# Information Security Plan & Disaster Recovery Plan

## Contents

**1.0 Purpose and Objectives** .......... 7
**2.0 Objective** .......... 7
2.1 The main policy objectives are: .......... 7
2.2 This policy aims to mitigate the following risks: .......... 7
**3.0 Scope** .......... 8
**4.0 Policy Details** .......... 8
4.1 TSCTI Information Security Management Program (Domain 1) .......... 8
4.1.1 Purpose .......... 8
4.1.2 Scope .......... 8
4.1.3 Strategy .......... 8
4.1.4 Compliance and Continuous Improvement .......... 8
4.1.5 Capital Planning .......... 9
4.1.6 Security Roles and Responsibilities .......... 9
4.1.7 Policy Management .......... 9
4.1.8 Policy Sanctions and Acceptable Use .......... 10
4.2 Endpoint Protection (Domain 2) .......... 10
4.2.1 Malware Protection .......... 10
4.2.2 Mobile Protection .......... 10
4.3 Portable Media Security (Domain 3) .......... 10
4.3.1 Use of Portable Media .......... 10
4.4 Mobile Device Security (Domain 4) .......... 10
4.4.1 Mobile Device Management .......... 10
4.4.2 Mobile Device Security .......... 10
4.4.3 Teleworking Policy .......... 11
4.5 Wireless Security (Domain 5) .......... 11
4.5.1 Wireless Security Standards .......... 11
4.6 Configuration Management (Domain 6) .......... 11
4.6.1 Compliance .......... 11
4.6.2 Change Management .......... 11
4.6.3 Secure Configuration Management .......... 12
4.7 Vulnerability Management (Domain 7) .......... 12
4.7.1 Asset Management .......... 12
4.7.2 Hardening .......... 13
4.7.3 Vulnerability Management .......... 13

4.7.4 Software Development Security ..... 13
4.8 Network Protection (Domain 8) ..... 13
4.8.1 Network Management ..... 13
4.8.2 Network Segmentation ..... 14
4.8.3 Firewall Management ..... 14
4.9 Transmission Protection (Domain 9) ..... 14
4.9.1 Data Protection ..... 14
4.9.2 Remote Access ..... 15
4.9.3 Encryption Management ..... 15
4.9.4 Electronic Signatures ..... 15
4.10 Password Management (Domain 10) ..... 15
4.10.1 Password Management ..... 15
4.10.2 User Password Responsibilities ..... 16
4.11 Access Control (Domain 11) ..... 16
4.11.1 Access Control Management ..... 16
4.11.2 User Verification ..... 17
4.11.3 Role Based Security ..... 17
4.11.4 Shared/Guest Accounts ..... 18
4.11.5 Privilege Account Management ..... 18
4.11.6 Network Access Security ..... 18
4.11.7 Remote Access ..... 19
4.11.8 Clear Desk/Clear Screen Policy ..... 19
4.12 Audit Logging & Monitoring (Domain 12) ..... 19
4.12.1 Audit Log Management ..... 19
4.12.2 Security Incident and Event Management ..... 19
4.12.3 Separation of Duties ..... 20
4.13 Education, Training and Awareness (Domain 13) ..... 20
4.13.1 Policy Awareness and Management ..... 20
4.13.2 Security Awareness Program ..... 20
4.14 Third Party Assurance (Domain 14) ..... 21
4.14.1 Third Party Management ..... 21
4.14.2 Third Party Software Development ..... 22
4.15 Incident Management (Domain 15) ..... 22
4.15.1 Security Incident Response ..... 22
4.15.2 Employee Incidents and Sanctions ..... 23

4.16 Business Continuity & Disaster Recovery (Domain 16) ........ 23
4.16.1 Business Continuity ........ 23
4.16.2 Disaster Recovery ........ 24
4.17 Risk Management (Domain 17) ........ 24
4.17.1 Risk Management Program ........ 24
4.17.2 Security Controls ........ 24
4.17.3 Vendor and Procurement ........ 25
4.17.4 Software Development Lifecycle ........ 25
4.18 Physical & Environmental Security (Domain 18) ........ 25
4.18.1 Physical Security ........ 25
4.18.2 Environmental Security ........ 26
4.18.3 Media Destruction ........ 26
4.19 Data Protection & Privacy (Domain 19) ........ 26
4.19.1 Data Protection ........ 26
4.19.2 Privacy Management ........ 27
4.19.3 Records Management ........ 27
4.20 Change Management ........ 27
4.20.1 Purpose ........ 27
4.20.2 Scope ........ 27
4.20.3 Policy Details ........ 27
4.20.3.1 Change Initiation ........ 27
4.20.3.2 Change Impact Analysis ........ 28
4.20.3.3 Change Review and Approval ........ 28
4.20.3.4 Planning & Scheduling ........ 28
4.20.3.5 Change Testing ........ 28
4.20.3.6 Change Deployment & Closure ........ 28
4.20.3.7 Backup and Roll back ........ 29
4.20.3.8 Change Documentation & Reporting ........ 29
4.20.3.9 Emergency Changes ........ 29
4.21 Antivirus Policy ........ 29
4.21.1 Purpose ........ 29
4.21.2 Scope ........ 29
4.21.3 Policy Details ........ 30
4.21.3.1 Selection of Antivirus ........ 30
4.21.3.2 Installation and Configuration ........ 30

4.21.3.3 Rules for Virus Prevention ........ 30

4.21.3.4 Antivirus Signature Update ........ 32

4.21.3.5 Antivirus Server Security ........ 32

4.21.3.6 Monitoring ........ 33

4.21.3.7 Tracking new threats and vulnerabilities ........ 33

4.21.3.8 External Users ........ 33

4.21.3.9 Backup and Redundancy ........ 33

4.21.3.10 Incident reporting ........ 33

4.21.3.11 Change Management ........ 33

4.21.3.12 Documentation ........ 34

4.22 Human Resource Security Policy ........ 34

4.22.1 Purpose of Policy ........ 34

4.22.2 Audience ........ 34

4.22.3 Exception ........ 34

4.22.4 Policy Details ........ 34

4.22.4.1 Roles and Responsibilities ........ 34

4.22.4.2 Personnel Screening ........ 34

4.22.4.3 Contractual Requirements ........ 35

4.22.4.4 Third Party Staff ........ 35

4.22.4.5 During Employment ........ 35

4.22.4.6 Job Change or Termination ........ 36

4.22.4.7 Disciplinary Action ........ 36

4.23 Teleworking Policy ........ 37

4.23.1 Purpose of Policy ........ 37

4.23.2 Objectives ........ 37

4.23.3 Scope of Policy ........ 37

4.23.4 Key Terms and Definition ........ 37

4.23.5 Policy Details ........ 38

4.23.5.1 Policy Statement ........ 38

4.24 Acceptable Use Policy ........ 39

4.24.1 Purpose ........ 39

4.24.2 Scope ........ 39

4.24.3 Responsibilities ........ 39

4.24.4 Policy Statement ........ 40

4.24.4.1 Use of TSCTI Information Systems & Processing Facilities ........ 40

4.24.4.2 Prohibition on the Use of Unauthorized Copies of Licensed Software & Hardware ................ 40
4.24.4.3 Restriction on the Use of Freeware, Shareware Applications and Games ................................ 40
4.24.4.4 Games are not permitted and must not be installed on systems. ............................................. 40
4.24.4.5 Prohibition on the Use of Pornographic Material ........................................................................ 40
4.24.4.6 Prohibition on the use of Destructive Programs .......................................................................... 40
4.24.4.7 Use of Removable Media........................................................................................................... 41
4.24.4.8 User Data Backups ...................................................................................................................... 41
4.24.4.9 Password Use............................................................................................................................... 41
4.24.4.10 Sensitive Data Encryption ........................................................................................................ 42
4.24.4.11 Clear Desk and Clear Screen Policy ......................................................................................... 42
4.24.4.12 Due Diligence ............................................................................................................................ 42
4.24.4.13 Right to Monitor System Use .................................................................................................. 42
4.24.5 Compliance Measurement ............................................................................................................ 43
4.24.6 Waiver Criteria................................................................................................................................ 43
5.0 Review Frequency .............................................................................................................................. 43

## 1.0 Purpose and Objectives

The purpose of Information Security Policies is to provide management direction and support for maintaining Information Security in the organization. The security policies contained in this document have been established to cover data and information stored in the software, hardware and transmitted over the communication networks owned and operated by TSCTI.

The need for such protection arises because information systems are potentially vulnerable to namely two main categories of unwanted events or threats. They are accidental threats (human error / equipment failure/ natural hazards) and deliberate or malicious threats (fraud / sabotage / vandalism / theft). There is also a threat of legal action if the information systems are misused, which TSCTI and its employees must be aware of.

## 2.0 Objective

The goal of this policy document is to provide guidance and direction for the protection of TSCTI' information, computer hardware, data and programs against any kind of accidental or deliberate damage or destruction. It is also TSCTI' intention to ensure that its information systems comply with relevant laws, regulations and standards.

The objective for developing and implementing Information Security Policies is to provide TSCTI' Management, direction and support for information security in accordance with business requirements and relevant laws and regulations.

### 2.1 <u>The main policy objectives are:</u>

- Segregation of duties for every employee shall be defined in order to prevent misuse of information or services. The duties shall be carefully considered while assigning responsibilities to the staff based on the nature of duties and the availability.
- Business requirements for confidentiality, integrity and availability of information and systems shall be met.
- Ensure that TSCTI' information and its intellectual properties are adequately protected against anticipated threats or hazards.
- Protect against unauthorized access to or use of customer information that might result in substantial harm or inconvenience to any customer or present a safety and soundness risk to TSCTI.
- Provide for the timely and comprehensive identification and assessment of vulnerabilities and risks that may threaten the security or integrity customer information.
- Comprehensive information security procedures shall exist to support the policy including various categories of information systems data, equipment, and processes.
- Ensure that TSCTI complies with all relevant regulations, common law, explicit agreements, international security standards or conventions that mandate the security and confidentiality of customer information.
- Ensure protection of the Information Technology infrastructure components that comprise the TSCTI' Information Systems.
- Protect against the use of TSCTI' assets in a manner contrary to the purpose for which they were intended, including the misallocation of valuable organizational resources, threats to TSCTI' reputation or a violation of the law.
- Business continuity management process shall be in place.
- Information security training shall be made available for all employees
- Incidents shall be reported and incident management process shall be in place.

### 2.2 <u>This policy aims to mitigate the following risks:</u>

- Compromise of Confidentiality, Integrity and Availability of information or information processing systems due to any type of vulnerabilities or threats that results in, damage of TSCTI' reputation, non-compliance to legal and regulatory laws (National and International) and affects customer services which are provided by TSCTI.

## 3.0 Scope

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.) of TSCTI and other entities or organizations that have access to and use TSCTI' information systems in order to perform their daily job-related responsibilities or meet their contractual obligations.
- Relevant TSCTI staff and third-party personnel responsible for administering and maintaining TSCTI' IT infrastructure

## 4.0 Policy Details

### 4.1 TSCTI Information Security Management Program (Domain 1)

### 4.1.1 Purpose

The TSCTI Information Security Management Program ("ISMP" hereafter) identifies, and controls risks to TSCTI' infrastructure, applications and data.

### 4.1.2 Scope

The scope of this Policy applies to all computing systems within TSCTI that are supported. This body of networks, systems, and applications are referred to as IT supported systems. The ISMP is the sum of the organizational structure, policies, planning, responsibilities, procedures, and systems that accomplish the security of the IT supported systems. The ISMP utilizes results of risk assessments and penetration tests conducted on business-critical applications and infrastructure components as the basis for mitigation efforts. The controls selected to address the identified risks drive the creation of the procedures and technical standards required by the ISMP.

### 4.1.3 Strategy

The TSCTI ISMP is based on an accepted industry framework that is reviewed and updated as needed. The TSCTI ISMP is based on the HITRUST CSF Framework.

The ISMP strategy will include the Information Security objectives, approach, scope, importance, goals and principles for the TSCTI Information Security Management Program.

The ISMP strategy shall be formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.

### 4.1.4 Compliance and Continuous Improvement

The ISMP will include methods and tools to monitor the effectiveness of the implementation of controls described in the previous section. TSCTI shall conduct independent reviews of the ISMP to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security.

The results of such independent ISMP reviews shall be recorded and reported to the management official/office initiating the review; and the results must be maintained for no less than three (3) years.

If the independent reviews identify that TSCTI' approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated within the ISMP Policy, Management will take corrective action which is actually the Act phase of the Plan-Do-Check-Act model of governance.

### 4.1.5 Capital Planning

Capital planning and investment requests will include the resources needed to implement the security program, employ a business case, and includes TSCTI executive management support in ensuring that the resources are available for expenditure as planned.

The information security capital planning and investment plan (budget) will include resources for an information security workforce improvement program that includes but not limited to hands-on training, certifications, seminars and/or conferences.

### 4.1.6 Security Roles and Responsibilities

A qualified senior-level information security official shall be appointed and is responsible for ensuring security processes are in place, communicated to all stakeholders, and addresses all requirements within the ISMP.

The CISO ensures the effectiveness of the ISMP through program oversight, establishes and communicates the ISMP priorities, reviews and updates the ISMP strategy, monitors compliance to the ISMP by the workforce, and evaluates and accepts security risks on behalf of TSCTI.

The CISO will charter an information security management committee that includes documented security contacts that are assigned from each major business unit.

User security roles and responsibilities shall be clearly defined and communicated to all employees throughout TSCTI.

TSCTI management will ensure users are briefed on their security role(s)/responsibilities and conform with the terms and conditions of employment prior to obtaining access to the TSCTI' information systems. Such terms will include guidelines regarding the security expectations of their roles; principals to motivate users to comply with security policies.

### 4.1.7 Policy Management

ISMP Security Policies (this document) must always present the TSCTI' policy direction and be in line with business objectives and demonstrate management's support for, and commitment to, Information Security across the supported TSCTI systems.

The leaders responsible for the execution of the functional topics addressed in this policy must annually review and approve those sections of this policy. These reviews must be documented.

The TSCTI Information Security program shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its human resources security protection program (e.g., through policy, standards, guidelines, and procedures).

TSCTI information security policies shall be regularly reviewed and updated to ensure they reflect leading practices (e.g., for systems and services development and acquisition), and all reviews/changes will be communicated throughout the organization.

### 4.1.8 Policy Sanctions and Acceptable Use

TSCTI will employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. Such sanctions process will notify defined personnel (e.g., supervisors) within a twenty-four (24) hour period. Further, the sanction process shall include specific procedures for license, registration, and certification denial or revocation and other disciplinary action.

TSCTI will ensure that individuals are capable of making complaints concerning the information security policies, procedures, or the organization's compliance with its policies and procedures. Such complaints will be documented and may include requests for changes, and records the user's disposition, if applicable.

## 4.2 Endpoint Protection (Domain 2)

### 4.2.1 Malware Protection

All servers and workstations shall run malware software configured for automatic updates such that latest versions of the malware software and malicious code definition tables are installed as promptly as possible. A schedule for complete, automated malware scans of servers and workstations shall be documented.

The anti-malware solution shall retain audit logs of scans and activity.

### 4.2.2 Mobile Protection

Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, ActiveX, PDF, postscript, Shockwave, and Flash).

Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

TSCTI shall implement and regularly update mobile code protection, including malware protection.

## 4.3 Portable Media Security (Domain 3)

### 4.3.1 Use of Portable Media

All portable media (including laptops) shall be registered prior to use and include security protections based on the data classification level. The data classification level, documents the reasonable restrictions on how such media may be used, labeled, and provides an appropriate level of physical and logical protection (including encryption) for media containing covered information until properly destroyed or sanitized.

Any portable media that contains covered information and is not encrypted, shall be inventoried and the status and location of unencrypted covered information will be maintained and monitored.

## 4.4 Mobile Device Security (Domain 4)

### 4.4.1 Mobile Device Management

TSCTI shall monitor for unauthorized connections of mobile devices (0403.01x1System.8). Specially configured mobile devices will be issued for personnel travelling to high-risk locations (e.g., security conferences, high risk countries, etc.) and shall be checked for malware and tampering upon return.

### 4.4.2 Mobile Device Security

Mobile computing devices shall be protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls or equivalent functionality, secure configurations, and physical protections.

If it is determined that encryption is not reasonable and appropriate, the rationale and acceptance of risk shall be documented and approved by management.

A documented list of approved application stores shall be defined as acceptable for mobile devices accessing or storing entity (client) or cloud service provider-managed client data, and the use of unapproved application stores will be prohibited for company-owned and BYOD mobile devices. Non-approved applications or approved applications not obtained through approved application stores will be prohibited.

TSCTI will prohibit the circumvention of built-in security controls on mobile devices such as jailbreaking or, rooting.

### 4.4.3 Teleworking Policy

Teleworking activities will only be authorized if security arrangements and controls comply with relevant TSCTI security policies.

Prior to authorizing teleworking, the physical security of the teleworking site will be evaluated and any threats/issues identified such as theft of equipment, unauthorized disclosure or unauthorized remote access shall be addressed.

## 4.5 Wireless Security (Domain 5)

### 4.5.1 Wireless Security Standards

Wireless LAN access points on the TSCTI network shall be protected from unauthorized access by using such measures as password protected access and encryption. Wireless networks shall use strong encryption with AES WPA2 as the minimum.

Vendor defaults for wireless access points shall be changed prior to authorizing the implementation of the access point. Wireless access points shall be placed in secure locations.

## 4.6 Configuration Management (Domain 6)

### 4.6.1 Compliance

Annual compliance reviews shall be conducted by security or audit individuals using manual or automated tools; if non-compliance is found, appropriate action will be taken. The results and recommendations of the reviews shall be documented and approved by management.

TSCTI shall perform annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools and will take appropriate action if non-compliance is found.

### 4.6.2 Change Management

All changes to a production system must follow a formal change management process that includes:

- Documented change requests.
- Stated change request approval cycle.
- Approval for the change by the owners of the systems or applications or network.
- Communication plan to the affected users.
- Applications and operating systems shall be successfully tested for usability, security and impact prior to production.
- Fallback procedures shall be defined and implemented, including procedures and responsibilities

for aborting and recovering from unsuccessful changes and unforeseen events.
- Documented outcome of change implementation.
- Changes to mobile device operating systems, patch levels, and/or applications go through the change management process.

Only authorized administrators will be allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.

Managers responsible for application systems will also be responsible for the strict control (security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

### 4.6.3 Secure Configuration Management

When purchasing new IT equipment (servers, laptops, mobile devices, network devices, etc.) the default configurations delivered with these devices are geared for ease-of-deployment and ease-of-use, not security. This is conducted as these settings can be exploitable in their default state, modifying their configuration settings with effective, standardized security properties shall be required before placing the equipment into production or connecting it to the network. TSCTI operating systems shall have in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of its baseline.

Additionally, Operational systems shall only hold approved programs or executable code.

The organization identifies and prevents the usage of unauthorized (blacklisted) software on the information system, including servers, workstations and laptops, employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system, and reviews and updates the list of unauthorized (blacklisted) software periodically but no less than annually.

Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier, and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application.

If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, TSCTI shall show evidence of a formal migration plan approved by management to replace the system or system components.

## 4.7 Vulnerability Management (Domain 7)

### 4.7.1 Asset Management

A reliable and comprehensive asset management system that identifies all assets associated with information and information system processing is to be implemented. The ability to identify and validate required security configurations that can be traced to specific hardware or software IT assets connected to or within the network is vital to protecting the enterprise and quantifying the security program’s overall effectiveness.

An inventory of assets and services shall be maintained.

The IT Asset Lifecycle Program will include details regarding the secure use, transfer, exchange, and disposal of IT-related assets.

The asset inventory shall not duplicate other inventories unnecessarily and ensures their respective content is aligned.

The asset inventory shall include an inventory of authorized wireless access points, including a documented business justification to support unauthorized WAP identification and response.

If TSCTI assigns assets to contractors, it must ensure that the procedures for assigning and monitoring the use of the property are included in the contract; and, if assigned to volunteer workers, there is a written agreement specifying how and when the property will be inventoried and how it will be returned upon completion of the volunteer assignment.

TSCTI shall create and document the process/procedure for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus.

### 4.7.2 Hardening

Hardening standards shall support all system and information integrity requirements to ensure that they will be developed, documented, disseminated, reviewed and updated annually.

### 4.7.3 Vulnerability Management

Critical network access points, internal systems that store sensitive data, and Internet facing systems shall be tested for vulnerabilities periodically.  Technical vulnerabilities identified shall be evaluated for risk and corrected in a timely manner.

Specifically, applications that store, process or transmit covered information shall undergo application vulnerability testing by a qualified party on an annual basis.

Exploitable vulnerabilities identified during penetration testing shall be corrected, and an adequate retest performed to demonstrate that the identified exploit is addressed.

### 4.7.4 Software Development Security

Applications developed by TSCTI shall be based on secure coding guidelines to prevent common vulnerabilities or will undergo appropriate vulnerability and penetration testing.

Procedures, guidelines, and standards for the development of applications shall be periodically reviewed, assessed and updated as necessary by the appointed senior-level information security official of the organization.

TSCTI checks the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.  For in-house developed software, TSCTI shall ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

## 4.8 Network Protection (Domain 8)

### 4.8.1 Network Management

TSCTI shall keep up to date and current diagrams which include all networks including wireless networks, system architecture, and data flow diagrams. Diagrams shall be updated whenever there are network changes and no less than every six months.

Agreed services provided by a network service provider/manager will be formally managed and monitored to ensure they are provided securely.

TSCTI shall monitor for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAPs) unless explicitly authorized in writing by the Director, Cybersecurity or the CISO.

TSCTI shall formally manage equipment on the network, including equipment in user areas.

### 4.8.2 Network Segmentation

TSCTI' network shall be logically and physically segmented with a defined security perimeter and a graduated set of controls, including: subnetworks for publicly accessible system components that will be logically separated from the internal network, based on organizational requirements; traffic is controlled based on functionality required; and classification of the data/systems based on a risk assessment and their respective security requirements.

The sensitivity of TSCTI applications/systems shall be explicitly identified and documented by the application/system owner.

TSCTI' security gateways (e.g., firewalls) shall enforce security policies and will be configured to filter traffic between domains, block unauthorized access, and will be used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs, and will enforce access control policies for each of the domains.

TSCTI shall ensure that the security of information in networks, availability of network services and information services using the network are protected from unauthorized access.

### 4.8.3 Firewall Management

Routing controls shall be implemented through security gateways (e.g., firewalls) used between internal and external networks such as the Internet and 3rd party networks.

The ability of users to connect to the internal network will be restricted using a deny-by-default and allow-by-exception policy at managed interfaces according to the Access Control Policy and the requirements of clinical and business applications.

For any public-facing web applications, application-level firewalls will be implemented to control traffic. For public-facing applications that are not web-based, a network-based firewall specific to the application type will be implemented. If the traffic to the public-facing application is encrypted, the device either sits behind the encryption or shall be capable of decrypting the traffic prior to analysis.

## 4.9 Transmission Protection (Domain 9)

### 4.9.1 Data Protection

Multiple safeguards shall be addressed before allowing the use of information systems for information exchange.

Communication protection requirements, including the security of exchanges of information, shall include policy development and compliance audits.

PII/PHI will not be sent over facsimile (FAX), unless it can be sent over securely.  If not, then other secure channels shall be used such as delivery by hand or secure email.

Data involved in electronic commerce and online transactions shall not contain covered information and security shall be maintained in all aspects of the transactions.

Approval of the CISO shall be obtained prior to using external public services, including instant messaging or file sharing.

### 4.9.2 Remote Access

Terms and conditions shall be established with any organization owning, operating, and/or maintaining external information systems, allowing authorized individuals to (i) access the information system from external information systems; and (ii) process, store or transmit organization-controlled information using external information systems.

Cryptography will be used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.

Strong cryptography protocols will be used to safeguard covered information during transmission over less trusted/open public networks. Stronger levels of authentication will be implemented to control access from publicly accessible networks.

### 4.9.3 Encryption Management

Stronger controls will be implemented to protect certain electronic messages.  Electronic messages shall be protected throughout the duration of its end-to-end transport path using cryptographic mechanisms unless protected by alternative measures.

Covered information shall be encrypted when stored in non-secure areas and in mobile/removable media and, if not encrypted at rest, the organization must document its rationale.

Unencrypted sensitive information shall never be sent through end-user messaging technologies such as email, instant messaging, and chat. Protocols used to communicate between all involved parties will be secured using cryptographic techniques such as SSL/TLS.

### 4.9.4 Electronic Signatures

Legal considerations, including requirements for electronic signatures, shall be addressed.

Identity verification of the individual shall be required prior to establishing, assigning, or certifying an individual's electronic signature or any element of such signature.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records. Signed electronic records shall contain information associated with the signing in human-readable format. Identification codes used in conjunction with passwords for electronic signatures shall be protected. Electronic signatures shall be unique to one individual, cannot be reused by, or reassigned to, anyone else.

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by any individual other than their genuine owners. Electronic signatures that are not based upon biometrics shall employ at least two distinct identification components that will be administered and executed.

## 4.10 Password Management (Domain 10)

### 4.10.1 Password Management

Passwords shall not be displayed when entered. Passwords will not be included in automated log-on processes. User identities will be verified prior to performing password resets. Temporary passwords will be unique and not guessable.

A password list shall be maintained that identifies commonly-used, expected or compromised passwords, and updates the list at least every 90 days and when organizational passwords are suspected to have been compromised, either directly or indirectly.  This list will verify when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected or compromised passwords. Password Management allows users to select long passwords and passphrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators.

All passwords shall be transmitted only when cryptographically-protected and will store passwords using an approved hash algorithm.

Passwords shall be encrypted during transmission and storage on all system components.

Password policies, applicable to mobile devices, will be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and prohibit the changing of password/PIN lengths and authentication requirements.

TSCTI shall avoid the use of third parties or unprotected (clear text) electronic mail messages for the dissemination of passwords.

TSCTI shall change passwords for default system accounts, whenever there is any indication of password compromise, at first logon following the issuance of a temporary password, and requires immediate selection of a new password upon account recovery.

### 4.10.2 User Password Responsibilities

Users shall acknowledge receipt of passwords and sign a statement acknowledging their responsibility to keep passwords confidential.

## 4.11 Access Control (Domain 11)

### 4.11.1 Access Control Management

User registration and de-registration, at a minimum, shall communicate relevant policies to users and require acknowledgement (e.g. signed or captured electronically), check authorization and minimum level of access necessary prior to granting access, ensure access is appropriate to the business and/or clinical needs (consistent with sensitivity/risk and does not violate segregation of duties requirements), address termination and transfer, ensure default accounts are removed and/or renamed, remove or block critical access rights of users who have changed roles or jobs, and automatically remove or disable inactive accounts.

Account managers will be notified when users' access rights change (e.g., termination, change in position) and modify the user's account accordingly.

Upon termination or changes in employment for employees, contractors, third-party users or other workforce arrangements, physical and logical access rights and associated materials such as passwords, keycards, keys, documentation that identify them as current members of the organization shall be removed or modified to restrict access within 24 hours. Further, old accounts shall be closed after 90 days of opening new accounts.

Access rights to information assets and facilities shall be reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors.

User registration and de-registration shall formally address establishing, activating, modifying, reviewing, disabling and removing accounts. User access rights will be reviewed after any changes and reallocated as necessary.

Acceptable use agreements shall be signed by all employees before being allowed access to information assets.

Users will be given a written statement of their access rights, which they will be required to sign stating they understand the conditions of access. Guest/anonymous, shared/group, emergency/ temporary accounts shall specifically be authorized and use will be monitored.

TSCTI shall review critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.

### 4.11.2 User Verification

User identities shall be verified prior to establishing accounts.

Help desk support extended by IT shall require user identification for any transaction that has information security implications.

Where tokens are provided for multi-factor authentication, in-person verification shall be required prior to granting access.

User identities will be verified in person in front of a designated registration authority with authorization by a designated organizational official (e.g., a supervisor or other individual defined in an applicable security plan) prior to receiving a hardware token.

### 4.11.3 Role Based Security

TSCTI shall maintain a current listing of all workforce members (individuals, contractors and Business Associates) with access to PHI.

Unique IDs that can be used to trace activities to the responsible individual will be required for all types of organizational and non-organizational users.

Actions that can be performed without identification and authentication will be permitted by exception.

Account types will be identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group.

Role-based access control will be implemented and is capable of mapping each user to one or more roles, and each role to one or more system functions

Privileges will be formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element.

Access rights from an application to other applications shall be controlled. Access rights to applications and application functions shall be limited to the minimum necessary using menus.

Outputs from application systems handling covered information shall be limited to the minimum necessary and sent only to authorized terminals/locations.

TSCTI shall facilitate information sharing by enabling authorized users to determine a business partner's access when discretion is allowed as defined by the organization and by employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.

The access control system for the system components storing, processing or transmitting covered information shall be set with a default "deny-all" setting.

### 4.11.4 Shared/Guest Accounts

Group, shared or generic accounts and passwords (e.g., for first-time log-on) will not be used.

Shared/group and generic user IDs shall only be used in exceptional circumstances where there is a clear business benefit, when user functions do not need to be traced, additional accountability controls are implemented, and after approval by management

Redundant user IDs will not be issued to other users and shall require that all users are uniquely identified and authenticated for both local and remote access to information systems

Non-organizational users (all information system users other than organizational users, such as patients, customers, contractors, or foreign nationals), or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization's information systems, shall be uniquely identified and authenticated

### 4.11.5 Privilege Account Management

Users who performed privileged functions (e.g., system administration) shall use separate accounts when performing those privileged functions .

Elevated privileges will be assigned to a different user ID from those used for normal business use, all users access privileged services in a single role, and such privileged access is minimized.

Replay-resistant authentication mechanisms shall be implemented such as one-time passwords, or time stamps to secure network access for privileged accounts; and, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline.

Restriction shall apply to all access to privileged functions and all security-relevant information.

Authorization to access specific security relevant functions (deployed in hardware, software, and firmware) and security-relevant information shall be addressed.

Use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users shall be implemented.

Default and unnecessary system accounts shall be removed, disabled, or otherwise secured such that the passwords are changed and privileges are reduced to the lowest levels of access.

### 4.11.6 Network Access Security

TSCTI shall protect wireless access to systems containing sensitive information by authenticating both users and devices.

Access to network equipment shall be physically protected.

If encryption is not used for dial-up connections, the Director, Cybersecurity provides specific written authorization.

When PKI-based authentication shall include validation of certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; enforces access to the corresponding private key; maps the identity to the corresponding account of the individual or group; and implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

### 4.11.7 Remote Access

Strong authentication methods such as multi-factor, Radius or Kerberos (for privileged access) shall be implemented for all external connections to the organizations network.

Multi-factor authentication methods shall be used in accordance with organizational policy, (e.g., for remote network access).

Remote access to business information across public networks will only take place after successful identification and authentication.

Copy (including print screen), move, print, and storage of sensitive data will be prohibited when accessed remotely without a defined business need.

### 4.11.8 Clear Desk/Clear Screen Policy

A time-out system (e.g., a screen saver) shall pause the session screen after 2 minutes of inactivity and closes network sessions after 30 minutes of inactivity. A time-out system (e.g., a screen saver) shall pause the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.

Covered or critical business information shall not be left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors.

Covered or critical information shall be protected when using internal or external mail services.

## 4.12 Audit Logging & Monitoring (Domain 12)

### 4.12.1 Audit Log Management

A secure audit record shall be created for all activities on the system (create, read, update, delete) involving covered information (1202.09aa1System.1). Audit records will include the unique user ID, unique data subject ID, function performed, and date/time the event was performed.

Audit logging shall be enabled in order to audit administrator activities; and reviews system administrator and operator logs on a regular basis.

Audit records will be retained for 90 days and older audit records are archived for one year. Information collected from multiple sources shall be aggregated for review.

Audit logging procedures shall specify how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

### 4.12.2 Security Incident and Event Management

TSCTI shall provide notice that the employee's actions may be monitored, and that the employee consents to such monitoring.

All applicable legal requirements related to monitoring authorized access and unauthorized access attempts will be met.

The activities of privileged users (administrators, operators, etc.) shall include the success/failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event.

The Cybersecurity Team & Director, Cybersecurity shall periodically test its monitoring and detection processes, remediate deficiencies, and improve its processes.

An intrusion detection system managed outside of the control of system and network administrators will be used to monitor system and network administration activities for compliance.

### 4.12.3 Separation of Duties

Separation of duties shall be used to limit the risk of unauthorized or unintentional modification of information and systems.

## 4.13 Education, Training and Awareness (Domain 13)

### 4.13.1 Policy Awareness and Management

Employees and contractors shall receive documented initial (as part of their onboarding within sixty (60) days of hire), annual and ongoing training on their roles related to security and privacy.

Employees and contractors shall be informed in writing, (e.g., when they sign rules of behavior or an acceptable use agreement) that violations of the security policies will result in sanctions or disciplinary action.

Rules shall be defined to describe user responsibilities and acceptable behavior for information system usage, including at minimum, rules for email, internet, mobile devices, social media and facility usage.

Employees, contractors and third-party system users will be made aware of the limits that exist for their use of the organization's information assets associated with the information processing facilities and resources; and they are responsible for their use of any of the information resources and any use carried out under their responsibility.

All users shall be prohibited from installing unauthorized software, including data and software from external networks. TSCTI will ensure users are made aware and trained on these requirements.

### 4.13.2 Security Awareness Program

The security awareness program shall identify how workforce members are provided security awareness and training; identify the workforce members (including managers, senior executives, and as appropriate, business associates/partners, and contractors) who will receive security awareness and training; describe the types of security awareness and training that is reasonable and appropriate for its workforce members; how workforce members are provided security and awareness training when there is a change in the organizations information systems; and how frequently security awareness and training is provided to all workforce members.

Training shall be provided on incident response. Contingency training shall be provided to information system users consistent with assigned roles and responsibilities within ninety (90) days of assuming an incident response role or responsibility; when required by information system changes; and within every three hundred sixty-five (365) days thereafter.

Personnel who telework shall be trained on the risks, the controls implemented, and their responsibilities.

Personnel using mobile computing devices shall be trained on the risks, the controls implemented, and their responsibilities, e.g., Shaller surfing, physical protections.

Personnel are appropriately trained on leading principles and practices for all types of information exchange (oral, paper and electronic).

## 4.14 Third Party Assurance (Domain 14)

### 4.14.1 Third Party Management

TSCTI shall address information security and other business considerations when acquiring systems or services; including maintaining security during transitions and continuity following a failure or disaster.

TSCTI shall maintain written agreements (contracts) that include: (i) an acknowledgement that the third-party (e.g., a service provider) is responsible for the security of the data and requirements to address the associated information security risks; and (ii) requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain.

A standard agreement with third-parties will be defined and includes the required security controls in accordance with the organization's security policies. Service Level Agreements (SLAs) or contracts with an agreed service arrangement shall address liability, service definitions, security controls, and other aspects of services management.

Such agreements ensure that there is no misunderstanding between the organization and the third-party and satisfies the organization as to the indemnity of the third party.

A list of current service providers shall be developed, disseminated and annually reviewed/updated, in which the list includes a description of services provided.

A service management relationship shall be established and a process between TSCTI and a third-party to monitor (i) security control compliance by external service providers on an ongoing basis; and (ii) network service feature and service levels to detect abnormalities and violations.

Service providers shall protect the TSCTI' data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.

Network services shall be periodically audited to ensure that providers implement the required security features and meet the requirements agreed upon with management, including new and existing regulations.

Regular progress meetings will be conducted as required by the SLA to review reports, audit trails, security events, operational issues, failures and disruptions, and identified problems/issues are investigated and resolved accordingly. The results of monitoring activities of third-party services shall be compared against the Service Level Agreements (SLA) or contracts at least annually.

A screening process shall be conducted for contractors and third-party users; and, where contractors are provided through an organization, (i) the contract with the organization clearly specifies the organization's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern and, in the same way; (ii) the agreement with the third party clearly specifies all responsibilities and notification procedures for screening.

Personnel security requirements shall be established, including security roles and responsibilities, for third-party providers that are coordinated and aligned with internal security roles and responsibilities.

The identification of risks related to external party access shall take into account a minimal set of specifically defined issues.

TSCTI ensures that customers shall be aware of their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets. They permit an individual to request restriction of the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or health care operations, and is not for purposes of carrying out treatment, and responds to any requests from an individual on the disclosure of the individual's covered information.

### 4.14.2 Third Party Software Development

Where software development is outsourced, formal contracts shall in place to address the ownership and security of the code and application.

TSCTI shall restrict the location of facilities that process, transmit or store covered information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual and other security and privacy-related obligations.

## 4.15 Incident Management (Domain 15)

### 4.15.1 Security Incident Response

A formal security incident response program shall be established to respond, report (without fear of repercussion), escalate and treat breaches and reported security events or incidents. Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that Shall be included in the incident notification. This reporting includes notifying internal and external stakeholders, the appropriate community Computer Emergency Response Team, and law enforcement agencies in accordance with all legal or regulatory requirements for involving that organization in computer incidents.

The security incident response program will prepare TSCTI for a variety of security incidents.

The program shall include an insider threat program that includes a cross-discipline insider threat incident handling team shall be implemented.

TSCTI adheres to the HITRUST requirements for responding to a data breach (of covered information) and reporting the breach to affected individuals, media, and federal agencies.

The program shall establish a point of contact for reporting information security events. This person will be made known throughout the organization, always available, and able to provide adequate and timely response. A list of third-party contact information (e.g., the email addresses of their information security offices), which can be used to report a security incident will be maintained.

The point of contact will be responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process.

TSCTI shall test and/or exercise its incident response capability regularly.

The information gained from the evaluation (tests) of information security incidents will be used to identify recurring or high-impact incidents and update the incident response and recovery strategy.

Workforce members will always cooperate with federal or state investigations or disciplinary proceedings.

### 4.15.2 Employee Incidents and Sanctions

Management shall approve the use of information assets and will take appropriate action when unauthorized activity occurs.

Sanctions shall be fairly applied to employees following violations of the information security policies once a breach is verified. TSCTI shall document personnel involved in incidents, steps taken, timeline associated with those steps, steps taken for notification, the rationale for discipline, and the final outcome for each incident.

A list of employees involved in such security incidents will be maintained with the resulting outcome from the investigation.

TSCTI will take disciplinary action against workforce members that fail to cooperate with federal and state investigations.

The sanctions program will ensure individuals are held accountable and responsible for actions initiated under their electronic signatures, to help deter record and signature falsification.

## 4.16 Business Continuity & Disaster Recovery (Domain 16)

### 4.16.1 Business Continuity

The business contingency program shall address required capacity, identify critical missions and business functions, define recovery objectives and priorities, and identify roles and responsibilities.

The business continuity program will be (i) based on identifying events (or sequence of events) that can cause interruptions to the organization's critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters acts of terrorism); (ii) followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period; (iii) based on the results of the risk assessment, a business continuity strategy is developed to identify the overall approach to business continuity; and (iv) once this strategy has been created, endorsement is provided by management, and a plan created and endorsed to implement this strategy.

The business continuity planning framework shall address a specific, minimal set of information security requirements.

The program shall include a minimum of one (1) business continuity plan and ensure each plan (i) has an owner; (ii) describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security; and (iii) specifies the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan.

Emergency procedures, manual "fallback" procedures, and resumption plans shall be the responsibility of the owner of the business resources or processes involved; and fallback arrangements for alternative technical services, such as information processing and communications facilities, are the responsibility of the service providers.

Copies of the business continuity plans will be distributed to key contingency personnel and shall be stored in a remote location.

When new requirements are identified through testing or system changes any existing emergency procedures (e.g., evacuation plans or fallback arrangements) shall be amended as appropriate.

### 4.16.2 Disaster Recovery

TSCTI will recover and restore business operations and establish an availability of information in the time-frame required by the business objectives and without a deterioration of the security measures.

A formal definition of the level of backup required for each system shall be defined and documented including how each system will be restored, the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory and business requirements.

When the backup service is delivered by the third-party, the Service Level Agreement (SLA) or contracts shall include the detailed protections to control confidentiality, integrity and availability of the backup information.

Backup copies of information and software will be made, and tests of the media and restoration procedures are regularly performed at appropriate intervals.

The backups shall be stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to the data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location.

Inventory records for the backup copies, including content and current location, will be maintained.

Workforce member roles and responsibilities in the data backup process will be identified and communicated to the workforce; in particular, Bring Your Own Device (BYOD) users are required to perform backups of organizational and/or client data on their devices.

## 4.17 Risk Management (Domain 17)

### 4.17.1 Risk Management Program

TSCTI shall perform risk assessments in a consistent way and at planned intervals, or when there are major changes to the organization's environment and reviews the risk assessment results annually. It will include evaluation of multiple factors that may impact security as well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems.

TSCTI will use a formal methodology with defined criteria for determining risk treatments and ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented.

Risk assessments will be re-evaluated at least annually, or when there are significant changes in the environment.

Any harmful effect that is known to the covered entity of a use or disclosure of PII/Confidential by the covered entity or its business associates, in violation of its policies and procedures shall be mitigated.

TSCTI will ensure that plans for security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency within the Risk Management Program.

### 4.17.2 Security Controls

TSCTI will implement an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.

TSCTI shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements and facilitate the implementation of system and information integrity requirements/controls.

Information system specifications for security control requirements shall state that security controls are to be incorporated in the information system, supplemented by manual controls as needed, and these considerations are also applied when evaluating software packages, developed or purchased.

Security requirements and controls shall reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security.

Where additional functionality is supplied and causes a security risk, the functionality shall be disabled or mitigated through application of additional controls.

### 4.17.3 Vendor and Procurement

A formal acquisition process shall be followed for purchased commercial products, and supplier contracts and will include the identified security requirements.

Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced, and the associated controls shall be reconsidered prior to purchasing the product.

### 4.17.4 Software Development Lifecycle

TSCTI will require developers of information systems, components, and developers or providers of services to identify (document) early in the system development life-cycle, the functions ports, protocols, and services intended for organizational use and requires the developer of the information system, system component, or information system service to provide specific control design and implementation information.

## 4.18 Physical & Environmental Security (Domain 18)

### 4.18.1 Physical Security

TSCTI shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e.g., through policy, standards, guidelines, and procedures).

Visitor and third-party support access shall be recorded and supervised unless previously approved.

Areas where sensitive information (e.g., covered information, payment card data) is stored or processed shall be controlled and restricted to authorized individuals only.

Maintenance and service shall be controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organizations maintenance program, taking into account whether this maintenance is performed by personnel on site or external to the organization.

TSCTI shall develop, approve and maintain a list of individuals with authorized access to the facility where the information system resides; issues authorization credentials for facility access; reviews the access list and authorization credentials periodically but no less than quarterly; and removes individuals from the facility access list when access is no longer required.

For facilities where the information system resides, TSCTI shall enforce physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that the organization determines necessary for areas officially designated as publicly accessible.

### 4.18.2 Environmental Security

TSCTI shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its equipment maintenance program (e.g., through policy, standards, guidelines, and procedures).

Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) shall be documented and retained in accordance with the organization's retention policy.

Fire extinguishers and detectors shall be installed according to applicable laws and regulations.

Fire authorities shall be automatically notified when a fire alarm is activated.

TSCTI shall obtain maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan.

TSCTI shall maintain a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

### 4.18.3 Media Destruction

Electronic and physical media containing covered information shall be securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal.

Surplus equipment shall be stored securely while not in use and disposed of or sanitized when no longer required.

The risk of information leakage to unauthorized persons during secure media disposal shall be minimized. If collection and disposal services offered by other organizations are used, care is taken in selecting a suitable contractor with adequate controls and experience.

Disposal methods shall commensurate with the sensitivity of the information contained on the media.

## 4.19 Data Protection & Privacy (Domain 19)

### 4.19.1 Data Protection

The confidentiality and integrity of covered information at rest shall be protected using an encryption method appropriate to the medium where it is stored; where TSCTI chooses not to encrypt covered information, a documented rationale for not doing so shall be maintained.

Covered information shall only be retained for as long as it is required; storage of such information shall be kept to a minimum and the information is controlled on where it can be stored.

Guidelines will be issued to all business units on the ownership, classification, retention, storage, handling and disposal of ALL records and information. Designated senior management within TSCTI will review and approve the security categorizations and associated guidelines.

Records with sensitive personal information shall be protected during transfer to organizations lawfully collecting such information.

The public shall have access to information about TSCTI' security and privacy activities and is able to communicate with its senior security official and senior privacy official.

### 4.19.2 Privacy Management

TSCTI shall formally appoint a data protection officer responsible for the privacy of covered information.

When required, consent shall be obtained before any protected information (e.g., about a patient) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.

TSCTI shall document compliance with the notice requirements by retaining copies of the notices issued by the covered entity for a period of at least six (6) years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement.

### 4.19.3 Records Management

TSCTI shall document restrictions in writing and formally maintains such writing, or an electronic copy of such writing as an organizational record for a period of at least six (6) years.

TSCTI shall document through policies & procedures and maintain the designated record sets that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of at least six (6) years.

Important records, such as contracts, personnel records, financial information, patient records, etc., of the organization shall be protected from loss, destruction and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, locked facilities or containers, etc.

TSCTI ensures that PHI will be safeguarded for a certain period and then securely deleted.

## 4.20 Change Management

### 4.20.1 Purpose

A change is defined as any alteration to software, hardware, or other aspect of the data processing environment and its attached networks. Unauthorized changes and unstructured implementation of information assets can lead to system downtime and cause denial of service to users who need access to the system. The purpose of this policy is to ensure that all the changes made to any of TSCTI' systems are properly prioritized and scheduled, authorized and tested before implementation

### 4.20.2 Scope

This policy applies to:

- All changes, upgrades or modifications made to the IT environment. This covers any change to the hardware, software, application, database and network system
- All TSCTI employees whether directly or indirectly, who require access to and responsible for introducing any changes in the system

### 4.20.3 Policy Details

#### 4.20.3.1 Change Initiation

- TSCTI shall permit only qualified and authorized individuals for initiating changes, including upgrades and modifications as those changes can potentially have significant effects on the overall security of the systems and those people are responsible for the changes.

- All proposed changes to existing IT infrastructure Shall be initiated using Change Management System or a formal Change management form (CMF) if Change Management System is not functional.
- TSCTI shall maintain record of the changes perform in the absence of Change Management System.

### 4.20.3.2 Change Impact Analysis

- TSCTI shall perform assessment of the potential impacts, including information security impacts, of changes before approving it.
- CISO shall ensure process that existing security and control procedures are not compromised by new changes.
- Change feasibility analysis Shall be conducted considering need for change; impact and coverage for change; current risks and security implications.
- All proposed changes Shall be assigned priority based on the Urgency, Coverage and Impact of the change. The priority Shall determine if the change needs to be done immediately or can be implemented at a later time.

### 4.20.3.3 Change Review and Approval

- TSCTI shall have formal approval process for changes to be approved and every initialized change Shall follow the formal approval process before implementation.
- CISO shall ensure that the information security requirements have been met by the change before approving it.

### 4.20.3.4 Planning & Scheduling

- All approved changes shall be scheduled for implementation based upon their priorities in the Schedule of changes.
- TSCTI shall take the system offline or replicated to the extent feasible, before testing can be conducted and accordingly service disruption notes shall be sent to all the concerned stakeholders if required.
- The change implementation Shall not disturb the ongoing work of other employees of TSCTI.

### 4.20.3.5 Change Testing

- All proposed changes shall be tested on a test environment before implementing changes in the operational environment.
- Testing procedure shall have verification that information security requirements have been met after the implementation of changes.

### 4.20.3.6 Change Deployment & Closure

- The changes shall be deployed into the production environment only after the approval from the Director, Cybersecurity.
- The Senior Manager – Site Reliability Engineer shall perform the post implementation review after the change has been released into the live environment.
- The Director, Cybersecurity shall close the change request by selecting any of the below closure code based on the post implementation review:
- Successful

- Successful with errors
- Failed
- The Director, Cybersecurity shall initiate any improvement activities based on the assessment made during the post implementation review.

#### 4.20.3.7 Backup and Roll back

- TSCTI shall implement adequate back up plans in the critical production systems ensure successful recovery of data in case of any failure during change implementation.
- All changes to the critical production systems shall be supported with detailed roll back plan to ensure successful system roll back in case of a failure.
- TSCTI shall define procedure for aborting and recovering from unsuccessful changes (roll backing) and unforeseen events.

#### 4.20.3.8 Change Documentation & Reporting

- Director, Cybersecurity shall ensure that an audit log containing all relevant information is retained after changes are made to ensure the integrity of system, applications and products.
- Each activity performed through the change management process shall be updated in the change ticket as a record and/or task for audit trail.
- Performance of the change management process Shall be measured as per the performance measurement procedure on a monthly basis and reports generated on the identified Key Risk Indicator (KRI).

#### 4.20.3.9 Emergency Changes

- TSCTI shall develop a process to enable quick and controlled implementation of changes to resolve an incident.
- The emergency changes shall be allowed only to resolve major production problems and it Shall be under the approval of Director, Cybersecurity.
- The post change implementation review for emergency changes Shall be same as that of the normal approved changes.

## 4.21 Antivirus Policy

### 4.21.1 Purpose

Malicious codes such as viruses, worms, Trojans, spy ware, root-kits etc. represents a significant threat to the performance and security of TSCTI. This policy aims to provide guidelines to protect TSCTI assets against malicious code through an enterprise level Antivirus solution suite.

### 4.21.2 Scope

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees (contractors, suppliers, vendors etc.) of TSCTI and other individuals, entities or organizations that have access to information systems of TSCTI in order to perform their daily job-related responsibilities or meet their contractual obligations.
- Relevant TSCTI or third-party personnel responsible for administering and maintaining TSCTI' Antivirus infrastructure.

### 4.21.3 Policy Details

#### 4.21.3.1 Selection of Antivirus

- Currently, TSCTI uses Crowdstrike Anti-Virus for end points (like PCs, Laptops, etc.). User is strictly prohibited from installing/configuring any other Anti-Virus on his/her official PC/laptop.
- All computers attached to the TSCTI network must have anti-virus installed and configured by TSCTI Infrastructure department only.
- Any activities with the intention to create and/or distribute malicious programs onto the TSCTI network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
- If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT Team immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
- No employee Shall attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT Team.
- Any virus-infected computer will be removed from the network until it is verified as virus-free.
- If for any reason, TSCTI Management and CISO has allowed any TSCTI staff or consultant to use his/her personal laptop/PC, still he/she must have any other standard Anti-Virus installed with updated virus definitions. ALL other clauses of this policy are still applicable in such exceptional case.

#### 4.21.3.2 Installation and Configuration

- TSCTI shall define and enforce strict policy on installation of software and its configurations.
- All servers, desktops, Laptops and mobile devices used for processing information of TSCTI shall have anti-virus agent installed in it.
- IT Support/ helpdesk and IT Team Shall ensure that all new systems including desktops, laptops, mobile devices and servers have anti-virus agent installed and configured as soon as they are connected to the network.
- All applications that support file upload and transfer Shall have respective antivirus systems installed.
- Antivirus shall be configured in such a way that it Shall not allow access to unauthorized software.

#### 4.21.3.3 Rules for Virus Prevention

- Always run the standard anti-virus software provided by TSCTI IT Team.
- Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
- Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
- Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
- Files with the following filename extensions must NOT be sent/received via e-mail or copied across network: (as such files could be potential viruses). If there is any business need for sending/receiving business-critical files with these prohibited extensions, you are kindly requested to contact TSCTI IT Team.

| Extension | File Type | Extension | File Type |
|---|---|---|---|

| | | | |
|---|---|---|---|
| .ade | Access Project Extension (Microsoft) | .mda | Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft) |
| .adp | Access Project (Microsoft) | .mdb | Access Application (Microsoft), MDB Access Database (Microsoft) |
| .app | Executable Application | .mde | Access MDE Database File (Microsoft) |
| .asp | Active Server Page | .mdt | Access Add-in Data (Microsoft) |
| .bas | BASIC Source Code | .mdw | Access Workgroup Information (Microsoft) |
| .bat | Batch Processing | .mdz | Access Wizard Template (Microsoft) |
| | | | |
| .cer | Internet Security Certificate File | .msc | Microsoft Management Console Snap-in Control File (Microsoft) |
| .chm | Compiled HTML Help | .msh | Microsoft Shell |
| .cmd | DOS CP/M Command File, Command File for Windows NT | .msh1 | Microsoft Shell |
| .com | Command | .msh2 | Microsoft Shell |
| .cpl | Windows Control Panel Extension (Microsoft) | .mshxml | Microsoft Shell |
| .crt | Certificate File | .msh1xml | Microsoft Shell |
| .csh | csh Script | .msh2xml | Microsoft Shell |
| .der | DER Encoded X509 Certificate File | .msi | Windows Installer File (Microsoft) |
| .exe | Executable File | .msp | Windows Installer Update |
| .fxp | FoxPro Compiled Source (Microsoft) | .mst | Windows SDK Setup Transform Script |
| .gadget | Windows Vista gadget | .ops | Office Profile Settings File |
| .hlp | Windows Help File | .pcd | Visual Test (Microsoft) |
| .hta | Hypertext Application | .pif | Windows Program Information File (Microsoft) |
| .inf | Information or Setup File | .plg | Developer Studio Build Log |
| .ins | IIS Internet Communications Settings (Microsoft) | .prf | Windows System File |
| .isp | IIS Internet Service Provider Settings (Microsoft) | .prg | Program File |
| .its | Internet Document Set, Internet Translation | .pst | MS Exchange Address Book File, Outlook Personal Folder File (Microsoft) |
| .js | JavaScript Source Code | .reg | Registration Information/Key for W95/98, Registry Data File |
| .jse | JScript Encoded Script File | .scf | Windows Explorer Command |
| .ksh | UNIX Shell Script | .scr | Windows Screen Saver |
| .lnk | Windows Shortcut File | .sct | Windows Script Component, Foxpro Screen (Microsoft) |
| .mad | Access Module Shortcut (Microsoft) | .shb | Windows Shortcut into a Document |
| .maf | Access (Microsoft) | .shs | Shell Scrap Object File |
| .mag | Access Diagram Shortcut (Microsoft) | .ps1 | Windows PowerShell |
| .mam | Access Macro Shortcut (Microsoft) | .ps1xml | Windows PowerShell |

| | | | |
|---|---|---|---|
| .maq | Access Query Shortcut (Microsoft) | .ps2 | Windows PowerShell |
| .mar | Access Report Shortcut (Microsoft) | .ps2xml | Windows PowerShell |
| .mas | Access Stored Procedures (Microsoft) | .psc1 | Windows PowerShell |
| .mat | Access Table Shortcut (Microsoft) | .psc2 | Windows PowerShell |
| .mau | Media Attachment Unit | .tmp | Temporary File/Folder |
| .mav | Access View Shortcut (Microsoft) | .url | Internet Location |
| .maw | Access Data Access Page (Microsoft) | .vb | VBScript File or Any Visual Basic Source |
| .mda | Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft) | .vbe | VBScript Encoded Script File |
| .mdb | Access Application (Microsoft), MDB Access Database (Microsoft) | .vbs | VBScript Script File, Visual Basic for Applications Script |
| .mde | Access MDE Database File (Microsoft) | .vsmacros | Visual Studio .NET Binary-based Macro Project (Microsoft) |
| .mdt | Access Add-in Data (Microsoft) | .vsw | Visio Workspace File (Microsoft) |
| .wsf | Windows Script File | .ws | Windows Script File |
| .wsh | Windows Script Host Settings File | .wsc | Windows Script Component |
| .xnk | Exchange Public Folder Shortcut | | |

- Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- Avoid direct disk sharing with read/write access. Always scan removable media (e.g.; a floppy diskette, USB) for viruses before using it.
- If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
- Sometimes false notification e-mails/ads (hoax) get circulated over the internet/e-mail creating unnecessary commotion/distrust. You must NOT forward such e-mails at random to all and sundry BUT send it to Cybersecurity team for further action. If you strongly feel that the matter is more urgent you may contact any TSCTI Cybersecurity staff on Phone or Mobile (All numbers available in SharePoint directory)
- TSCTI employees must connect their laptops to TSCTI network at least twice in a month to have the latest virus definitions updated on them.

#### 4.21.3.4 **Antivirus Signature Update**

- Antivirus signature update shall be taken by the approval of antivirus administrator / System Admin of the IT Team.
- Antivirus administrator / System Admin shall ensure that new Antivirus signatures are applied as soon as they are released by the Antivirus Solution Vendor.
- TSCTI shall also establish a process like firewalls at network borders, increase monitoring to detect actual attacks, turning off the services, etc. until new signature update.

#### 4.21.3.5 **Antivirus Server Security**

- Antivirus servers and application shall be configured as per the latest secure configuration document.

- Antivirus servers shall be protected from unauthorized logical and physical access.
- Antivirus server shall be monitored for critical system parameters and resource utilization.
- Logging shall be enabled for the operating system as well as for the anti-virus application on the antivirus servers.
- Antivirus application, server, configuration and log files backup shall be taken on a case-to-case basis.

-

#### 4.21.3.6 Monitoring

- IT Team of TSCTI with the help of the vendor shall develop guidelines for performance monitoring and acceptable performance threshold levels of the antivirus servers.
- The log reports shall be sent to the Cybersecurity Team. These logs shall be available for at least once 3 months and shall be analyzed to identify abnormal events in the system.

#### 4.21.3.7 Tracking new threats and vulnerabilities

- Cybersecurity Team shall keep track of new threats arising from malicious code with respect to TSCTI' environment.
- When a new vulnerability is published, IT & Cybersecurity Team shall identify the steps that need to be taken to ensure that the associated risks are mitigated.

#### 4.21.3.8 External Users

- External users (including vendors, customers and service providers) who bring laptops/desktops/servers into TSCTI' premises shall not be allowed to connect to the TSCTI' Ethernet LAN network without prior approval from the Director, Cybersecurity and CISO.
- IT Team shall verify whether the device has antivirus installed and updated with latest signature pattern and that there are no active viruses. It shall also be checked whether all the necessary security patches have been installed. The device shall be allowed to connect only if all of the above conditions are met.

#### 4.21.3.9 Backup and Redundancy

- Backup of the Antivirus systems shall be carried out as required by the Data Backup and Recovery Policy.

#### 4.21.3.10 Incident reporting

- Users shall report to IT team in the event of a virus not being cleaned by the antivirus agent. Antivirus administrator shall initiate Incident management process once the incident is notified by the user.

#### 4.21.3.11 Change Management

- All changes needed in antivirus infrastructure shall follow the change management procedures.

#### 4.21.3.12 Documentation

- Documents for the following shall be maintained and updated by IT Team:
- Antivirus Report
- Antivirus agent installation procedure
- Troubleshooting FAQs/Manuals for administrators

## 4.22 Human Resource Security Policy

### 4.22.1 Purpose of Policy

- All users with access to information systems of TSCTI shall be aware of their responsibilities in protecting information systems of TSCTI. Failure to adhere to information security responsibilities shall entail appropriate disciplinary action. Access to information systems shall be provided based on job responsibilities, and revoked or modified with changes in such responsibilities.
- Personnel security must be implemented to address the risks of human error, theft, fraud or misuse of facilities and assist all personnel in creating a secure computing environment.
- The goal of this policy is to ensure that employees comply with security policies that are designed to protect TSCTI and to make employees aware of company policies, procedures and their roles and responsibilities towards it.

### 4.22.2 Audience

All Staff including permanent employees, authorized third party staff members, IT Assets used towards achieving policy objectives and processes involved.

### 4.22.3 Exception

All exceptions to this policy shall be explicitly approved by the Information Security Steering Committee (ISSC). The exception shall be valid for a specific time period and shall be reassessed and re-approved when necessary

### 4.22.4 Policy Details

#### 4.22.4.1 Roles and Responsibilities

- Roles and responsibilities of each employee shall be defined and documented. The HR Manager shall ensure that all the employees are aware of their roles and responsibilities.
- The HR Manager in consultation with the CISO shall identify security responsibilities for employee group as per access control classification and explicitly specify the responsibility in the employee job description and responsibility statement. This will include any general responsibilities for implementing or maintaining security policy, legal responsibilities and rights as well as any specific responsibilities for the protection of particular assets (such as employer's data) or for the execution of particular security processes or activities, internal or external to TSCTI.

#### 4.22.4.2 Personnel Screening

- Human Resource team of TSCTI shall define and follow the procedures for employment, screening and verification. The procedure shall include who is eligible to screen people and how, when and why verification reviews are carried out.
- The Human Resource team / Personnel in charge of recruitment shall ensure that relevant checks are conducted during recruitment of new staff to verify information submitted by them. Screening

process must include the following primary checks:

I. Verification of personal data (including date of birth, address and contact details)
II. Verification of relevant educational and professional qualifications
III. Verification of previous employment data
IV. An assessment of reliability, by seeking professional references from previous employers
V. An assessment of personality, by seeking personal references from known sources
VI. An assessment of background, by seeking criminal or political records or activities verifications through designated sources
VII. OIG exclusion check

- When an individual is hired for a specific information security role, the Human Resource team / Personnel in charge of recruitment shall make sure that the candidate:
  I. Has the necessary competence to perform the security role.
  II. Can be trusted to take on the role, especially if the role is critical to the organization.

### 4.22.4.3 <u>Contractual Requirements</u>

- TSCTI shall develop the contractual obligations for employees or contractors which shall reflect the organization’s policies for information security.
- All employees and contractors who are given access to confidential information of TSCTI shall sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.
- The contractual obligation shall include legal responsibilities and rights of employees or contractors, responsibilities for the classification of information and management of assets associated with information, information processing facilities and information services handled by the employee or contractor, responsibilities for the handling of information received from other companies or external parties, etc.
- It shall also include actions to be taken if the employee or contractor disregards TSCTI’s security requirements.

### 4.22.4.4 <u>Third Party Staff</u>

- Respective department heads who engage third parties and their staff to work for TSCTI shall ensure that relevant aspects of TSCTI’ Information Security are identified and applied to the work.
- Respective department heads who engage third parties and their staff shall ensure that relevant policies are made available and may involve TSCTI’ Cybersecurity Team in explaining the meaning of Policy to the third parties.
- Respective department heads who engage third parties and their staff shall ensure that suitable background checks are conducted where third-party staffs are to be engaged in critical duties. Background checks applied to third-party staff engaged in TSCTI’ duties must be of the same type and scope as applied to TSCTI’ staff.
- The contractors/personnel involved in any engagement that provides access to TSCTI’ confidential information shall be bounded by a Non-Disclosure Agreement or similar master agreements.

### 4.22.4.5 <u>During Employment</u>

- Human Resource team with TSCTI Department Heads shall ensure that employees and contractors:
  I. are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems
  II. are provided with guidelines to state information security expectations of their role within TSCTI
  III. achieve a level of awareness on information security relevant to their roles and

responsibilities within an organization

IV. conform to the terms and conditions of employment, which includes the organization’s information security policy and appropriate methods of working

V. continue to have the appropriate skills and qualifications and are educated on a regular basis

- Human Resource Team with direct manager of the employee shall ensure that staff records are maintained up to date, accurate and complete.
- Human Resource Team with direct manager of the employee shall ensure that staff immediately report any change related to their personal data to them (e.g., marital status, professional certifications, address, contacts etc.).
- HR Manager with direct manager of the employee shall ensure that day to day conduct of staff in TSCTI premises is in pursuance with their respective code of conduct as per Acceptable Usage Policy and the laws & regulations of the region.

#### 4.22.4.6 Job Change or Termination

- The HR Manager in consultation with CISO shall include the appropriate security clauses and procedures in Job Change/Job termination procedures for employees of TSCTI department and ensure that appropriate and timely actions are taken so that internal controls and security are not impaired by such occurrences.
- The procedures shall include but not be limited to:

  VI. Recovery of TSCTI’ documents, e-mail data, issued keys, tokens, records, reports, books, manuals, borrowed IT equipment (e.g., Desktop, Laptop, data media) and TSCTI identity badges. (All organizational assets in possession)

  VII. Revoking or deleting all entry and access rights held by the departing staff. This includes external access authorizations over data communications equipment. If, in exceptional case, several persons shared access right to an IT system (e.g., by using a common password), the access rights must be altered upon termination of employment by one of those individuals

  VIII. It shall be explained explicitly to the departing person that all confidentiality agreements remain in force and that no information obtained in the course of their work may be disclosed

- Third party organization supplying staff to TSCTI Department shall notify the owner of the contract about their staff terminations.
- Change in employment due to a job promotion or transfer shall follow similar process for return of assets as necessary.

#### 4.22.4.7 Disciplinary Action

- ISSC (Information Security Steering Committee) shall not take action against employee without evidences or prior verification that an Information Security breach has occurred.
- Human Resource team in coordination with CISO shall ensure that non-compliance with the information security policies, procedures and standards are investigated and disciplinary measures are enforced.
- TSCTI shall adhere to a disciplinary process in place, to take action against employees who have committed an information security breach.
- The disciplinary process shall provide for a graduated response by taking into account following factors:

  I. Nature and gravity of the breach

  II. Its impact on business

  III. Whether it’s a first or repeated offence

  IV. Whether the violator was properly made aware and trained

V. Relevant legislation

- All staff who has been convicted of a felony must be immediately terminated and applicable legal proceedings shall be initiated under a competent court of law. Disciplinary measures may range from reproach to dismissal, suspension, prosecution.

## 4.23 Teleworking Policy

### 4.23.1 Purpose of Policy

Purpose of this policy is to set high-level principles and expectations that apply to Teleworking.

The goals of this policy are:

- To provide users secure ways to perform operational activities in conditions when not able to access TSCTI Office
- Ensure that the users teleworking and accessing the TSCTI assets and services are aware of the limitations of the use of the services for business purpose within the defined level of security

This policy aims to mitigate the following risks:

- Misuse of organizational or unintentional disclosure of information
- Information loss
- Damage to reputation of TSCTI.

### 4.23.2 Objectives

The objective of this policy is to set out the minimum ethical conduct requirement for TSCTI' employees and addresses their intent to safeguard computing resources from threats.

### 4.23.3 Scope of Policy

Audience: All TSCTI Staff including permanent employees, and all external and all authorized third-party staff members and parties who have remote-enabled business relationships with TSCTI, such as investors, directors, supply chain, consultants, vendors, service providers, etc.

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.) of TSCTI Department and other individuals, entities or contractors who have access to and use TSCTI' information systems in order to perform their daily job-related responsibilities or to meet their contractual obligations.
- All laptops, communication and network devices, smart devices feasible and compatible for operational work.

All exceptions to this policy shall be explicitly approved by the ISSC (Information Security Steering Committee). The exception shall be valid for a specific time period and shall be reassessed and re-approved when necessary.

### 4.23.4 Key Terms and Definition

**Teleworking:** It refers to all forms of work outside of the office, including non-traditional work environments, also referred to as "telecommuting", "flexible workspace", "remote work", "virtual work" environments. Telework can refer to routine, as well as specialized or ad hoc business tasks performed outside of the office by any means of remote access.

### 4.23.5 Policy Details

#### 4.23.5.1 Policy Statement

- Teleworking is a privilege, and has mutual benefits for the Teleworker and for TSCTI. Eligibility will be determined by the suitability of the job to be conducted remotely.
- TSCTI employee teleworking may use the services, listed below, of TSCTI for operational activities;
  I. Email Services
  II. Shared File
  III. HR Self services
  IV. Remote desktop (on a need basis and approval from Cybersecurity Team)
  V. Corporate Directory
  VI. ITSM
- Teleworking employee shall ensure that physical security of the building and local environment of the teleworking site are at an acceptable level.
- TSCTI shall take serious care of communication link when highly sensitive data is accessed remotely.
- Teleworking employee shall avoid use of privately owned devices for processing and storage of information from remote site.
- Teleworking employee shall be responsible to ensure that unauthorized users (friends, family) are not allowed access to TSCTI internal networks.
- TSCTI shall define the acceptable ways to perform telework on home networks and may put restrictions on the configuration of wireless network services;
  I. E.g., the teleworking network access point shall have secured configurations like strong password, file sharing on local network shall be disabled, PC discovery within the local network shall be disabled
  II. Teleworking user shall not use public open networks for official work such as free Wi-Fi at Malls, cafés, hotels, etc.
- TSCTI shall define the work permitted, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access before giving rights to work from teleworking sites.
- The teleworking employees shall follow "Data Backup and Recovery" policy of IT security Policies for backup.
- The teleworking employees shall communicate as soon as is practical with Network, Security and Infrastructure and IT Support /helpdesk in case of any security incidents or problems, even if the employee is on holiday or otherwise off work.
- TSCTI shall establish monitoring system to monitor employee's activity working from teleworking site for security purpose.
- TSCTI shall revoke authority and access rights, and the return of equipment when the teleworking activities are terminated.
- Teleworkers will agree to an audit in the event that they are terminated for any reason, which includes review of data usage and storage, and may require examination of some personal equipment if it was used in any way for company purposes. They will be billed for equipment not promptly returned and services not promptly settled.
- Prior to authorizing teleworking, TSCTI shall provide a definition of the work permitted, standard operating hours, classification of information that may be held / stored, and the internal systems and services that the teleworker is authorized to access, suitable equipment and storage furniture for the teleworking activities, suitable communications equipment including methods for securing remote access, rules and guidance on family and visitor access to equipment and information, hardware and software support and maintenance, procedures for back-up and business continuity, a means for teleworkers to communicate with information security personnel in case of security

incidents or problems, and audit and security monitoring.

- TSCTI shall instruct all personnel working from home to implement fundamental security controls and practices, including but not limited to passwords, virus protection, personal firewalls, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate worksites.

## 4.24 Acceptable Use Policy

### 4.24.1 Purpose

TSCTI considers its information resources (i.e., information maintained in electronic form and systems that process, store, or transmit such information) as assets. This policy addresses the need of TSCTI to impose certain responsibilities on the users of information resources to ensure its legality, confidentiality, integrity and availability. Compliance with this policy is essential in creating an environment that is conducive to sound security practices.

### 4.24.2 Scope

This policy applies to all users of information assets including TSCTI employees, vendors, business partners, contractor personnel and functional/business units regardless of geographical location.

This policy covers all Information Technology Environments operated by TSCTI or contracted with a third party by TSCTI. The term “Information Technology Environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware, ICT equipment, software and information.

Although this policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other TSCTI Information Security policies, standards, and procedures define additional responsibilities. Information Security Steering Committee (ISSC) shall resolve any conflicts arising from this policy. In case of any conflict, US laws & regulations shall always supersede this policy.

### 4.24.3 Responsibilities

- Information Security Steering Committee (ISSC) is responsible for approving the policy and providing necessary support and resources to ensure its compliance.
- ISSC shall ensure that the policy is enforced and communicated on regular basis.
- Director, Cybersecurity and CISO shall be responsible for reviewing the policy on regular basis, for maintenance and accuracy.
- Individual users are responsible for adhering to the policy at all times.

### 4.24.4 Policy Statement

This policy addresses the need of TSCTI to impose certain responsibilities on the users of information resources to ensure its legality, confidentiality, integrity and availability.

#### 4.24.4.1 Use of TSCTI Information Systems & Processing Facilities

- Users are only authorized to utilize TSCTI information resources for official business purposes for which they have been authorized. Usage of TSCTI information systems and resources for personal use or on behalf of a third party (i.e., personal client, family member, political or religious organization, etc.) is strictly prohibited.
- Usage of TSCTI information technology to store, process, download, or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment is strictly prohibited.
- All users accessing TSCTI' information systems & information processing facilities shall establish a Non-Disclosure Agreement (NDA). Employees shall sign this as part of their employment contract & contractors, consultants, vendors, visitors, etc. will have to explicitly sign such agreements before accessing any TSCTI information system.
- Sharing or distribution of TSCTI' sensitive information is strictly prohibited unless authorized by the CEO.
- Any usage of TSCTI' information resources by guests, contractors, vendors, or any external users shall be approved by the Director, Cybersecurity and CISO and such access will be strictly reviewed.
- Printing, transmitting, or otherwise disseminating proprietary data, company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited.
- Users are not allowed to run programs obtained from external sources (via the WWW or other non-trusted source) without prior permission from IT Team and without virus protection checks.

#### 4.24.4.2 Prohibition on the Use of Unauthorized Copies of Licensed Software & Hardware

- Introduction of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement) to TSCTI information resources and the copying of such material is prohibited.
- The storage, processing, or transmittal of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement), by TSCTI personnel/ associates is strictly prohibited.
- Users shall install and use applications which are declared as acceptable to TSCTI. Such applications shall be maintained in an approved & authorized whitelist, by the IT Team.

#### 4.24.4.3 Restriction on the Use of Freeware, Shareware Applications and Games

- Introduction of freeware and shareware software whether downloaded from the Internet or obtained through any other media to TSCTI information systems will be subject to a formal security evaluation and approval process.

#### 4.24.4.4 Games are not permitted and must not be installed on systems.

#### 4.24.4.5 Prohibition on the Use of Pornographic Material

- Introduction of pornographic material into any TSCTI' information systems environment is strictly prohibited. Furthermore, any storage, processing, or transmission of pornographic material on TSCTI information systems, by TSCTI employees, contractors or any associates is strictly prohibited.

#### 4.24.4.6 Prohibition on the use of Destructive Programs

- Introduction of destructive programs (e.g., viruses, Trojans, worms, rootkits, self-replicating code, back doors, etc.) to cause intentional damage, interference with others, gain unauthorized access, or inhibit production to TSCTI information systems is strictly prohibited.

- Use of network traffic analyzer/sniffing tools without prior authorization from the Director, Cybersecurity and CISO is strictly prohibited.

### 4.24.4.7 Use of Removable Media

- Use of removable media such as USB storage and CD/DVDs are not allowed in TSCTI environment.

### 4.24.4.8 User Data Backups

- Each user is responsible to take backups of the critical information under their control.
- Users shall periodically backup the data based on its criticality in appropriate storage service provided by IT Team.
- The backups shall be treated with same level of security as the actual data.

### 4.24.4.9 Password Use

- All user-level and system-level passwords shall conform to the Password Policy:

    I. Passwords Shall be something you easily remember, and no one else can guess.

    II. Passwords shall contain both upper- and lower-case characters (e.g., a-z, A-Z)

    III. Passwords shall have digits and special characters as well as letters e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./)

    IV. User-level passwords must be at least 8 characters long & system-level passwords must be at least 12 characters long. The longer, the better.

    V. Passwords shall not be a word in any language, slang, dialect, jargon, etc.

    VI. Passwords shall not be based on personal information, names of family, friends, relations, colleagues, etc.

    VII. Passwords shall be kept confidential at all the times. User shall not share passwords with anyone.

    VIII. Passwords must not be written down, stored on any information system or storage device.

    IX. Password shall be changed at least once in 60 days by the administrators and at least once in 90 days by the users.

### 4.24.4.10 Sensitive Data Encryption

- All TSCTI users shall be accountable for the protection of TSCTI sensitive information under their custody.
- Users shall identify and encrypt all TSCTI sensitive information under their custody as per TSCTI' Data Encryption Policy that may include, but not be limited to, data stored on desktops, laptops, CDs/DVDs, USB storage and any removable media.
- Loss of or unauthorized access to TSCTI confidential information shall be immediately reported to the Director, Cybersecurity and IT Team.

### 4.24.4.11 Clear Desk and Clear Screen Policy

- All sensitive documents and any storage media containing sensitive documents shall be locked away when not required and especially when the office is vacated.
- All sensitive documents being printed shall be immediately removed from printer areas to prevent unauthorized access.
- All sensitive documents that may no longer be required or left unattended near printer areas shall be destroyed securely.
- All computer screens shall be locked when left unattended. All computer screens shall be set to lock automatically after 10 minutes of inactivity.
- All computers are to be configured to request user password on resumption from standby/screensaver.

### 4.24.4.12 Due Diligence

- Each user has the responsibility to notify the IT Team immediately of any evidence of or suspicion of any security violation with regard to:
- Unauthorized access to network, telecommunications, or computer systems.
- The apparent presence of a virus on a PC or Laptop.
- The apparent presence of any information resource prohibited by any TSCTI policy.
- Apparent tampering with any file for which the user established restrictive access controls.
- Violation of this policy or any other information security policy or procedure by another user, employee, contractor or third-party service provider.
- Each user has the responsibility to prevent unauthorized access, including viewing, of information resources in his possession or control (such as portable computer or desktop terminal/computer or printouts or media).
- Each user is responsible for providing access security against relatives, friends & neighbors, customers/clients, vendors, and unknown visitors. In situations where such people must be provided access (e.g., a vendor who has come to install a product or make repairs), then the user must oversee and monitor the actions of the individual given temporary access.

### 4.24.4.13 Right to Monitor System Use

- The systems and all information contained in the systems (including computer files, E-Mail and voice mail messages, Internet access logs, etc.) are TSCTI property.
- At any time, with or without notice, this information may be monitored, searched, examined, reviewed, disclosed, or intercepted by TSCTI for any legitimate purpose, including, but not limited to, the following:
- To monitor performance,
- Ensure compliance with TSCTI policies, legal and regulatory requests for information,
- Prevent misuse of the systems,
- Troubleshoot hardware and software problems,

- Investigate disclosure of any confidential, proprietary information, or conduct that may be illegal or adversely affect TSCTI.
- To gain access to communications deleted from the systems.
- This examination assures compliance with company policies, supports the performance of internal investigations, and assists with the management of TSCTI information systems.

### 4.24.5 <u>Compliance Measurement</u>

Any employee found to have violated this policy and other applicable laws & regulations, may be subject to disciplinary and corrective action, up to and including termination of employment. Penalties or disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Other actions as deemed appropriate by management, Human Resources, and the Legal Department.
- All exceptions must be communicated through the Policy Waiver Request Form, as defined in the waiver criteria.

### 4.24.6 <u>Waiver Criteria</u>

Requested waivers must be formally submitted to the ISSC, including justification and benefits attributed to the waiver, and must be approved by the ISSC. The waiver Shall only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time (subject to a maximum period of 1 year).

The waiver Shall be monitored to ensure its concurrence with the specified period of time and exception. At the completion of the time period the need for the waiver Shall be reassessed and re-approved, if necessary. No policy Shall be provided waiver for more than three consecutive terms.

## 5.0 Review Frequency

Review frequency and approval of this document will be at least annual or on a needed basis.

# Disaster Recovery Plan

**Plan Overview:** 22nd Century developed this disaster recovery plan (DRP) to be used in the event of a significant disruption. The goal of our DR plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible. The specific objectives of our disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical complexities of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team.

Organizations cannot always avoid disasters, but with our careful planning, the effects of a disaster can be minimized. Our objective of a disaster recovery plan is to minimize downtime and data loss. Our primary objective is to protect the organization data, including data related to our contracts with various clients, in the event that all or part of its operations and/or computer services are rendered unusable. Our plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will prevail. We measure minimizing downtime and data loss in terms of two concepts: The Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

22nd Century's Disaster Recovery (DR) and Continuity of Operations (COOP) plan is based on ensuring high priority systems and applications are architected to provide the highest degree of failover responsiveness. We will work with the line of a business owner to identify the right Recovery Time Objective (RTO) and Recovery Point Objective (RPO) metrics for applications. Our specialist develops the schedule as requested by the government and ensure that a 100% backup is completed. These recommendations based on industry best practices and our experience providing backup solutions where we back up more than 100TB of data. Our process includes ensuring backup data integrity by performing a restore of a backup randomly selected once a month. Recovery specialists restore the files, folders, and server data required by the clients within required SLAs. 22nd Century maintains a tape library and tape management system and transports tapes to the production area as needed.

**Disaster Recovery Procedures:** 22nd Century has broken disaster recovery into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.

**Response Phase: The immediate actions following a significant event.**

- On call personnel paged
- Decision made around recovery strategies to be taken
- Full recovery team identified

**Resumption Phase: Activities necessary to resume services after team has been notified.**

- Recovery procedures implemented
- Coordination with other departments executed as needed

**Restoration Phase: Tasks taken to restore service to previous levels.**

- Rollback procedures implemented
- Operations restored

**Contract Labor Provider's data back-ups:** 22nd Century backup procedures ensure that the data and software are regularly and securely backed-up, are essential to protect against the loss of data and software and to facilitate a rapid recovery from any IT failure. Whenever, data owners request data to be backed up while our backup operator (IT Technician) checks with data owners the validity of the requirements on regular basis, depending on the business environment. Our backup operator defines the backup strategy such as, job schedules and destination media for local backups and recoveries. Each and every backup job is checked for errors upon completion and the respective owner informed about the missed job. Each failed job should be recorded for auditing and problem escalation purposes. If the off-site backup media is tapes, then we restore some files from the previous tapes on regular basis and the same applies if the off-site media is a remote storage location such as, cloud or on-line backup's providers. Our backup strategy and off-site schedules vary with data criticality and with the business requirements.

Our best practice backup procedures must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates).
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- At least three generations of backup data must be retained at any one time.
- The backup media must be precisely labeled and accurate records must be maintained of backups done and to which backup set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken to ensure that they can be relied upon for use in an emergency.

**Contract Labor Provider Systems:** 22nd Century ensures full system recovery capability by scheduling proper system backups and executing daily, weekly, and incrementally. Our specialist develops the schedule as requested by the government and ensure that a 100% backup is completed. These recommendations will be based on industry best practices and our experience providing backup solutions for backup more than 100TB of data. Our process includes ensuring backup data integrity by performing a restore of a backup randomly selected once a month. The responsibility for backing up data held on the systems of individuals or multiple users. Our specialist ensures that data is backed up using one or a combination of the following methods:

- Backing-up to a local device e.g. floppy disk, Zip Drive, CD-ROM, USB storage.
- Copying critical data on a regular basis to a server that is properly backed up by the organizations.
- Backups should be scheduled regularly.
- All users should backup their data before updating or upgrading software on their systems.

Our Network Managers, System Administrators, and Application Administrators who are responsible for systems backups or for a collection of data held either remotely on a server or on the hard disk of a computer must ensure that they have comprehensive, documented and tested disaster backup procedures in line with the best practice guideline.

**Power back-ups:** 22nd Century can assist with power backup procedures and onsite training and are able to provide multi-year maintenance contract to ensure generator is properly maintained and tuned. Our emergency standby generator in place will keep business services going, ensuring continuity and possibly preventing damage while providing a safe environment. We work with electricians to develop the most cost-effective implementation strategy and help with the decisions sizing backup power generator, type of generator, fuel type and the most cost effective point at which to insert the emergency power transfer. Our industrial standby generators and generator transfer switches are configured to most demanding electrical tolerances. We have power backups that allow an organization to continue working even in rare cases of power failure. Our system administrators are responsible for maintaining equipment's, network and data backups. We have an alternate, geographically remote, secure vault for storing data backups for disaster recovery purposes.

**Telecommunications**: 22nd Century telecommunication policies and procedure have been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Our procedures have been addressing to ensure that communications can be quickly established while activating disaster recovery. Our IT Disaster Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology. Our communication team responsible for all communication during a disaster, specifically they will communicate with organizations employees, clients, vendors, and even the media if required.

Our first priority is to ensure that the appropriate authorities have been notified of the disaster, providing the following information – locations of disaster, nature of the disaster, the impact of a disaster, anticipated timelines. Our second priority to ensure that the entire company has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference for the following methods - E-mail (corporate or personal), Telephone (Home, mobile). Employees will need to be informed of the following - whether it is safe for them to come into the office, which services are still available to them. After all of the organization's employees have been informed of the disaster, our communications team will be responsible for informing media outlets of the disaster in the form of radio, television, and newspaper.

Our disaster management team that will oversee the entire disaster recovery process. They will be our first team that will need to take action in the event of a disaster and evaluate the disaster and will determine what steps need to be taken to get the organization back to business as usual in twenty-four (24) hours or less.