Security and Safeguard

This document explains how DataTracks (including its affiliates outside the EEA) secure and safeguard Personal Data collected from you during transit for processing and rest.

Information Collection

As a registered user, the information provided by you will be used to

- contact you in relation to the services and solutions you signed up for
- make updates that may affect the use of such services and solutions
- continually evaluate, develop and improve such services and solutions as well as your experience thereof.

Any Personal Data like the name of Shareholders of companies or entities contained in financial statements or documents sent to us for processing will be used only for the purpose of providing intended services or support.

We retain and use your Personal Data as long as it is necessary for fulfilment of the respective purposes as specified in this section.

We classify all Personal Identifiable Information (PII) as Confidential as per our Information Classification procedure and handle appropriately.

Disclosure

Personal Data collected from you will not be disclosed without your consent. Exception to this is when such disclosure is necessary for compliance to any legal and/or law enforcement obligations. We will do so after following necessary due processes.

We will make every effort, where possible, that such mandated disclosures are communicated to you.

Data Security and Safeguard

We are committed to protecting your Data in our custody.

We take reasonable steps to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data from unauthorized access, alteration, transmission and deletion.

- DataTracks undergoes several independent third party audits SOC 1 (Formerly SSAE18 or ISAE 3402) and ISO 27001
- DataTracks retains a 3rd party to conduct periodic penetration tests.
- DataTracks performs periodic network vulnerability scans using commercial tools.
- Customer data is logically segregated by domain to allow data to be produced for a single tenant only.
- DataTracks has built multiple redundancies in its systems to prevent data loss.
- DataTracks operates a global network of data centers to reduce risks from geographical disruptions.
- DataTracks performs annual testing of its business continuity plans and disaster recovery

program.

- DataTracks team maintain all policies and procedures
- Data stored at rest can be configured to stay in a geographic region.
- DataTracks supports the use of open encryption methodologies.
- DataTracks has established procedures and technical controls to help ensure production data remains in the secure boundary of the production network.
- DataTracks maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
- DataTracks use and management of encryption keys is transparent to customers.
- DataTracks maintains a personnel policy that includes disciplinary procedures.
- Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, DataTracks confidentiality and privacy policies.
- DataTracks reviews NDA and confidentiality documents as needed.
- DataTracks maintains a security awareness program for its personnel.
- DataTracks monitors its access lists carefully to minimize the potential for unauthorized account use.
- DataTracks employs a vendor management process that includes contractual requirements to adhere to security policies and onsite inspections, as needed, to confirm compliance.

Service Delivery centre security

- The service delivery zone is a restricted area with all entries/exits controlled, monitored and recorded.
- All workstations are located within the service delivery zone and contain high quality computing and telecommunication assets.
- No recording medium or device (paper, pen, USB flash drives, mobile phones with cameras or CD/DVDs) is permitted inside the service delivery zone.
- No paperwork can be taken out of the service delivery zone. Everything is either stored in the zone or shredded in the zone depending on our archiving policy.
- Our service delivery centre network is ring fenced by firewalls that control access, protect our databases, detect intrusion and provide logical security.
- Our service delivery centres are also inter-connected via dedicated high-speed private leased lines.
- All software in our delivery centres is licensed.
- Our service delivery centres have full power back up from two independent sources to minimise disruption in service due to power outage.