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, Hong Kong and Australasia and UAE. 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.

End to end Encryption

The optional Encryptions module on FTP-Stream provides secure data transfer using SFTP, HTTPS or FTPS. The site administrator can disable unencrypted protocols, per login or sitewide.

Push replication traffic is encrypted using the SFTP protocol.

Quatrix provides secure data transfer using HTTPS and SFTP. Optional PGP Encryption provides advanced security.

All authentication records and other sensitive data are stored encrypted. Customer data is encrypted at rest using the NSA approved AES algorithm with 256 bit key strength.

Password Policy

With the optional Extended Authentication module customers can set a password policy. Including: Users can / cannot change their passwords, must change their passwords on first login, must periodically change their passwords, must use strong passwords.

Government Procurement Service Supplier
DSS COMPLIANT
McAfee SECURE
HIPAA COMPLIANT

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.

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 center. Retired storage media are always destroyed onsite at the data center.

Intrusion Detection

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

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

Compliance

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

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