INFORMATION SECURITY POLICY

Doc. Reference:	TRAQ-ISMS-01-100
Revision:	3.0
Confidentiality level:	Public
Effective Date:	01/01/2024
Owner:	Information Officer (IO)
Reviewed by:	Managing Director

Revision History

Date	Revision	Change by	Description of change
01/09/2022	1.0	Deidre Miller	Document Creation
21/09/2022	1.1	Azel Marais	Updated header + footer with new logo, updated confidentiality level.
27/10/2022	1.1	Tinus van Staden	Document Review
13/02/2023	1.2	Tinus van Staden	Document Reviewed and amendment of formatting of section 3.
06/03/2023	1.2	Anthea Canham, Azel Marais	Effective date updated, added full document name for Scope, US to UK spelling.
26/06/2023	2.0	Anthea Canham	Inclusion of introduction, definitions, classification, objectives, info labelling, handling of classified info and training. Addition of policy references where applicable.
16/11/2023	3.0	Anthea Canham, Tinus van Staden, TJ de Bruyn	Change in document letterhead in line with rebrand, change in font and general layout. Amended Types of Information under section 7. Corrections to spelling and punctuation

Contents

1. Introduction & Purpose

This policy acts as the foundational document to all other security policies and associated standards. We acknowledge and understand the need to protect sensitive information. This policy therefore defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
- manage the risk of security exposure or compromise.
- assure a secure and stable information technology (IT) environment.
- identify and respond to events involving information asset misuse, loss, or unauthorised disclosure.
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can have a negative impact on business (e.g., infrastructure damage / failure, financial loss etc.) and result in legal and regulatory non-compliance.

Traq Software (Pty) Ltd t/a Traq Software Solutions (inclusive of Traq Technical (Pty) Ltd), hereafter referred to as "Traq", will conduct business in compliance with applicable laws, rules, standards, and its values. The confidentiality, integrity and availability of information assets are key to Traq's objectives. This policy sets to define how Traq intends to deal with information security. Traq's information security strategy includes the implementation of a robust risk management structure, to ensure the security of its information assets.

2. Scope

This policy applies to the scope as defined in the scope document, titled, TRAQ-ISMS-01-101.1_ISMS_Scope.

3. Objectives of the ISMS

- To ensure that organisation information assets are available, when required, to authorised users.

- To ensure organisation information assets are adequately protected against unauthorised access, malicious or accidental loss, misuse, or damage.
- To ensure that all users of the organisations information assets are aware of and fully comply with this policy, supplementary policies, processes, standards, procedures, and guidelines.
- To ensure that all users of the organisation's information assets understand their responsibilities for protecting the confidentiality and integrity of the organisations Information Assets.
- To ensure that the risks to the Organisation Information Assets are appropriately managed.
- To perform risk management as a critical process to determine the organisation's foresight on how risks will be mitigated during any phases of business growth.
- To ensure that information security incidents are identified and resolved promptly and appropriately.
- To raise awareness of issues from approved Cyber Security vendors to build and improve the capability for the Organisation to manage cyber security threats effectively.
- To ensure the effectiveness of the ISMS, continuous improvement initiatives shall be regularly reviewed by management and shall be communicated to all relevant stakeholders. Relevant metrics will be reviewed on an annual basis to assess whether it is appropriate to change them, based on collected historical data. Ideas for improvement will be obtained via regular meetings and other forms of engagements.
- To protect the Organisation from any legal liability resulting from information security incidents.
- Data classification and appropriate information handling procedures will facilitate good information management within the Organisation and ensure that Organisation data (from creation to retention and / or destruction) is handled in a manner that safeguards the confidentiality, integrity, and availability of the data.
- To establish processes that will ensure essential business operations and services are sustained while recovering from a major information system failure or a disaster.
- Management of information security incidents in a prompt and appropriate manner will enable the Organisation to efficiently mitigate the risks of any legal implications that may be associated with information security incidents.

4. Definitions

Term	Definition
Information Security	The state of being protected against the unauthorised use of information.
Cyber Security	Is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
Confidentiality	Ensuring that only those who are authorised, have access to specific assets and those who are unauthorised are actively prevented from obtaining access.
Integrity	The assurance that the data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.
Availability	Ensuring that authorised users have timely, reliable access to resources when they are needed.
Classification	The grading or regrading of information in accordance with its sensitivity or in compliance with a security requirement.
Re-classification	
Public	See subsection 6.2.
Private	See subsection 6.2.
Confidential / Internal	See subsection 6.2.
Restricted	See subsection 6.2.
Compromise	Unauthorised disclosure, modification, substitution, or use of data, or the unauthorised modification of a security system, device, or process.
Breach	Involves the unauthorised access, disclosure, or acquisition of personal data, protected &/or confidential data.

5. Roles & Responsibilities

The Organisation is responsible for compliance with Legislation, Rules, Standards, Codes of Good Practice. Responsibility is delegated to senior management and Employees who are responsible for compliance with this Policy and Legislation, Rules, Standards and Codes of Good Practice.

The Governing Body & Executive Management shall:

Ensure the information security strategy aligns with the organisation's strategic objectives.

- Endorse the implementation of approved policies, processes, standards, and procedures.
- Provide access to adequate resourcing and supporting information security initiatives.
- Ensure risks are mitigated to acceptable levels.

The Head of Information Systems and technology is responsible for ensuring the protection of IT-based Information systems and the implementation of specific security processes.

Management shall:

- Communicate policies and procedures.
- Monitor adherence to this Policy.
- Ensure risks are identified and mitigated to acceptable levels.
- Report any non-compliance with this Policy.

All Employees shall:

- Ensure that they familiarise themselves with and comply to this Policy, and all applicable processes, standards, procedures, and guidelines.
- Ensure that they complete the information security training and understand their obligations.
- Report information security incidents via the appropriate procedure promptly.

All Service Providers, Third Parties and guests who access, use, handle and / or manage Organisation information assets shall:

- Ensure that they familiarise themselves with the Information Security Policy, and all applicable processes, standards, procedures, and guidelines.
- Ensure that they provide the necessary awareness and training to their staff.
- Report information security incidents via the appropriate procedure promptly.

6. Data Classification

6.1 Classification Criteria

The level of confidentiality is determined based on the following criteria:

- value of information – based on impacts assessed during risk assessment.
- sensitivity and criticality of information – based on the highest risk calculated for each information item during risk assessment.
- Legal and contractual obligations.

6.2 Confidentiality Levels

Confidentiality level	Labeling	Classification criteria	Access restriction

Public	(unlabeled)	Data should be classified as public when the unauthorised disclosure, alteration or destruction of that data would result in little or no risk to Traq. While little or no controls are required to protect the confidentiality of public data, some level of controls is required to prevent unauthorised modification or destruction of public data.	Information is available to the public.
Private	Private	Data should be classified as Private when the unauthorised disclosure, alteration or destruction of that data could result in a moderate level of risk to Traq or its Clients. Data that is not explicitly classified as restricted or public data should be treated as Private data. A reasonable level of security controls should be applied to Private data. - Can be shared with a client etc. if an NDA or contract is in place.	Information is available to all employees and selected third parties.
Confidential / Internal	Confidential / Internal	Data is restricted to management approved internal access and protected from external access. Unauthorised access could influence Traq's operational effectiveness, cause a financial loss, provide a significant gain to a competitor, or cause a major drop in Customer / Client confidence. Information integrity is vital. The highest level of security controls should be applied to confidential / internal data.	Information is available only to a specific group of employees and authorised third parties.
Restricted	Restricted	Data should be classified as Restricted when the unauthorised disclosure, alteration or destruction of the data could cause a significant level of risk to Traq or its Clients. The highest level of security controls should be applied to restricted data.	Information is available only to individuals in the organisation and must be password protected if shared with authorised third parties.

6.3 List of Authorised Persons

Information classified as "Restricted" and "Confidential/Internal" must be accompanied by a list of Authorised Persons in which the information owner specifies the names or job functions of persons who have the right to access that information.

The same rule applies to the confidentiality level "Private" if people outside the organisation will have access to such a document.

6.4 Reclassification

Asset owners must review the confidentiality level of their information assets every year and assess whether the confidentiality level can be changed. If necessary, the confidentiality level should be lowered.

7. Types of Information

- Documentation (physical hard copy and electronic).
- Information transfer (email, SFTP, Teams, face to face, telephonically).
- Data stored on NAS, SharePoint, OneDrive, SQL Databases.
- Applications (WhatsApp).

8. Handling Classified Information

All persons accessing classified information must follow the rules listed in the following table. Line Managers must initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorised persons. Each incident related to handling classified information must be reported in accordance with TRAQ-ISMS-01-204_Incident_Management_Procedure.

Information assets may be taken off-premises only after obtaining authorisation in accordance with the TRAQ-IT-01-110_Acceptable_Use_Policy.

The method for secure erasure and destruction of media is prescribed in the document TRAQ-IT-01-105_Disposal_&_Destruction_Policy.

	Private	**Confidential / Internal**	**Restricted**
Paper documents	• Only authorised persons may have access. • Documents may only be kept in rooms without public access. • Documents must be frequently removed from printers.	• The document must be stored in a locked cabinet. • Documents may be transferred within and outside the organisation only in a closed envelope. • If sent outside the organisation, the document must be mailed with a return receipt service. • Documents must immediately be removed from printers. • Only the document owner may copy the document.	• The document must be stored in a locked cabinet, in a controlled /restricted area. • The document may be transferred within and outside the organisation only by a trustworthy person in a closed and sealed envelope. • The document may be printed out only if the authorised person is

		• Only the document owner may destroy the document.	standing next to the printer.
Electronic documents	• Only authorised persons may have access. • When files are exchanged via services such as SFTP, instant messaging, etc., they must be password protected. • Access to the information system where the document is stored must be protected by a strong password. • The screen on which the document is displayed must be automatically locked after 3 minutes of inactivity.	• Only persons with authorisation for this document may access the part of the information system where this document is stored. • When files are exchanged via services such as SFTP, instant messaging, etc., they must be encrypted. • Only the document owner may erase the document.	• The document must be stored in encrypted form. • The document may be stored only on servers which are controlled by the organisation. • The document must not be exchanged via services such as SFTP, instant messaging, etc. • The document must be password protected.
Information systems	• Only authorised persons may have access. • Access to the information system must be protected by a strong password. • The screen must be automatically locked after 3 minutes of inactivity. • The information system may only be in rooms with controlled physical access.	• Users must log out of the information system if they have temporarily or permanently left the workplace. • Data must be erased only with an algorithm which ensures secure deletion.	• Access to the information system must be controlled through an authentication process using smart cards or biometric readers. • The information system may only be installed on servers controlled by the organisation. • The information system may only be in rooms with controlled physical access and identity control of people accessing the room.
Electronic mail	• Only authorised persons may have access. • The sender must carefully check the recipient. • All rules stated under "Information systems" apply.	• E-mail attachments must be encrypted if sent outside the organisation.	• All e-mail attachments must be encrypted.
Electronic storage media	• Only authorised persons may have access. • Media or files must be password protected. • If sent outside the organisation, the medium must be sent as registered mail. • The medium may only be kept in rooms with controlled physical access.	• Media and files must be encrypted. • Media must be stored in a locked cabinet. • If sent outside the organisation, the medium must be mailed with a return receipt service. • Only the medium owner may erase or destroy the medium.	• Media must be stored in a locked cabinet, in a controlled /restricted area. • Media may be transferred within and outside the organisation only by a trustworthy person in a closed and sealed envelope.
Information transmitted orally	• Only authorised persons may have access to information.	• The room must be soundproof. • the conversation must not be recorded	• Conversation conducted through a means of communication must be encrypted.

	• Unauthorised persons must not be present in the room when the information is communicated.		• No transcript of the conversation may be kept.

9. Training & Awareness

9.1 All Staff

- In line with the annual policy review, all employees shall refresh their understanding annually via the LMS. This will be self-study and include an assessment.
- Awareness posters will be utilised to enhance understanding.
- All employees will always have access to the policy via the LMS.

9.2 Suppliers & Contractors

This will apply to all Service Providers, Suppliers, Contractors, and Third Parties. They will be made aware of this policy upon onboarding, and where changes to the policy are made.

10. Incident Management

In the event of a compromise or breach please follow the incident management procedure as depicted in TRAQ-ISMS-01-204_Incident_Management_Procedure.

11. Disciplinary Disclaimer

Non-compliance, either intentionally or negligently may lead to an improvement request being issued as part of continuous improvement, or to disciplinary action, which may lead to termination of employment.

The employee may be personally liable for civil and / or criminal penalties.

The Organisation may, in its discretion and will, if so required, report violations to the relevant authorities.

NB: Refer to HR disciplinary policy.

12. Contractual Action: Non-Staff Members

Non-compliance, either intentionally or negligently, by Suppliers, Service Providers, Third Parties and / or guests will lead to contractual remedies which may lead to termination.
The Service Provider, Third Party and / or guest may be personally liable for civil or criminal penalties.

13. Validity & Document Management

This document is valid as of **01/01/2024.**
The owner of this document is the Information Officer who must check, and if necessary, update the document at least once a year.