Version: 2.0

Maytech Security and Confidentiality Statement

January 2018
Author: Maytech

maytech
GLOBAL DATA TRANSFER

Maytech Security and Confidentiality Statement

maytech
GLOBAL DATA TRANSFER

Business and public service agencies worldwide rely on Maytech to share confidential data in mission critical workflows. This document outlines the Maytech security environment and confidentiality policy.

Physical Security
Maytech servers are located in secure areas at Tier 3 data centers in Europe, USA, Asia and Australia. The facilities benefit from strong physical and electronic security, uninterruptible power and fire suppressant systems.

Firewall
The Maytech networks are protected by a stateful packet inspection firewalls. All ports, other than those required for the provision of service are closed.

Operating Systems
Maytech's products run on Linux. Updates and security patches are applied daily.

Customer Access
Customer access to Maytech servers is restricted to the supported protocols, we do not offer access over SSH or telnet. All sessions are automatically terminated after fifteen minutes inactivity.

Confidentiality
Each customer account operates in a discrete filesystem or VPS. Each user is jailed to their home folder with no visibility outside unless specifically granted.

Data Tokenisation
Maytech services utilises tokenisation technology to protect critical business data and reduce associated data breach risks by storing data off-site and away from your network. Quatrix Vault® is built on split secret methodology that ensures no access to tokenised records even by the service provider.

End to end Encryption
Maytech offers secure data transfer with end-to-end encryption as standard. Data is encrypted in transit using HTTPS or SFTP and at rest using AES-256 bit encryption. All authentication records and other sensitive data are stored encrypted.

Quatrix® provides secure data transfer using HTTPS or PGP encrpytion. The browser-based PGP module is available in Quatrix and ensures you enjoy the highest level of encryption leverage.

The optional SFTP module on Quatrix provides secure data transfer using SFTP. The site administrator can disable unencrypted protocols, per login or sitewide.

DATA ON BOARD

Maytech Security and Confidentiality Statement

maytech
GLOBAL DATA TRANSFER

Password Policy

Maytech strong password policy improves data security by motivating users to create dependable, secure passwords and then store and utilize them properly. Therefore, customers passwords must meet complexity requirements. Complexity requirements are enforced when passwords are changed or created.

Multi-Factor Authentication

Maytech provide a second layer of security to customer online accounts - multi-factor authentication ("MFA"). Verifying customers identity using a second factor (via phone or other mobile device) prevents invalid logins even if the password is compromised.

Granular Permissions

Maytech products offer detailed control over access, visibility, file and folder permissions for each user.

Test and Support Access

Where support staff need to access customer accounts in response to customer trouble tickets, temporary access is granted by support management with a one-time authentication token. Access is limited to filesystem navigation and does not include rights to read or download files.

Data Persistence and Backups

Maytech provide a high-availability service with significant redundancy in all critical resources. Hourly snapshots (backups) are retained and available to customers to restore deleted or overwritten files for 28 days. We do not keep persistent backups of customer data, nor is data ever replicated outside the chosen data centre. Retired storage media are always destroyed onsite at the data centre.

Intrusion Detection

Maytech operate multiple systems to detect intrusion and block IPs attempting DoS attacks or unauthorized access.

Maytech systems are hardened against SQL injection scams with fully parameterized queries and test sites are regularly subjected to third-party pen testing.

Antivirus

All file uploads are scanned for malware on the server side and email alerts are sent to the account owner.

Compliance

Maytech sites will pass a PCI-DSS penetration test. All sites meet the requirements for a GDPR and HIPAA compliant workflow. Customers can download a full audit trail of file transfer activity.

Maytech's information security management system has ISO 27001 certification.