TTI SUCCESS INSIGHTS HOLDINGS

INFORMATION SECURITY MANAGEMENT SYSTEM MANUAL

Introduction **4**
Outline 4
Definitions 4

Authorization and Change History **5**

Management System and Documentation **6**
General 6
Objectives and Controls 6
Statement of Applicability and Supporting Documentation 7

Context of the Organization **8**
Understanding the Organization and its Context 8
Interested Parties: Their Needs and Expectations 9
External Parties 10
Internal Parties 10
Key Assets to be Protected 10
Risks and Opportunities 10
Scope 11

Leadership **12**
Leadership and Commitment 12
Information Security Policy 12
Organizational Roles, Responsibilities and Authorities 13

Planning **14**
Risk Management (See DOC A2) 14
Risk Treatment and Statement of Applicability 14
Objectives 14

Support **15**
Provision of Resources 15
Competence 15
Awareness 15
Communication 16
Internal Communication 16
External Communication 16
Documented Information (See Appendix A) 17

Operation **18**

Performance evaluation **19**
Monitoring, Measurement, Analysis and Evaluation 19

Internal Audit (See Appendix B) 19
Management Review 19
Review Input and Output 19

Improvement **20**
Corrective Action (see Appendix C) 20
Continual Improvement 20

Legal and Other Requirements **21**

Document Owner and Approval **22**

Change History **23**

Appendix A: Document Control **24**

Appendix B: Internal Audit **26**

Appendix C: Corrective Action and Improvement Process **28**

1 Introduction

This manual provides the framework for the policies and procedures which the top management of TTI Success Insights Holdings (TTI) have adopted to implement an Information Security Management System (ISMS), which complies with ISO/IEC 27001:2013 (“the ISMS”).

1.1 **Outline**

This manual explains TTI’s approach to information security.

ISO27002:2013 provided guidance on the selection and implementation of controls.

1.2 **Definitions**

Where terms used in ISO27001:2013 or ISO27002:2013 are used here, the definitions provided in ISO27000 are applied.

In particular, the ISMS is defined as the part (which includes organizational structure, policies, planning activities, plans, responsibilities, working practices, procedures, processes and resources) of TTI’s overall management system which, based on a business risk approach, enables management to establish, implement, operate, monitor, review, maintain and improve information security within TTI.

2 Management System and Documentation

2.1 General

TTI has defined a policy statement that addresses information security. This policy is stated in DOC A5

Improvements in processes within the ISMS are made using an appropriate improvement model. The preferred model is the Plan-Do-Check-Act cycle explained as:

PLAN
Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). When possible start on a small scale to test possible effects.

DO
Implement the plan, execute the process, make the product/service. Collect data for analysis in the following "CHECK" and "ACT" steps.

CHECK
Study the actual results (measured and collected in "DO" step above) and compare against the expected results (targets or goals from the "PLAN" step) to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do."

ACT
Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product.

This cycle is repeated as necessary until the desired results are consistently achieved.

Although this is the preferred model, other improvement models may be used as appropriate.

2.2 Objectives and Controls

The overall objectives contained in the policy are supported by measurable objectives as shown in DOC A3.

2.3 **Statement of Applicability and Supporting Documentation**

The Statement of Applicability is contained in the Statement Of Applicability (SOA) and includes control objectives and controls identified as necessary both as deduced from the risk assessment and from other inputs.

To support the ISMS the following information is available in documented form:

- Risk methodology and acceptance criteria
- Internal audit process
- Control of information (documents and records)
- Risk assessment
- Objectives/Measures of effectiveness
- Nonconformance, Corrective action and improvement processes
- Legal, Regulatory and other relevant requirements

This information is documented as necessary within the ISMS system.

3 Context of the Organization

3.1 Understanding the Organization and its Context

The external and internal issues that are relevant to the organization's purpose which affect its ability to achieve the intended outcome of its information security management system are:

- Gain credibility with clients and potential clients
- Conform with regulatory compliance requirements in the US and abroad (e.g. GDPR)
- Improve internal governance
- Support growth of the company and provide a framework for new staff joining the organization
- Provide credibility for partner organizations across the globe through a recognized international standard

The outcomes of the information security management system are:

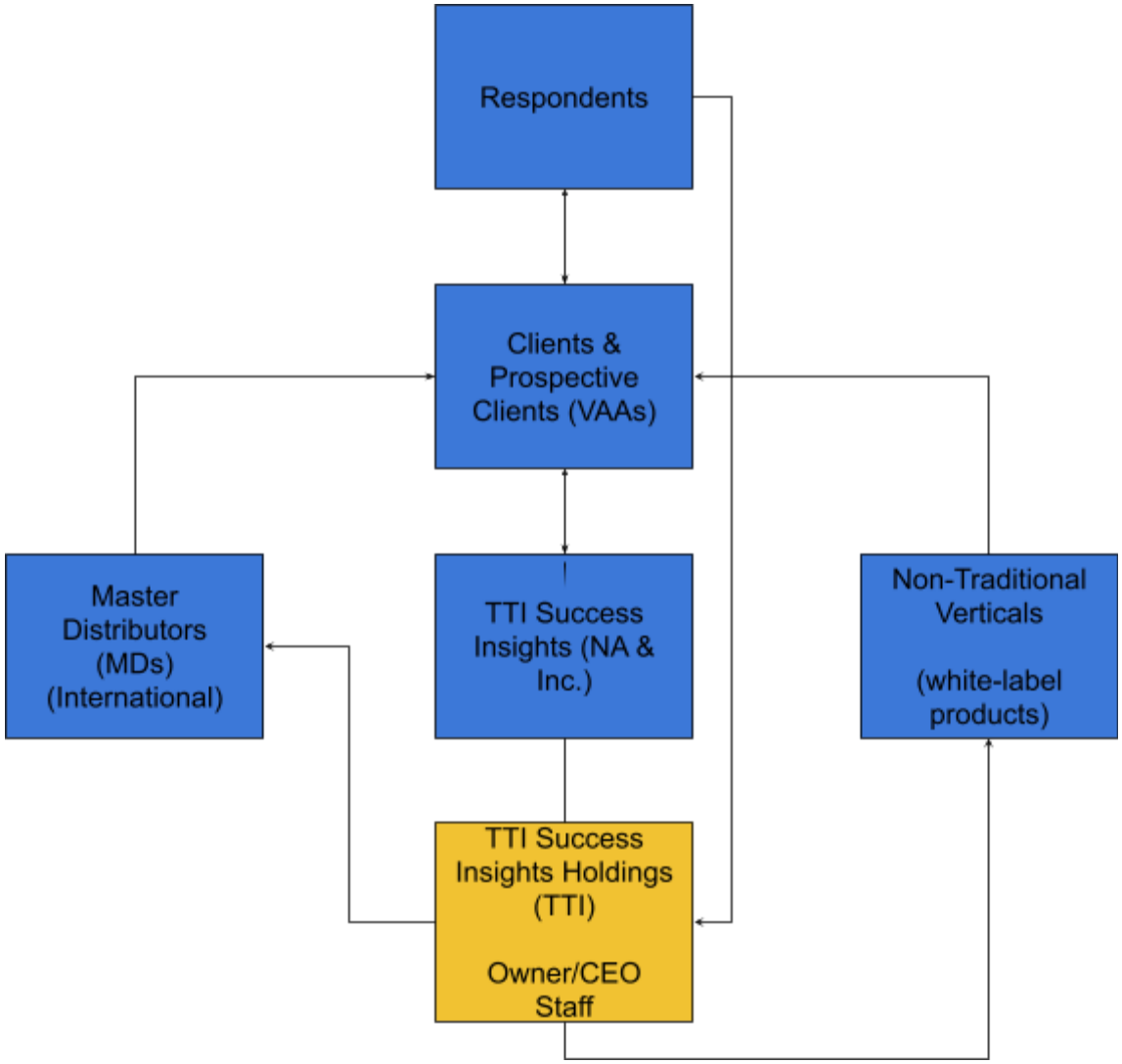
- Improved internal governance
- Demonstrable assurance to customers and partners regarding security of information
- Assist with future growth of the company

TTI identifies, and has access to, applicable legal and regulatory requirements relevant to the Management System and the interests of relevant interested parties. These legal, regulatory and other requirements have been taken into account in establishing, implementing and maintaining the Management System.

This information is documented in the Legal Register (REC 18.1), which has been compiled by the senior management team and the company's lawyers and is to be reviewed at least annually or when a significant change occurs by the same.

New or variations to legal, regulatory and other requirements are communicated to affected employees and other interested parties accordingly.

3.2 Interested Parties: Their Needs and Expectations



3.2.1 External Parties

Respondents:

- Protection of information shared (Respondent information) for confidentiality, integrity and availability and that this information will not be misused or use for any other purpose than originally collected

Clients and prospective clients, TTI Success Insights (Inc. & NA), Partner/Master Distributors (International) and Non-traditional Verticals:

- Protection of information shared (Respondent information) for confidentiality, integrity and availability and that this information will not be misused or use for any other purpose than originally collected

- Protection of client information

3.2.2 Internal Parties

Owner/CEO:

- Compliance with contractual, legal and regulatory obligations
- Security of data that is held
- Protection of the reputation and brand of the organization
- Support growth of the company
- Protection of intellectual property including patents and company information

Staff:

- Provided with a framework of appropriate rules for information security
- Provided with appropriate training
- Protection of their own personal data

3.2.3 Key Assets to be Protected

Following the review of the interested parties and their needs and expectations the following key assets require protection:

- Client information/data including respondents information
- Reputation
- Company information and intellectual property
- Staff personal data

3.2.4 **Risks and Opportunities**

Risks and opportunities relevant to the implementation of the ISMS:

- Risk that management do not follow through with commitment to information security
- Risk that resources are not available to the management system because of competing priorities
- Opportunity that the implementation of an ISMS will provide additional openings for growth
- Opportunity that internal governance arrangements are improved and provide a framework for dealing with security incidents

3.3 **Scope**

To meet its requirements for information security, TTI has established an Information Security Management System (ISMS) which operates where applicable and according to defined boundaries. The scope of the management system describes the extent to which TTI operates and includes:

- People - All IT staff, the CEO, the VP of People and any embedded or temporary contracted persons;
- Facilities - Office facilities in Scottsdale, Arizona;
- Information Processing - all IT equipment owned by, or under the control of TTI, including hardware, software, databases, mobile devices, storage media and documentation as described in business asset and documentation registers;
- Products - Intellectual property, bundled/combined services, process development environments and test products used by TTI to create business solutions. Intellectual property associated with networks designed, supplied and maintained and
- Services - Data hosting and processing, access to client data, support and maintenance services

Where the company uses the services of suppliers, contractors, or other third parties, for business support or related activities; internally or externally, information security will be addressed through formal arrangements with those parties.

The logical boundary of the ISMS is the internal network, and remote access arrangements where applicable.

The ISMS includes:

- All information processing and information assets owned or controlled by TTI
- Data which is in the custody of TTI;
- All IT people employed by TTI, including IT contractors and temporary staff;
- Processes for the provision of support services and software, including design, development, testing and delivery and;
- Products developed and sold by TTI

TTI's operates from a single office in Scottsdale, Arizona. The company is led by its founders and assigned heads of departments. TTI employs full-time staff who are office based, but also work from home or other remote locations; as required and at the discretion of the individual's manager. Additionally, there are some dedicated remote employees.

The provision of products and services offered by the organization is a key component for TTI's clients who rely on its Software-as-a-Service (Saas) products to incorporate into their own product offerings. TTI relies on suppliers of IT hardware, software and services for the operation of the business, and the delivery of services to customers.

The SaaS is offered to all customers and is not dependent on any other services. None of the services used are subject to internal regulation, nor do they have any health and safety aspects.

4 Leadership

4.1 Leadership and Commitment

TTI's information security policy (DOC A5) demonstrates top management's commitment to information security and the ISMS.

This commitment extends to all objectives, processes and controls defined within the scope of the ISMS.

Management is committed to the establishment, implementation, operation, review, maintenance and improvement of the ISMS:

- A policy for information security is established
- Objectives and plans for the ISMS have been established
- Responsibilities for specific processes are clearly defined throughout the ISMS, and are documented in individual job descriptions or otherwise where necessary
- The importance of meeting objectives and conforming to the policy, its responsibilities under the law and the need for continual improvement is communicated to the organization
- Resources are provided to establish, implement, operate, monitor, review, maintain and improve the ISMS
- An acceptable level of risk has been decided for accepting risks
- Internal ISMS audits are conducted
- Management reviews of the ISMS, including the policy, are conducted

Appropriate records of the above activities are retained.

4.2 Information Security Policy

The information security policy is developed by top management to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

The policy is shown in DOC A5. This policy and others that support the ISMS are reviewed at planned intervals, or when and if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.

The Information Security Manager (ISM) is the Owner of the information security policy and has approved management responsibility for the development, review and evaluation of the policy.

All changes to the information security policy are subject to approval by a senior management representative.

4.3 Organizational Roles, Responsibilities and Authorities

The CEO is ultimately responsible for ensuring information security is maintained at TTI and authorizes the overall policies including this manual.

The Senior Managers and Managers are responsible for ensuring that their staff and those working under their control are aware of and follow the tenets of the information security policy and the supporting management system.

Senior Managers and Managers have authority to improve the ISMS as necessary.

All staff are responsible for complying with the information security management system including reporting of information security events and incidents in accordance with stated procedures.

The ISM is responsible for ensuring that the management system complies with this manual and the supporting documentation and reporting on performance to top management. The ISM has authority for implementing and maintaining the ISMS.

See also DOC A6.1 organization

Please note: For the purposes of this manual and the ISMS that Senior Managers is the collective description (name) for the CEO, CTO, CIO and other senior roles as appropriate.

5 Planning

5.1 Risk Management (See DOC A2)

TTI has a risk management framework that identifies risks and opportunities. Risk is assessed and, where the risk exceeds a predetermined limit, then appropriate mitigations are selected. If mitigations cannot be selected or are inappropriate, then the risk owner as a function of management may accept the risk.

The risk assessment is reviewed and updated as necessary at least annually or if a significant (as deemed by the organization) change is made that affects the ISMS.

5.1.1 Risk Treatment and Statement of Applicability

TTI has considered options for treatment of risk in accordance with its risk methodology.

It has produced a Statement of Applicability (DOC SOA) which identifies the controls chosen to mitigate risk, identifies whether the control is applied, its justification for inclusion and, if applicable, the justification for exclusion of any control or controls.

A risk treatment plan is formulated to show how the measures and/or controls to mitigate risk are implemented. This includes priorities, responsibilities and proposed actions as necessary. This plan may be archived when all risk treatments have been implemented but may be resurrected should any new risks be identified that require treatment.

In approving this manual, the CEO and the ISM acknowledge that the risk owners approve the residual risk (that is the risk remaining after treatment) and the risk treatment plan.

5.2 Objectives

The objectives are identified in DOC A3 which also indicates the method of measurement, frequency and potential target as appropriate.

6 Support

6.1 Provision of Resources

The Information Security Manager is responsible for the planning, implementation and control of the ISMS and reviews all relevant procedures to ensure that they are aligned with the ISMS.

Management ensures that controls are implemented correctly and achieve the level of security required.

Management also ensures that the necessary resources (people, technology, funding, processes and time) are available to implement, maintain and continuously improve the ISMS.

Audits are performed to ensure controls and processes are functioning as expected and actions taken where identified as necessary.

Where improvements are identified, management ensures that these are actioned within an agreed time period.

6.2 Competence

Persons working within the ISMS have the necessary knowledge and skill to perform the tasks required.

Management assesses the competence as appropriate. Where the required competence is not demonstrable then the necessary skills and knowledge are obtained either from external resource, training of internal resources or a combination of these approaches.

Relevant records of competence assessment, training and other aspects are retained as necessary.

External service providers are also similarly assessed for appropriate competence in any work they provide to, or on behalf of, the company.

6.3 Awareness

Awareness of the Information Security Policy, how it relates to an individual's role, and the implications of nonconformity with the ISMS applies to relevant persons doing work under the organization's control.

Such awareness is provided to relevant staff and others as necessary and suitable records of this retained.

6.4 Communication

6.4.1 Internal Communication

Managers have responsibility, within the ISMS, for ensuring that processes for information security are effectively implemented. This will entail communicating the importance of information security and, to some extent, supervising the activities of personnel. All personnel should be made aware of their responsibilities in achieving the policy and objectives of the ISMS, and the implications of not conforming to the ISMS requirements.

The performance and effectiveness of the ISMS is reviewed by top management on a regular basis. The outcome of these reviews is fed back to all personnel.

All personnel should maintain awareness of changes to the threat environment, and to newly identified vulnerabilities, as appropriate to their roles. This may include meetings, and briefings.

Training for employees, and any other persons within the ISMS, takes place when joining the company, and on a regular basis.

Internal emails, instant messaging (i.e. Slack) and face-to-face meetings are the normal method for directed communications.

TTI's Google drive is used to store and access ISMS documentation its linked to from the Gitlab wiki so staff has a central place to access from.

Any questions regarding the information security arrangements should be directed to the Information Security Manager in the first instance.

6.4.2 External Communication

All external communication must be undertaken with consideration to the confidentiality of information, and the security requirements of the ISMS.

Customers or other external organizations may need to be informed about breaches of information security. The relevant directors or managers will inform external organizations if the breach has been shown to or has the potential to impact them. Communication should not be delayed where such a delay could increase the risk or impact on the external party. In such circumstances, an information security incident report will be raised, and the incident log should record all activities, including communications made.

If any employee is approached by a reporter, or member of the press or media, requesting comment on Company's activities, they should say nothing other than "I can't comment on that. Please get in touch with one of the company senior managers or directors." The main phone number of the company can be shared. Press communications should be properly planned and approved. If in doubt, seek advice.

Communication with supplier organizations should be carried out to ensure clear understanding of the information security arrangements of the company. Where the third party is required to implement or comply with information security arrangements, this should be documented, and agreed in writing. This may be within a contract, or other agreement.

6.5 **Documented Information (See Appendix A)**

Documented information is controlled to ensure that it remains appropriate and up to date. The control process ensures it is available and suitable for use, where and when it is needed and that it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

TTI ensures that distribution, access, retrieval and use are controlled and that the documented information is appropriately stored, preserved and legible. Changes to documents are version controlled and obsolete information is prevented from use.

Documented information of external origin necessary for the planning and operation of the ISMS is identified as appropriate and controlled.

7 Operation

This manual contains references to all of the policies and procedures that describe TTI's ISMS, its risk assessment program and its risk treatment program. These policies and procedures are implemented, and records are retained to the extent necessary to ensure that the ISMS processes have been carried out.

8 Performance Evaluation

8.1 Monitoring, Measurement, Analysis and Evaluation

TTI monitors, measures, analyzes and evaluates the performance of the ISMS. The primary measures are the objectives defined under section 6.2 above. Changes, capacity and availability are constantly monitored via Prometheus, which collects and stores measurements and alerts the operations team when metrics fall out of tolerance. Gafana is used to visualize these measurements. Logs are centralized and reviewed on an exception basis.

8.2 Internal Audit (See Appendix B)

Management have put an audit program in place and all sections of the ISMS are audited at least once a year to ensure that the ISMS:

a. conforms to the requirements of the relevant standards and any other legal, regulatory or contractual requirements;
b. meets all identified information security and business continuity requirements;
c. is effectively implemented and maintained;
d. performs as expected;

A program of audits and audit information (such as audit reports) is retained for a minimum of two years after creation. Auditors are selected and assigned based upon identified competence, objectivity and impartiality regarding the subject audit.

8.3 Management Review

A review is undertaken at least once a year to review the ISMS. The review shall make recommendations for improvement, which shall then be implemented and monitored by TTI. The ISM is responsible for ensuring this review is organized and recorded. The Senior Management receives the output from the review.

8.3.1 Review Input and Output

To ensure an informed view, the review includes, but is not limited, to the following:

a. the status of actions from previous management reviews;
b. changes in external and internal issues that are relevant to the information security management system;
c. feedback on the information security performance, including trends in:
    1) nonconformities and corrective actions;
    2) monitoring and measurement results;
    3) audit results; and
    4) fulfilment of information security objectives;
d. feedback from interested parties;
e. results of risk assessment and status of risk treatment plan; and
f. opportunities for continual improvement.
g. review and endorsement of the ISMS policies and the ISMS itself for suitability and effectiveness

The outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the ISMS.

9 Improvement

As noted in 3.1 of this document, TTI continually improves the ISMS.

9.1 Corrective Action (see Appendix C)

TTI identifies nonconformities and takes appropriate action to eliminate the cause of the nonconformity. This is achieved by reviewing the nonconformity, determining the cause(s) of the nonconformity wherever possible, determining if similar nonconformities exist, or could potentially occur, evaluating the need for corrective action, determining and implementing the corrective action needed, reviewing the effectiveness of any corrective action taken and making changes to the ISMS, if necessary.

Any action needed is implemented and such action reviewed for effectiveness including changes to the ISMS.

Appropriate documented information on the action taken is retained.

9.2 Continual Improvement

Continual Improvement is a continuous process through various elements of the ISMS as documented throughout this manual. Information used includes; Risk & Opportunities Analysis, the Quality Policy, objectives, individual training matrices, internal audits, 3rd party audits and the management reviews.

10 Document Owner and Approval

The Information Security Manager is the Owner of this document and is responsible for ensuring that this document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This manual was approved by the Chief Executive Officer (CEO)

Signature: David Bonnstetter

Date: 2021 / 08 / 17

Change Log

11 Appendix A: Document Control

11.1.1 Documents within the ISMS are controlled.

11.1.2 Each document has a title and a reference. The reference is defined by the ISM. Generally, 'DOC' refers to procedures or work instructions, 'REC' applies to forms/records. If in a wiki, the document can omit the title DOC or REC and the title of the wiki page will be self-evident.

11.1.3 Each document has an issue number. The initial issue is 1. This is incremented by 1 for each revision so that the second issue is 2, the third issue is 3 and so on. Filenames may use 'v' to denote the issue (e.g. v1 represents issue 1, v2 represents issue 2 and so on: this is to prevent confusion with the letter 'i' for issue as in i1). In the case where a Google document is used, a new document version shall be named when editing is complete. If said document is a wiki page, it is unnecessary to maintain any such versioning as the nature of the wiki keeps a record off all saved changes.

11.1.4 Each procedural document (procedure/work instruction) has a history 'block' to show the revision status and the changes made. This procedure may be used as a model for any similar document. In the case where a Google document is used, a new document version will also be named. Furthermore a Google document has no need of a change history block, since all changes are preserved. If said documentation is in a wiki, it is unnecessary to maintain any such revision block as the nature of the wiki keeps a record off all saved changes.

11.1.5 Once authored, each relevant document is approved. In general, the document is approved by the head of function to which it applies. If the document is applicable to the entire organization then the approval is that of the CEO unless they have delegated such authority. During the creation phase (that is prior to approval), filenames of documents should be appended with the term 'draft' to signify that the version is not yet approved. The 'draft' term is removed once the document is approved. Thus a new document would have in its filename "DOC X.Y {Document title}_ v1_ draft". Once approved the document would have the draft removed and become "DOC X.Y {Document title}_ v1". Similarly a revised version would become "DOC N.M {Document title} _v2_draft" until approved at which time the 'draft' would be removed and the document issued as "DOC N.M {Document title} _v2".

11.1.6 Once approved, the document is changed to PDF format and added to the master ISMS location and staff are informed (usually by e-mail) of the issue/revision of the document.

11.1.7 Documents of external origin required to support the ISMS are marked as the property of TTI and filed by the ISM in a location with controlled access.

11.1.8 Once superseded, old documents are withdrawn. The ISM retains a copy of the superseded/withdrawn document in the native format (Word, Excel etc.) in an Archive folder which has limited access granted only to authorized persons. All other versions (PDFs, etc.) are destroyed (deleted).

11.1.9 The CEO authorizes the ISM to mark documents as approved where appropriate by use of a signature image that can only be accessed by the CEO and the ISM.

11.1.10 Records

Records are retained by the organization.

The following are key record types retained:

Record type	Owner	Minimum retention	Location
Client records	CEO	<3> years	Databases
Financial records	CEO	<6> years	Quickbooks
Code	CTO	indefinitely	Gitlab
HR records	CEO	<6> years	HRIS (Bamboo)
Sales Records	CEO	<3> years	Netsuite
Internal audit	ISM	<3> years	Google Drive
Management review	ISM	<3> years	Google Drive
Contracts	CEO	<6> years	HelloSign or filing cabinets
Corrective actions	ISM	<2> years	Google Drive
Incidents	ISM	<2> years	Google Drive

12 Appendix B: Internal Audit

12.1 Internal audits shall be carried out to obtain objective evidence that TTI consistently conforms to planned arrangements in the following areas:

- Meeting the requirements of the ISO 27001:2013 Standards;
- The ISMS has been effectively implemented and maintained;
- The agreed processes, procedures and policies are being followed;
- To identify improvement opportunities;
- To ensure conformance to identified information security requirements and relevant legislation and regulations.

12.2 An audit program is planned and an Audit Schedule documented considering the status and importance of the activities and areas to be audited, together with the results from previous audits.

12.3 The scope, frequency and methodology are decided during audit planning, ensuring that the entire ISMS is audited annually. Only suitably trained personnel will carry out internal audits.

12.4 The results of all audits conducted will be documented on the Audit Report Form and subject to management review.

12.5 Timely corrective actions are taken on any non-conformities found and preventive action is taken and documented on the Risk Register to prevent recurrence.

12.6 Non-conformities and/or opportunities for improvement will be managed in the Improvement Log. An audit follow-up will be conducted to verify that all planned actions have been satisfactorily completed.

14 Appendix C: Corrective Action and Improvement Process

14.1 A Nonconformity is any non-fulfilment of one or more requirements. A few examples of this are:

i) A procedure not being followed as defined
ii) A policy not being complied with
iii) An output of a process deviating from that required such as an induction form not being completed for a new hire

14.2 When such a problem or potential improvement is identified, each Employee/Staff has a duty to inform their Manager of the issue, either verbally, by e-mail or by using a Nonconformity Report (REC MS-3A).

14.3 The nonconformity is entered by the Manager into the Improvement log (REC MS-4A).

14.4 The ISM assigns the item to a responsible Director or Manager. As necessary, the REC MS-3A report is also provided to the responsible Director or Manager.

14.5 The Director or Manager identifies:

- Root cause where possible
- Immediate action to correct the issue (correction)
- Action to prevent recurrence (corrective action)

14.6 The responsible Manager/Director is then responsible for ensuring the action is undertaken within the agreed timeline/due date.

14.7 This is reported to the ISM and entered onto the REC MS-3A form as appropriate and returned to the ISM. The ISM ensures the REC MS-4A log is amended accordingly along with a due date.

14.8 After the due date has fallen, the ISM reviews the action taken with the responsible Manager or Director and determines if the item has been appropriately addressed, the effectiveness of the action taken and whether any further action is required. The log (REC MS-4A) is updated with the status and the issue is closed when the action taken has been completed satisfactorily.

14.9 If the action taken is ineffective and the responsible Manager or Director is not able to address the issue in a satisfactory manner, then the ISM may raise the issue to the next level of management and eventually with the CEO or equivalent.

14.10 Similarly, observations from audit, relevant points from risk assessment, feedback and suggestions from client and staff are fed into the corrective action process for review and action as opportunities for improvement.

14.11 The ISM regularly monitors the progress of outstanding Nonconformity Reports. If any action has not been completed by the previously agreed date, they will agree and record new actions and/or dates. If not satisfied that achievable progress is being made, they will escalate the matter to higher line management responsible for that area.

HELLOSIGN

Audit Trail

TITLE	Information Security Manual
FILE NAME	Information Security Manual
DOCUMENT ID	9a5feceea3e7bab2a21ca88b9400c74e6def45bb
AUDIT TRAIL DATE FORMAT	YYYY / MM / DD
STATUS	● Completed

This document was requested from n-tladee57e5xfjw46eosnyz4qawcbuqhlg6pb6ry-0lu-script.googleusercontent.com

Document History

SENT	**2021 / 08 / 17** 11:12:42 UTC-6	Sent for signature to Dave Bonnstetter (dave.bonnstetter@ttiltd.com) from john.kloian@ttiltd.com IP: 208.186.1.4
VIEWED	**2021 / 08 / 17** 11:47:00 UTC-6	Viewed by Dave Bonnstetter (dave.bonnstetter@ttiltd.com) IP: 208.186.1.4
SIGNED	**2021 / 08 / 17** 11:47:17 UTC-6	Signed by Dave Bonnstetter (dave.bonnstetter@ttiltd.com) IP: 208.186.1.4
COMPLETED	**2021 / 08 / 17** 11:47:17 UTC-6	The document has been completed.