Information Security Policy

V1.6 update November 2019
3 pages

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. We believe this offers the best means to maximise safety and promote security resilience.

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.

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 SLA (Service Level Agreement). 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. Firewall protection is managed through the enterprise support team who advise on server hardening. Server software patches and updates are applied as they become available.

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 via SMS or email). User passwords are stored in encrypted form in the database and the encryption algorithm uses a salted hash repeated 512 times (hash algorithm 'SHA512').

As a principle we strongly advocate customers and users do not record client identifiable information anywhere in the system. This is emphasised at both the commissioning and training stage. In areas where users may be prone to lapses, there are automatic warning messages about safeguarding patient identity.

Where client electronic contact details are collected, these are subject to a verification process to minimise data entry errors. Once confirmed the contact details are one-way encrypted and cannot subsequently be viewed. Client notes and textual data of any kind are stored in encrypted form using the Rijndael-128 algorithm and there is a hierarchical permissions structure to control user access.

In addition to protection at the server level, our application software includes self-monitoring routines that check for application file changes and database integrity. Log files and alert mechanisms are in place. There is built-in event monitoring that records all user login events (username, time, IP address) and all major operations performed by each user (creates, edits, deletes etc). These are all recorded in the main database 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.

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 aware of matters that may affect data protection and security. This begins at the commissioning stage when we undertake an Implementation Survey to determine the customers particular operational needs and security issues that may emerge from that. The system is highly configurable and capable of collecting a wide range of information. We scrutinise and advise the customer on the appropriateness of the data they are wanting to collect and the data protection implications that are relevant.

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. This help material is structured to be very easy to access and includes video tutorials. In parts of the system there are pop-up messages that remind users of actions where care must be taken.

End of Document