned and operated by TTI SI and TTI SI's office building located at 17785 North Pacesetter Way, Scottsdale, Arizona 85255 (the "Facility"). TTI SI utilizes secure, certified third-party datacenters in the following locations: Phoenix (48th Street and Van Buren); Amsterdam; Russia; and Canada. This Policy does not apply to third-party data centers that are not owned or operated by TTI SI.

3.0 FACILITY SECURITY

3.1 SECURITY AREAS

Public

This includes areas of the Facility that are intended for public access.

- Access Restrictions: None
- Additional Security Controls: None
- Examples: Main entrance, lobby, common areas of building

Company

This includes areas of the Facility that are used only by employees and other persons for official company business.

- Access Restrictions: Only TTI SI personnel and approved/escorted guests
- Additional Security Controls: Additional access controls should be used, such as keys, as well as security cameras
- Examples: Hallways, private offices, work areas, conference rooms

Private

This includes areas that are restricted to use by certain persons within TTI SI, such as executives and information technology personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel
- Additional Security Controls: Additional access controls must be used, such as keys or keypads, with access to these areas logged. These areas are monitored by security cameras.
- Examples: Network room, file storage areas

3.2 ACCESS CONTROLS

Access controls are necessary to restrict entry to TTI SI premises where Information Technology is held and security zones to only approved persons.

Keys

The use of keys is acceptable, as long as keys are marked "do not duplicate" and distribution is limited. Keys must not be copied. If a key is lost or stolen, it must be reported to the Facility so that the lock can be immediately rekeyed. If an individual is terminated or resigns, that individual's key must be returned to TTI SI.

Alarm System & Security Cameras

TTI SI mandates the use of professionally monitored alarm systems. The system must be monitored 24x7, with TTI SI personnel being notified if an alarm is tripped at any time. The security cameras record from 5:00 p.m. to 7:00 a.m. Monday through Friday, and 24x7 on weekends.

3.3 ENTRY SECURITY

TTI SI's policy is to provide a safe workplace for personnel. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to TTI SI systems and data.

Use of ID Badges

Identification (ID) badges are useful to identify authorized persons on TTI SI premises. TTI SI has established the following guidelines for the use of ID badges:

- Visitors: Visitor badges are required. If possible, specific, non-generic, badges should identify visitors by name.

Sign-in Requirements

TTI SI maintains a sign-in log in the lobby and visitors must be required to sign in upon arrival. At a minimum, the register must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

Visitor Access

Visitors should be given only the level of access to TTI SI premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by TTI SI. Examples of a trusted visitor may be TTI SI's outside legal counsel, financial advisor, or a courier that frequents the office. Others will be decided on a case-by-case basis.

3.4 PHYSICAL DATA SECURITY

Certain physical precautions must be taken to ensure the integrity of TTI SI's data. At a minimum, the following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
- Personnel must log off or shut down their workstations when leaving for an extended time period or at the end of the workday.
- Network cabling must not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- Network ports that are not in use must be disabled.

3.5 PHYSICAL SYSTEM SECURITY

In addition to protecting the data on TTI SI's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

Minimizing Risk of Loss

In order to minimize the risk of data loss through loss or theft of TTI SI property, the following guidelines must be followed:

- **Unused systems:** If a system is not in use for an extended period of time, it should be moved to a secure area or otherwise secured.
- **Mobile devices:** Special precautions must be taken by employees to prevent loss or theft of mobile devices. Password protection should be used on all employee mobile devices containing TTI SI information.
- **Systems that store confidential data:** Special precautions must be taken to prevent loss or theft of these systems, including physically securing those systems and allowing only authorized individuals to access such systems.

Minimizing Risk of Damage

Systems that store TTI SI data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of TTI SI systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.
- Strong magnets must not be used in proximity to TTI SI systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above TTI SI systems. Beverages must never be placed where they can be spilled onto TTI SI systems.
- Uninterruptible Power Supplies (UPS) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

4.0 DATA SECURITY

4.1 DATA CATEGORIES

Data residing on TTI SI systems is classified into the following categories:

- **Public:** includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
- **Operational:** includes data for basic business operations, communications with vendors, personnel, etc. (non-confidential). The majority of data will fall into this category.
- **Critical:** any information deemed critical to business operations (often this data is both operational and confidential). It is extremely important to identify critical data for security and backup purposes.
- **Confidential:** any information deemed proprietary to the business and customer or personnel personal data, including the following:
  - Employee or customer personally identifiable information (PII)
  - Medical and healthcare information
  - Electronic Protected Health Information (EPHI)
  - Customer data
  - Company financial data
  - Sales forecasts
  - Network diagrams and security configurations
  - Communications about corporate legal matters
  - Passwords
  - Bank account information and routing numbers
  - Payroll information
  - Credit card information
  - Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)
- **Credit Card:** any full credit card primary account number (PAN), encrypted or unencrypted.

4.2 DATA STORAGE/RETENTION

Operational: Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of TTI SI personnel.

Critical: Critical data must be stored on a server that gets the most frequent backups. System-or-disk-level redundancy is required.

Confidential: Confidential data must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential data should be stored under lock and key, with the key secured. Confidential data must not be stored on laptops or other mobile devices without the use of strong encryption or password-protected files. Confidential data must never be stored on non-company-provided machines (i.e., home computers).

Credit Card: Credit card data must be stored within NetSuite. Credit card data must not be stored in any other location, and must not be moved, copied, or placed on backup media.

Data is maintained indefinitely, both online and offline, unless TTI SI is presented with a request to remove records. If destruction of data is requested or appropriate, data will be disposed of in a secure manner pursuant to Section 4.4.

4.3 DATA TRANSMISSION

The following guidelines apply to transmission of the different types of company data.

Operational: No specific requirements apply to transmission of operational data, but, as a general rule, the data should not be transmitted unless necessary for business purposes.

Critical: There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential.

Confidential: Confidential data must not be (1) transmitted outside the TTI SI nework without the use of strong encryption or password-protected files; or (2) left on voicemail systems, either inside or outside of TTI SI's network. When faxing confidential data, personnel must use cover sheets that inform the recipient that the information is confidential.

4.4 DATA DESTRUCTION

The following guidelines apply to the destruction of the different types of company data.

Operational: Cross-cut shredding is required for documents. Storage media should be appropriately sanitized and/or wiped or destroyed.

Critical: Shredding is encouraged if the data in question is considered operational or confidential; the applicable policy statements would apply.

Confidential: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required or disposal in secure shred bin.
- Storage media (CDs, DVDs): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, TTI SI must use the most secure commercially-available methods for data wiping. Alternatively, TTI SI has the option of physically destroying the storage media.

Credit Card: When disposing of physical media that has been used in a device which processes, stores, or transmits credit card data, it must be disposed of in a manner which is compliant with NIST 800-88.

4.5 DATA SECURITY - CONFIDENTIAL DATA

Examples of Confidential Data

The following list is not intended to be exhaustive but provides guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer personally identifiable information (PII)
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data
- Sales forecasts
- Product and/or service plans, details, and schematics
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

Use of Confidential Data

A successful data security policy is dependent on TTI SI personnel knowing and adhering to TTI SI's standards involving the treatment of confidential data. The following applies to how TTI SI personnel must interact with confidential data:

- Personnel must be advised of any confidential data to which they have been granted access. Such data must be marked or otherwise designated "confidential."
- Personnel may only access confidential data to perform their job functions.
- Personnel must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Personnel must protect any confidential data to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their job or the action is approved by their supervisor.
- Personnel must report any suspected misuse or unauthorized disclosure of confidential information immediately to their supervisor in accordance with Section 5 of TTI SI's Emergency Management Plan for Data Security Incidents.
- If confidential data is shared with third parties, such as contractors or vendors, a confidential data or non-disclosure agreement must govern the third parties' use of confidential data.

Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. TTI SI requires that the following guidelines are followed:

- **Strong Encryption.** Strong encryption must be used for confidential data transmitted outside of TTISI. If confidential data is stored on laptops or other mobile devices, it must be stored encrypted or password protected.
- **Authentication.** Strong passwords must be used for access to confidential data. See Section 5.0.
- **Background Checks.** All personnel, new employees and anyone requiring access to or managing access of confidential data must successfully pass a background check prior to being granted the privileged access.
- **Physical Security.** Systems and paper that contain confidential data should always be secured.
- **Printing.** When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers used for confidential data must be located in secured areas.
- **Faxing.** When faxing confidential data, personnel must use cover sheets that inform the recipient that the information is confidential.
- **Emailing.** Confidential data must not be emailed outside TTI SI without the use of strong encryption.
- **Discussion.** When confidential data is discussed, it should be done in non-public places and where the discussion cannot be overheard. If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.
- **Redaction.** Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- **Storage.** Confidential data must never be stored on non-company-provided machines (i.e., home computers and personal mobile devices).

Expanded Security Controls for Credit Card Data

Credit card data is a special type of confidential data requiring additional security controls and specifications. Credit card data must be protected in accordance with PCI-DSS. Specifically, but not exclusively:

- All access to credit card data is logged via NetSuite CRM, where access log and card numbers are retained indefinitely.
- Credit card PANs must never be sent via any unsecure communication method such as email, fax, IM, or voicemail.
- Credit card data must never be written, copied, or stored on paper.
- The only acceptable method for communicating full PANs is a completed DocuSign template or a direct phone call to a TT SI Solutions Consultant, who will accept and enter the PANs into the NetSuite CRM.

5.0 DATA SECURITY

5.1 GENERAL

- All system-level passwords (for example, root, admin, application administration accounts, etc.) must be changed every ninety (90) days.
- All TTI SI personnel-level passwords such as workstation and e-mail passwords must be changed every one hundred sixty (160) days.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- TTI SI uses two-factor authentication for email accounts, which is valid for thirty (30) days on the same computer. After thirty (30) days, the user must re-authenticate their account.
- All default vendor settings for wireless must be changed. This includes but is not limited to, Simple Network Management Protocol (SNMP) strings, passwords, and if possible, user names.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public,” “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

5.2 PASSWORD GUIDELINES

All user-level and system-level passwords must conform to the guidelines described below:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least eight (8) alphanumeric characters
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Avoid characteristics of weak passwords:
  - Words found in a dictionary (English or foreign)
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software
  - Any derivative of common company terms
  - Birthdays and other personal information such as addresses and phone numbers
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.3 PASSWORD PROTECTION STANDARDS

- Do not write down or store passwords on-line without encryption.
- Do not reveal a password in email, other electronic communication, questionnaire or security form.
- All usernames must be unique and the use of shared accounts is prohibited.
- Do not speak about a password in front of others.
- Change system-level password every ninety (90) days.
- Change personnel-level password every one hundred sixty (160) days.
- Do not hint at the format of a password (e.g., "my family name").
- If someone demands a password, refer them to this policy and direct them to the Information Technology department.
- Passwords are to be transmitted only after verification of end-user by either sight or confirming telephone number.
- Consultant or vendor accounts are required to be set to expire after a period of thirty (30) days or under to ensure that the accounts are still valid and needed.

6.0 NETWORK SECURITY

6.1 SERVER SECURITY

- Ensure that Windows / Linux & MacOS Server updates are applied on a regular basis.
- Check backup jobs to ensure that they complete successfully and that the backups are valid.
- For users logging in over Remote Desktop Connection, ensure that they are logging in on a non-default port and are logging off the server to free any used resources instead of simply closing their RDC windows.
- Remote Desktop Services will always prompt a client for passwords upon connection.
- Remote Desktop Services will be configured with the client connection encryption set to the required level.
- Control access to exported files, for the protection of critical systems, monitoring file integrity.
- Delete users and groups that are no longer in use.
- Remove services and software packages that are not required for the server.
- Limit the access to services when possible.
- Scan server for viruses, rootkits, backdoors and local exploits.
- Encrypt data when needed.
- The shutdown option will not be available from the logon dialog box.
- Local volumes will be formatted using NTFS or approved format.
- The required legal notice will be configured to display before console logon.
- Anonymous enumeration of shares will be restricted.
- The system will be configured with a password-protected screen saver.
- Autoplay will be disabled for all drives.
- Network shares that can be accessed anonymously will not be allowed.
- If the time service is configured, it will use an authorized time server.

6.2 FIREWALL SECURITY

Every firewall must have the following configuration standards prior to implementation:

- Intrusion Detection System.
- No local accounts and the built-in admin account(s) must be renamed and password changed.
- Any firewall rule change must be approved via TTI SI's Change Management Policy prior to implementation.
- The enabled or privileged password on the firewall must be kept in a secure encrypted form and must be changed on a regular basis.
- Disallow the following:
  - IP directed broadcasts
  - Incoming packets at the sourced with invalid addresses, such as RFC1918 address
  - Transmission Control Protocol (TCP) small services
  - User Data Protocol (UDP) small services
  - All source routing
  - All web services running on firewall
  - Any unsecure protocols not specifically allowed by the firewall protocol policy
- Idle timeout for a period of inactivity in a management console must be enabled to prevent unauthorized users from accessing the management console.
- Access rules are to be added as business needs arise after approval through rule review process.
- Firewall rule sets are subject to quarterly review.
- The firewall configuration must satisfy the minimum requirement of supporting 3DES (triple-DES).
- The Use of IPSEC VPN tunnel(s) is limited to approved users and must use the best security available.
- Implement Internet Security Association and Key Management Protocol (ISAKMP) policy parameters on all firewalls.
- Secure Shell (SSH) is the preferred management protocol. Telnet is forbidden for use as the management protocol for the firewall unless there is a secure tunnel protecting the entire communication path. HTTPS is allowed IF and ONLY if SSH is not an option, but satisfying Policy item #1 is REQUIRED for authentication.
- Remove unused rules from the firewall rule bases when services are decommissioned.
- Organize Firewall Rules for Performance.

6.3 WIRELESS SECURITY

Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default.
- Encryption must be used to secure wireless communications. Stronger algorithms are preferred to weaker ones (i.e., WPA2 and Radius). Encryption keys must be changed and redistributed quarterly.
- Administrative access to wireless access points must utilize strong passwords.
- Vendor default settings are to be changed prior to use.
- All logging features should be enabled on TTI SI's access points.
- Security profile is configured to protect not only access point from wireless attacks, but also SSID and clients associated to the SSID. An example of the type of attacks protected against through policy (IDS) configuration are:
  - AP Impersonation Attacks/Spoofing
  - De-Auth Broadcasts
  - AirJack
- Access to backend systems via mobile devices is restricted by access control lists and password security in order to limit access to data. (Password security in this instance is defined as having unique accounts per device that are not shared on backend system which restricts area of access.)
- Enabling and configuration of Wireless Intrusion Prevention System (WIPS) (when available) is required in order to protect not only the wireless access point (WAP) but the end-user as well.

Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent TTI SI's security controls or be easily accessible to.
- Wireless devices must be installed only by TTI SI's information technology department.
- Channels used by wireless devices should be evaluated to ensure that they do not interfere with company equipment.

Inactivity

- Personnel should disable their wireless capability when not using the wireless network.
- Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.

Audits

- The wireless network must be audited twice each year to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, and use of strong encryption.

6.4 TIME SYNCHRONIZATION

- TTI SI employs a central time server sync'd to time.nist.gov.
- All network devices, servers, and workstations must sync to the TTISI's central time server.
- Any devices not able to communicate with the central time server must sync independently to time.nist.gov and must not have any devices sync their time to said device.
- Access to time settings must be restricted to administrators.
- Systems logging must include changes to time settings whenever possible.
- Central time server must be reviewed periodically to verify functionality, accessibility, and time accuracy.

6.5 CENTRAL LOG MANAGEMENT

Central Log Servers

The logs contained on the servers are restricted to production servers, network devices, and any system deemed critical to the day-to-day business operations at TTI SI.

Restricted Access

Access to the central log server is restricted to senior level TTISI Information Technology department staff. Only authorized personnel are allowed to access the system via SSH or an encrypted form of remote access.

Log Delivery

TTI SI log delivery is via socket over secure network links. Depending on the system role, the proper server will be selected to ship logs for analysis.

Notification Mechanisms

Each system is configured to alert on predefined thresholds, including but not limited to system health, disk utilization, failed logins attempts.

Logging Configuration
Dependent on system role, each system is required to be configured to deliver the following logs for audit and retention purposes.

- Account Log-on Events - Success and Failure
- Account Management Events - Success and Failure
- Logon Events - Success and Failure
- Network Events - ALL
- Policy Change Events - Success and Failure
- Privilege Use Events - Failure
- System Events - Success and Failure
- Directory Service Access Events - Domain Controller restricted

Log Data Review
Log data are required to be reviewed on a weekly basis.

Log Backup
Log files are to be backed up (compressed to preserve disk space) on a 24 hour schedule.

Log Storage
Log files are to be stored for a period of ninety (90) days.

6.6 ANTI-VIRUS

All TTI SI systems must have standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into TTI SI's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

All systems are required to run the standard, supported anti-virus software ("Anti-Virus") that is installed and maintained by the Information Technology department.

Anti-Virus must be configured to perform the following actions upon detection of a potential threat:

- Delete as primary action
- Quarantine as secondary action

Anti-Virus is required to:

- Send log alerts including but not limited to malware infection, root kit infection, and outbreak threat
- Send notification alerts including but not limited to malware infection, root kit infection, and outbreak threat
- Use heuristic technology to provide an additional layer of zero-day threat protection;
- Run scheduled scans (full) on a weekly basis
- Update detection signatures on an hourly schedule, and if an hourly schedule is not possible or an option, anti-Virus must be configured to update detection signatures on a daily schedule.

Personnel must be instructed to:

- Never download files from unknown or suspicious sources
- Never open any file or macros attached to an e-mail from an unknown or suspicious source
- Exercise caution when connecting to untrusted networks as risk of virus infection is high
- Exercise caution before connecting any unknown portable storage devices (USB flash drive) to TTI SI-owned equipment.

6.7 CHANGE MANAGEMENT

Every change to TTI SI business technology resources, including but not limited to operating systems, hardware, network infrastructure, and applications, is subject to this policy and must follow these procedures.

A Change Management Committee (CMC), appointed by information technology department leadership, will review change requests to ensure that change reviews and communications are being satisfactorily performed.

The Change Management Committee (CMC) includes:

Team Member	Title	E-Mail
Brent Rowland	Chief Technology Officer	brent.rowland@ttiltd.com
Craig Casimir	Systems Administrator	craig@ttiltd.com
Amy Lane	Executive Assistant	amy@ttisi.com

Change Management procedures include:

- A Change Review Meeting is scheduled, and key information and technology services stakeholders are required to attend. The meeting occurs quarterly.
- A formal change request must be submitted for all changes, both scheduled and unscheduled.
- Change requests must contain all of the following:
  - Change plan
  - Backup plan
  - Backout plan
  - Test plan or validation plan
  - Progress notes and change outcome
- All scheduled change requests must be submitted so that the CMC has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal CMC approval before proceeding with the change.
- The CMC may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- When possible, changes must first be performed in a test environment and cannot be moved to production until validation of successful change in test is acknowledged by someone other than the person performing the change and the move is approved by IT senior management.
- When possible, the test environment must be segmented off from the production environment, with no communication permitted between the two segments.
- When moving changes into production, confidential data must not be moved from test to production.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
  - Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change
  - Indication of success or failure

6.8 USER PROVISIONING

- Each user with access to the TTI SI network or any TTI SI application must have a unique account login.
- All account creation and modification requests must follow these guidelines and procedures:
  - Accounts should only be requested for users with a business need for accessing the specific network and application in order to perform their job function.
  - Account rights will only be given in order for a user to perform their job function, following the principal of least privilege.
- Access for third parties will remain deactivated until requested to be activated by a member of IT leadership or infrastructure team.
- Once third party has completed work, the original requestor will notify the infrastructure team so the access can be revoked.
- As a secondary control, all third party accounts expire every 30 days and are reviewed for need on a monthly basis.
- The request and provisioning process is as follows for each account type. Any non-standard requests must be supplemented by written correspondence between the provisioning department, the user's manager, and the CIO.
  - NETWORK ACCOUNT
    - All network account creation and modification requests are initiated by either the IT department, or the department head responsible for the user for which the request is being made.
    - A member of TTI SI's infrastructure team will complete the request according to guidelines, including the password guidelines for creation, expiration, and communication.

6.9 REMOTE ACCESS

- Remote access is granted to TTI SI users only on an as-needed basis.
- VPN sessions are automatically disconnected after one hundred eighty (180) minutes of inactivity.
- RDP server sessions are automatically disconnected after sixty (60) minutes of inactivity, and the default port should be changed.

6.10 NETWORK SCANNING AND SECURITY ASSESSMENT

TTI SI performs the following network vulnerability and penetration testing activities:

- Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). In the event of a failed scan, remediation must take place and the scan re-run. Remediation must be completed within the quarter, and at least one successful scan must be performed each quarter.
- Run continuous wireless vulnerability assessments. All vulnerabilities must be immediately addressed.
- Through third-party, perform yearly external penetration testing. Any critical, high, or PCI-related exploited vulnerabilities are remediated within sixty (60) days.

6.11 RISK ASSESSMENT

On an annual basis or as needed basis, but no less frequent than annually, TTI SI's IT leadership and infrastructure teams perform a detailed, comprehensive IT security risk assessment. The risk assessment must include the following process phases and tasks:

Discover

- Review of most recent internal and external vulnerability scan results
- Review of most recent internal, external, and wireless pen test results
- Discuss new threats resulting from new vulnerabilities, hacking techniques, information security trends, security threats
- Discuss any upcoming relevant regulatory changes or End-of-Life (EOL) deadlines
- Discuss any other security bulletins or advisories that have been received

Assess

- Determine any weaknesses discovered from scans and pen tests that have not already been remediated
- Determine any exposures resulting from new threats

Plan

- Categorize threats based on risk and required timeline to address/remediate
- Establish remediation plan to for each threat
- Determine course of action for any changes needed for compliance reasons
- Establish communication plan to alert others as needed of potential risks and plans

Execute

- Carry out remediation plan
- Establish and implement compensating controls for those threats which cannot be fully addressed through remediation

Re-Assess

- Confirm all risks have been mitigated successfully
- Repeat process for all critical risks which have not been addressed

7.0 SERVICE PROVIDERS

The following is a list of TTI SI's current service providers:

- Cybersource - Credit card processing - authorization and settlement
- Zayo - Multiprotocol Label Switching (MPLS), Phone, and Internet services
- Cloud Hosting - Digital Ocean, Amazon S3, NQHost, Linode
- Datacenter - IO Datacenters, PhoenixNAP (eu)

For service providers that interact with credit card data or the credit card data environment, the following requirements are in place and must be adhered to:

- Selection process of new service providers must be structured and include documentation of TTI SI's requirements, evaluation criteria, and due diligence of the service provider.
- Written agreement or contract between TTI SI and each service provider.
- Service provider must agree in writing to provide their services in a PCI-compliant manner.
- Account and service review with service provider on at least an annual basis.
- Service review to make sure services are being provided in accordance with the agreement.
- Establish service provider is continuing to provide in a PCI-compliant manner.
- Maintain a current matrix of service providers and the PCI-DSS requirements they are responsible for or participate in managing or maintaining.

8.0 SECURITY & TRAINING

Data security is a key focus for TTI SI and a responsibility of all users with network and application accounts. Security and awareness is a key tool to ensure users are equipped to fulfill their responsibilities in this space. TTI SI requires the following review and training:

All Personnel

- All personnel with a network or application account or who interact in any way with credit cards will receive the following training/communication regarding information and credit card security practices, trends, and threats.
- Required review of this Information Security Policy upon hire or upon being granted an account.
- Annual compliance training with detailed review of information and credit card security practices, including acknowledgement of understanding and acceptance of the training and practices by personnel, either electronic or written.
- Periodic bulletins and memos regarding key reminders, current threats, and areas of observed weaknesses.

IT Leadership and Security Personnel

All personnel that work with IT security, as well as IT leadership must take the following measures to remain current with information security practices, trends, and threats:

- Subscribe to multiple security-focused or security-related newsletters.
- Have active membership in credible websites providing security bulletins.
- Attend at least one webinar, seminar, or conference annually with a strong security emphasis.
- Through above methods or via independent method, stay current with data security best practices.

9.0 ENFORCEMENT

TTI SI personnel found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

10.0 REVISION HISTORY

When revisions are made to this policy, it will be documented with a brief description below.

Revision History	Date	Author	Comments