



FTP-Stream Security and Confidentiality Statement

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

Physical Security

Maytech servers are located in secure areas at Tier3 data centers in London, New York and Hong Kong. The buildings 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

FTP-Stream runs on Solaris 10 from Sun Oracle, widely accepted as the world's most secure operating system. Updates and security patches are applied daily.

Customer Access

Customer access to FTP-Stream servers is restricted to the supported FTP-Stream protocols, we do not offer access over SSH or telnet. All sessions are automatically terminated after five minutes inactivity.

Encryption

Customers login to the control panel over HTTPS, this traffic is therefore always encrypted.

The optional Encryptions module provides secure data transfer using SFTP, HTTPS or FTPS.

The site administrator can disable unencrypted protocols, per login or sitewide.

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.

Confidentiality

Each customer account operates in a discrete filesystem or VPS. Each login is jailed to their home folder with no visibility outside.

Granular Permissions

FTP-Stream offers 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 time-limited authentication token.

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 12 weeks. We do not keep persistent backups of customer data, nor is it ever replicated outside the chosen data center. Retired storage media are always destroyed onsite at the data center.

Compliance

An FTP-Stream site will pass a PCI-DSS penetration test. FTP-Stream sites meet the requirements for a HIPAA compliant workflow

Maytech Communications Ltd is, in preparation for an ISO 27001 (Information Security Management) audit.

Revised February 2011
<http://www.maytech.net/>