TRUST
INTEGRITY
COMPLIANCE

Data Management and Data Security Policy

JUNE 2023

ticcompany

www.ticcompany.com

Data Management and Data Security Policy

The Customer Due Diligence (CDD) process requires that tic companies collect confidential and legally privileged data from our clients, and their customers. Data is managed using strict and clearly defined processes. Tic company has adopted the ISO 27001 international standard as its governance framework for the hosting, retention and security of data collected.

How does tic secure client data?

Tic company provides our Clients with two primary mechanisms to transfer confidential and legally privileged data:

1) an Online Form; and

2) Secure Cloud File Storage.

As a 3rd option and a fallback, we also accept data sent to us via email.

- For both transfer mechanisms, any data (files) shared with tic company via email (or Dropbox) is stored at rest in an online cloud file store, with 256bit Encryption, and with 2- factor authentication.

  Data is encrypted in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) between the File store and the linked online form. This creates a secure tunnel protected by 128-bit or higher.

- Photos transferred to tic company via our online e-forms are attached only to the form itself, and not stored on the device that took the photo (i.e., not stored on the smartphone).

  This helps people collecting private information by preventing them from inadvertently storing their customers personal information on their devices, and thereby breaching privacy obligations.

What does tic use our data for?

- For the purposes of conducting AML/CFT Customer Due Diligence tic company acts as agents (with authority under section 34 of the AML/CFT Act).
- The Act requires that for standard Customer Due Diligence information is captured and confirmed as follows:

    - Correct legal name, and any previous names as necessary
    - Physical residential address
    - Sufficient information to establish the risk posed by the customer, in the context of the transaction being carried out.

- Tic company only uses data collected for AML/CFT purposes, and in accordance with the requirements of the AML/CFT Act.
- Information gathered is compartmentalised by client: tic company is careful to prevent co-mingling.
- The primary activity is to verify information supplied against other sources to confirm reliability.
- Tic company does gather Open-Source information on an event driven basis. In crude terms this is like (and may literally be) a “Google” search. While we note this was carried out, we only capture specific, relevant information if it arises.

What is retained, and for how long?

- For the purposes of conducting AML/CFT Customer Due Diligence tic company acts as agents (with authority under section 34 of the AML/CFT Act).
- Files are retained for 5 years from the time the Customer ceases their business relationship, in accordance with the requirements of the AML/CFT Act.
- Tic company retains summary level information, together with sufficient referencing to allow the source to be verified.
- Tic company’s primary records only hold basic information to minimise the risk of identities being confused such as name, address, date & place of birth, together with relationship links (such as connecting an individual to their family Trust).
- Information is stored across different cloud platforms, segregated according to sensitivity and client workflow options. This is compartmentalisation approach significantly reduces risk of breach. Each platform is subject to stringent standards for backup, disaster recovery and security that can be accessed at the following links: 1, 2, 3, and 4.

When a client submits a CDD request what data is sent back to the requestor?

- On submission of a Customer Due Diligence Request a copy of ALL information and a link to the attachments is sent via email to the nominated AML Compliance Manager and/or AML Coordinator.
- The Outcome Report confirming completion of Customer Due Diligence is only sent to the AML Compliance Manager.
- Neither the submission receipt or the outcome report is sent to any other party.
- The report confirms the entities upon which due diligence was carried out, the risk rating that was assessed against the Customer, the type of due diligence carried out and the fee for the job.
- No information other than this (including personal details) is shared.

Do clients of tic company also keep a copy of the information collected on their behalf?

- In accordance with good Privacy practice, tic company encourages its clients to keep only the bare minimum information necessary.
- Tic company retains sufficient information to meet AML/CFT data retention requirements related to onboarding.
- Tic company does not retain transaction information - the Client retains these records.
- In the event a government supervisor or auditor requires access, Tic undertakes an authorisation process and then provides necessary records.

Does tic company perform vulnerability and penetration testing?

Vulnerability and penetration testing is performed by tic company's CRM provider, Salesforce. The performance reviews are undertaken annually and any issues discovered are tracked and resolved in accordance with corporate policy and industry best practice. Reports and attestations are available on request.

Validity and document management

This document is valid as of 22 June 2023. This policy must be published at www.ticcompany.com. The owner of this document is tic company IT department, who must check and, if necessary, update the document at least annually. Any concerns or major amendments must be notified to the tic company board for consideration.