manyother ltd

Pragmatic TRACKER

Information Security Policy

Version 1.0	Sept 2016
V1.1 update	Dec 2016
V1.2 update	April 2017
V1.3 update	Nov 2017
V1.4 update	Feb 2018
V1.5 update	April 2018

Introduction

This document describes the policy approach that Manyother Ltd takes towards information governance across the organisation. The company was formed in 2011 with the intention of developing innovative products and services to facilitate change management in the health and wellbeing field.

We take a systemic and holistic approach to information security, regarding it as an iterative process of continuous review and refinement.

Legal frameworks

The intellectual property right (IPR) of our products and services is wholly owned by ourselves and are protected by licence agreements. In turn, we take care not to infringe the intellectual property of others and ensure we observe copyright rules and have licences where we need them.

To govern business relationships, we use appropriate legal agreements to establish secure professional boundaries. These include non-disclosure agreements (NDA) and service level agreements (SLA).

Security at the company level

Manyother Ltd places high priority on data protection and adherence to the Data Protection Act 1998, including the new General Data Protection Regulation (GDPR) implications that apply from May 25th 2018. Our data protection policy distinguishes between specific types of data and the procedures that must be followed in handling it. This lays the foundations for internal and external communications. All personnel are trained in distinguishing between data types and how to handle them appropriately. Documents of any kind, electronic or non-electronic, must be handled according to their sensitivity. Provision is made for secure data storage, both physical and electronic. Locks and passwords are mandatory and staff are trained in how to do this effectively.

Risk awareness training is provided to ensure personnel take due account of the consequences that can result from data loss. Risk management is considered a collective responsibility that all personnel must engage with. A culture of deliberate safe practice is promoted both within the organisation and with partner organisations. There is a clear reporting procedure for untoward incidence, actual or suspected.

Policies and procedures are reviewed bi-annually as a minimum, but there is a culture of continuous assessment. Whenever a risk is identified action will be taken as a priority.

Security at the server level

Our software systems are only hosted on secure servers at certified data centres. As our customer base is international and subject to different regulatory standards we operate to the standards relevant in each country. Generally, ISO27001 is the default standard.

Each instance of the PT system is mounted on a unique URL with its own SSL certificate. The servers are maintained and monitored 24/7/365 by an enterprise support team at the hosting provider under an Service Level Agreement. Dual off-site backup systems provide both whole server disaster recovery protection and individual file/database recovery.

Anti-virus and malware detection are in operation and updated every 24 hours. Server operating system and infra structure software updates and patches are checked daily.

Security at the application level

Our systems are built to meet user and login security requirements of ISO27001 (ie. timed logout after inactivity, failed login counting and IP / Account locking, password re-use prevention (to n previous), password length & complexity checking, 2 factor authentication).

Our position on privacy is simple, straightforward and pragmatic. If no personally identifiable data are captured, privacy is ensured. Our guiding principle to all of our users is NOT to capture client identifiable data. To this end the system provides automatic pseudonymisation to ensure records are not person identifiable. Client ID fields have built in warning messages to remind users to safeguard client identity.

Pragmatic Tracker has self-monitoring mechanisms that check for file changes and database integrity. There is built-in event monitoring that records all user activity and can’t be deleted or modified at the application level. All entries remain for the life of the database and are not overwritten after a set period. Alert mechanisms inform us immediately about suspicious activity.

Advanced encryption techniques are used in our database to protect client information.

Security at the user level

Recognising that human factors are typically the weakest link in any security system, we take a proactive approach to ensuring customers are made fully aware of matters that may affect data protection and security generally. This begins at the commissioning stage when we undertake an Implementation Survey that leads to a document detailing how the system will be configured to meet the customer's needs. This describes the nature of the information to be captured and how access to it will be structured, controlled and kept secure.

Product training and support is the next stage in assisting users to adopt safe and proper practices in the use of our system. This comes in two forms; direct one to one training of key personnel who will oversee and manage the system, and extensive help material, built into the software itself. In parts of the system there are pop-up messages that remind users of actions where care must be taken.

All users of Pragmatic Tracker agree to our 'Terms of Use' where we explicitly state how they are responsible for ensuring they do not write any material anywhere in client notes or session notes that could identify a client or anyone else involved with the client.

End of Document