DATA SECURITY OVERVIEW

The TicTocTrack Monitoring platform and apps are hosted with 6YS a Brisbane based company founded in 2003 with the express purpose of providing highly reliable, business-grade hosting services.

In addition to the services they offer iStaySafe they also look after commercial grade secure hosting for companies such as Queensland Rail, Treasury and several universities to name a few.

INFRASTRUCTURE

We host our platform on a **Virtual Server** with **Virtual private cloud infrastructure** in order to isolate our software from other virtual networks in the cloud.

Type of Servers and Firewalls

- VMware Enterprise and Dell Servers
- NetApp storage
- Brocade switches & routers
- and Fortinet Firewalls.

6YS provides us with a **managed service** that includes 1 months worth of off site back ups that are maintained by them.

6YS SECURITY COMMITMENT

Introduction

6YS security is addressed at several different levels. At a high level, these are:

- Physical Security
- Network Security
- Data Security
- User Security

6YS utilises a broad spectrum of security technologies to ensure a vastly superior level of security as to what most small or medium enterprises could afford.

In order to protect the security of our clients, and as many of our security mechanisms are proprietary, there is a limit to the level of detail we can disclose in this document. We have, however, tried to give a high level overview as to how we achieve a secure operating environment.

Physical Security

6YS utilises multiple data centre facilities throughout Australia.

All 6YS facilities comply with the following minimum requirements:

- Located in buildings where the name of the data centre is not advertised or otherwise visible from the street / front of the premises. It is also not obvious in any other way that these buildings contain data centres
- Two factor authentication to gain physical access to the facility (e.g. any two of the following: physical access token or key, PIN code, biometric scan, personal identity verification through photo ID check)
- 24x7 CCTV recording
- Individually keyed racks
- All 6YS equipment is labeled in such a way that it does not identify that it belongs to 6YS as visible from outside the rack cabinet

Furthermore, our primary data centre facilities comply with the following additional requirements:

- Manned 24x7 with Network Operations / Security staff on-site
- Access to individual racks must be granted by 6YS management
- Tier 3 power design including, full 2N power rails to protect against sabotage or failure of a power subsystem
- Facility power is fully contained (i.e. all power systems including generators & fuel tanks are contained within the concrete DC structure) ensuring the facility can operate on diesel for a minimum of 72hrs without refueling in the event of physical damage to mains power feeds
- PCI-DSS Compliance

Network Security

Integrity and security of 6YS networks is ensured using a combination of the following technologies and methodologies:

External / Internet Networks

- Exclusive use of industry-leading ICA Certified FortiGate firewalls
- Intrusion Detection and Prevention (IPS)
- Core web-facing systems are located in a DMZ
- Strict change management and approval processes for ALL firewall changes

Internal / Local Area Networks

- Virtual LANs (VLANs) used to separate networks
- Internal FortiGate firewalls used as gatekeepers between VLANs
- Centralised data logging of all activity on core systems (including configuration changes, network events etc)

Data Security

Since 6YS stores customer data in various different ways depending upon the service being consumed (e.g. APPSPOINT, Hosted Exchange, IRONPOINT etc) the methodologies used differ between systems. Some of these methodologies include:

- Automated management of Access Control Lists from our Provisioning System (to eliminate user error during customer provisioning)
- Use of Access Based Enumeration (users can only see the data that they have permission to access, removing temptation and rendering resource enumeration attempts ineffective)
- Leveraging technologies with multi-tenancy built into their DNA (e.g. NetApp Virtual Filers)
- All backup data is secured with equal importance to production data
- No data (backup or otherwise) ever leaves Australia without the customers' explicit authorisation
- Deeply ingrained philosophy across all engineering and support staff of our single most important core value: The absolute separation of customer data. By adopting this value in our organisational culture, we can ensure that human error is virtually non-existent

User Security

Over 90% of all electronic security breaches occur due to user error, or social engineering (i.e. giving away a password to a hacker over the phone). As a result, 6YS treats user security very seriously:

Internal Staff:

- All administrative account passwords meet high complexity requirements and are changed at regular intervals
- There is no means by which an administrative account can directly access the 6YS network externally, without first authenticating via another means
- Auditing is used throughout all systems to track administrative logins and access to resources
- We run police and background checks on all new staff
- New staff are vetted for a minimum of 30 days before being issued any administrative access whatsoever to 6YS systems

Customers:

- When setting passwords for users, we always utilise passwords that represent an optimal combination of security, and ease of remembering.
- We encourage our users to regularly change their passwords, and enforce minimum security standards when doing so.
- We endeavour to educate our customers in safe practices regarding the protection of their credentials.
- Several methodologies are implemented to detect attempts to compromise user accounts and to lock these out as required.