Version: 3.0

Maytech Security and Compliance Statement

April 2018
Author: Maytech

maytech
GLOBAL DATA TRANSFER

Business and public service agencies worldwide rely on Maytech to share confidential data in mission critical workflows. This document outlines Maytech's security and compliance environment.

Data Encryption, Storage, Retention, Backup and Restoration

In Transit: TLS with strict transport security. HTTPS and SFTP. There is also a unique user-friendly PGP encryption feature which offers advanced security for highly confidential data.

At Rest: Data is protected with AES-256 bit encryption.

Residency: Service can be provisioned at a data centre location of your choice ensuring compliance with local and international data regulations. On sign up, simply select a service hub from the option list and your data will be stored at that location. For details of available locations go to https://www.maytech.net/data-residency.html.

Data Retention: We do not keep persistent backups of customer data, nor is data ever replicated outside the chosen data centre.

Data Back up: Maytech services are backed up every hour on the hour locally at your chosen data centre.

Data Restoration:

- In FTP-Stream, we retain site backups called snapshots for 28 days. In snapshots you can explore the contents of each snap and restore any files or folders that may have been accidentally deleted or overwritten.
- In Quatrix®, deleted files can be restored from the Trash folder in your file explorer for up to 28 days, unless it is emptied manually before this period.

Authentication

- Username with strong password both of which are stored one way encrypted.
- Additionally we support enhanced authentication - two factor authentication for web access and SSH public key authentication for SFTP. Using SSH-key authentication for SFTP, the private key remains under customer control.

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 15 minutes inactivity.

Test and Support Access: Where support staff need to access customer accounts in response to customer support 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.

Information Confidentiality and Assurance

Central administrative controls over user provisioning and access rights and a full audit trail. Each user is jailed to their home folder with no visibility outside unless specifically granted.

Network Boundaries, Intrusion Detection and Security Testing

Firewall and Intrusion Detection: Maytech networks are protected by a stateful packet inspection firewalls. All ports, other than those required for the provision of service are closed. We operate intrusion detection (SNORT). An attempt to gain unauthorised access results in lockout of offending IP on the firewall.

Monitoring: Service is monitored by over 100 monitoring daemons continuously probing for fault conditions at levels ranging from basic hardware health to emulated file transactions. Ports are monitored for suspicious activity such as password scams or Dos attack.

Security Patching: Governed by ISMS OP 29 Security and Patching Policy, critical security patches are installed when they become available. A typical time window for non critical patch release is two working weeks of patches being released.

Virus Scanning: All files uploaded are scanned using ClamAV to inspect uploaded files.

Penetration Testing: Annual penetration tests are conducted by a CREST member company and a National Cyber Security Centre (NCSC) CHECK scheme "Green Light" subscriber authorised to conduct testing on government systems under the terms of the CHECK scheme[1].

Vulnerability Scanning: Daily vulnerability scanning and PCI-DSS conformance scanning using McAfee Secure.

Compliance

Maytech Information Security

Maytech's Information Security Management System (ISMS) is ISO 27001:2013 certified and audited twice yearly by Lloyd's Register Quality Assurance, one of the leading global business assurance providers.

Scope of Applicability: Information security relating to the design, development, support and provisioning of Maytech's Saas hosted service.

Statement of Applicability

There are 114 controls in 14 clauses and 35 control categories in ISO 27001: 2013. Our statement of applicability, available on request, details the controls specified in ISO 27001: 2013 and a cross reference to the document with the Information Security Management System which implements the requirements of each control.

1 The CHECK scheme is UK specific and enables penetration testing by National Cyber Security Centre (NCSC) approved companies, employing penetration testing personnel qualified to assess IT systems for HMG and other UK public sector bodies.

A.5: Information security policies (2 controls)
A.6: Organization of information security (7 controls)
A.7: Human resource security - 6 controls that are applied before, during, or after employment
A.8: Asset management (10 controls)
A.9: Access control (14 controls)
A.10: Cryptography (2 controls)
A.11: Physical and environmental security (15 controls)
A.12: Operations security (14 controls)
A.13: Communications security (7 controls)
A.14: System acquisition, development and maintenance (13 controls)
A.15: Supplier relationships (5 controls)
A.16: Information security incident management (7 controls)
A.17: Information security aspects of business continuity management (4 controls)
A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

SOC 1 and SOC 2 Compliance

Maytech do not offer SOC 1 or SOC 2 reports. Our information security management systems are instead ISO 27001 certified. The criteria / controls required by the two standards were developed to mitigate similar risks and there is considerable overlap in the criteria defined in the Trust Service Principles of SOC 2 and the controls defined in Annex A of ISO 27001.

Both standards provide independent assurance that the necessary controls are in place and whereas ISO 27001 is an international standard, SOC 2 is created and governed by the American Institute of Certified Public Accountants, AICPA.

Product Compliance

PCI-DSS: Your site will pass a PCI penetration test. As a PCI compliant hosting provider, we also run daily McAfee scanning for over 40,000 vulnerabilities and PCI specific vulnerabilities ensuring potential risks are identified in a timely manner. Our PCI SAQ (level D) together with Attestation of Compliance are available on request.

HIPAA: Our products are compliant with the Health Insurance Portability and Accountability Act (HIPAA) - a US legislation providing data privacy and security provisions for safeguarding medical information.

General Data Protection Regulation (GDPR): While Maytech does not view, use or access your data, if Personal Identifiable Information (PII) is to be stored on our systems we are classed as a Data Processor. Maytech provide a *Data Processing Agreement* which we will both sign to confirm that appropriate controls and systems are in place for the relevant data processing activities we undertake on your behalf. This demonstrates you have carried out your obligations under GDPR in relation to the secure storage and transfer of your sensitive PII data.

Pan Government Accredited: Services are Pan Government Accredited for Official Sensitive Data.