Security and Compliance Frequently Asked Questions

Version 2.0

September 2019

maytech
GLOBAL DATA TRANSFER

Contents

Maytech's products are supplied as a software as a service, with service being subject to our terms and conditions. Our Security and Compliance Statement outlines Maytech's security and compliance environment and should be read in conjunction with the following security FAQs.

Data Encryption, Storage, Retention & Backup

Identity & Access Management

Physical & Network Security

Compliance

Confidentiality & Privacy

Feel free to contact support@maytech.net if you couldn't find the answer to your question.

1 Data Encryption, Storage, Retention & Backup

	Encryption	
1	How is sensitive information that is transferred protected? Are all communication links within the Maytech's platform fully secure and using encryption or other secured techniques for information transmission? Who holds the encryption keys i.e. can Maytech access and decrypt the Customer data?	All sensitive data is stored encrypted. Customer data is encrypted at rest using the NSA approved AES algorithm with 256 bit key strength and in transit over HTTPS / SFTP or PGP. Maytech's mail servers are set to require TLS encrypted communication. None, we never access Customer data. Administration of production servers containing customer data is restricted to named individuals only. Access is restricted to SSH2 and locked to specific Maytech's IPs. Authentication is two factor - public key and Time Based one Time Password (TOTP). General support staff cannot access the Customer's Mutual data and are granted a one time read only access link to review account information at the request of the customer.
2	What cryptography protocols are used by web site and/or web services used in Maytech's platform? What are Maytech cryptographic infrastructure and standards used to secure data?	Transport Layer: TLS 1.2. Authentication and Key Exchange; ECDHE-RSA 256 bit (with forward secrecy) . Symmetric Algorithm: AES256bit in GCM Mode. Integrity Algorithms: SHA-256 (https://community.qualys.com/blogs/securitylabs/2014/09/09/sha1-deprecation-what-you-need-to-know).
3	Does the Customer control & own the encryption keys?	SSH-key authentication for SFTP is available.
4	How and where do you store encryption keys? (How do you ensure isolation of the keys from the data?)	Software keyring, keyring is stored on separate encrypted volume.
5	Are there any controls in place to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information?	All administrative access is encrypted (SSH with public key and 2FA authentication), customer access is encrypted (secure TLS or SSH), data at rest encrypted (AES-256), the LUKS container key is rotated quarterly.

6	At which layer do you terminate SSL (i.e. is internal data transmission encrypted by SSL as well)?	Load balancer with HTTPS communication to web servers.
7	Is data encrypted at-rest: 1. Database data? 2. Server disks? 3. SAN storage? 4. Backup data?	Database data, server disks, SAN storage and backup data are encrypted at rest with AES-256 bit encryption.
	Storage	
8	Where do Maytech store customer data?	Maytech store customer data at customers' chosen data centre and we never replicate it or back it up outside the chosen data centre.
9	How long do Maytech keep customer data?	Maytech retain customer data for 28 days after it is deleted. We do not keep persistent backups of customer data.
10	Can data be moved without prior agreement from the Customer?	No, data is never replicated outside the chosen data centre.
11	What are the locations from which services will be provided? / In which data centres or facilities the Customer's data will be stored or processed?	Maytech services can be provisioned at a data centre location of Customer's choice ensuring the compliance with local and international data regulations. Operating Data Centre hubs can be found on Maytech's Data Residency page. On sign up, a Customer selects a service hub from the option list. Data is never transferred or replicated outside the chosen hub.
12	Describe any specific dependencies on third party vendors for you to deliver the proposed contracted services, e.g. hosting, cloud services, development, etc.	We use third party data centres to deliver the hosting services. Take a look at the full list here. Where you require a data processing agreement for GDPR compliance, the relevant third party will be documented.

13	What are your security requirements for supplier relationships (data centres)?	Each data centre meets, or exceeds, Tier 3 data centre standards. Any supplier must, at a minimum be ISO 27001 compliant and Soc 1 and 2 compliant as applicable. Third party supplier compliance reports can be provided upon request.
14	Can you confirm that your data centre location(s) supports twin connection resilient Internet breakouts with guaranteed bandwidth?	Maytech data centre locations support twin connection resilient Internet breakouts with guaranteed bandwidth.
15	Does the solution provide high-availability and fault-tolerance that can recover from events within a data centre?	Maytech's platform is highly-available and a resilient web application and continues to function despite expected or unexpected failures of components in the system. If a single instance fails or an entire zone experiences a problem, Maytech's application remains fault tolerant—continuing to function and repairing itself automatically if necessary. Because stateful information isn't stored on any single instance, the loss of an instance—or even an entire zone—should not impact the Maytech platform's performance.
16	Describe the physical security controls in place at the locations where Customer's data (or those of its customers) will be stored or managed.	Maytech's data centres feature a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. The data centre floor features laser beam intrusion detection.
17	What procedures exist to ensure the data integrity of the Customer's information assets used in production systems?	The Customer's data on the Quatrix server is transient and not modified on our systems. Any integrity check required by the Customer should be performed at source and at destination.
18	Is data stored in a secure manner, accessible only to officers of their subsidiaries or their approved representatives?	Yes, the Customer controls data and service access policy.
19	Is it possible to request a bespoke retention period?	Yes, it is possible to request a bespoke retention period upon Customer's request.

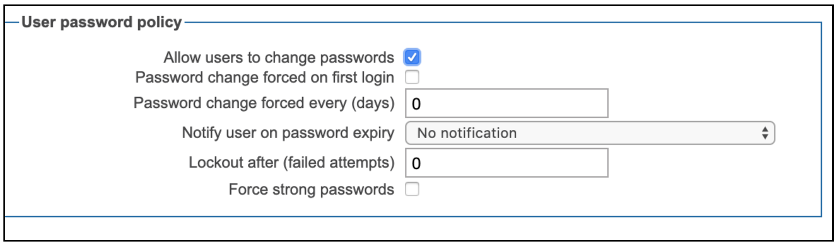
20	Do you offer any data server redundancy?	Live streaming mirror to a second data centre with one hour migration time in the event of a major disaster - an additional cost is 60% of the primary quote. Offsite backup with 48 hours restore to the original or new data centre - additional cost is 25% of the primary quote.
21	Describe any cases where Customer's data will be shared with, or made accessible to, third-party providers.	We never share Customer's data with third parties.
22	What is your process for notifying customers of data breaches?	On identification of any breach we would inform the Customer within an hour or as soon as it is practicable.
	Retention & Backup	
23	How often do you back up customer data?	Maytech back up customer data every hour locally at the chosen data centre.
24	What is the data backup methodology and schedule?	Maytech's approach to data backup is governed by ISMS OP 31 - Data Backup Policy. Maytech utilise our cloud offering to act as our primary backup solution for all of Maytech's critical data. Backups are performed according to the nature of the data as follows: Client Data: • All data is backed up using Solaris ZFS from the primary data centre node to the secondary node. • Clients can opt to replicate the data between global hubs as an added resilience measure if they so wish but this will not be performed by default.
25	Will Customer's backed-up data be stored on shared media (such as tape) alongside the data of other customers?	Yes.
26	Are backup tapes sent to an offsite storage facility?	By default we do not backup offsite, we backup to a SAN within the data centre. Backups on the SAN are encrypted at rest and in transit.

27	Can we restore deleted data?	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.

2 Identity & Access Management

1	Does the solution support Single Sign-On integration?	Yes, Maytech support Single Sign-On and ADFS integrations. Maytech's customers can sign in to their accounts using their existing corporate Active Directory credentials or any other identity provider (i.e. Duo, Okta, OneLogin, etc.).
2	Does the solution distinguish user roles and admin roles within the application?	FTP-Stream: All users except admin are jailed to their home folders and cannot see files or folders outside. To exchange confidential files with customers give each login a distinct home folder. Account owners can add new secondary admins who can help to manage FTP-Stream account and Billing admin, who helps with payments and invoices. In Quatrix there are several user roles that determine what actions can be performed in the account. The account owner is the top administrator of the account that has access to all Quatrix features and can purchase more users for the account. Admin has the same rights as the account owner with the exception of tracking and paying invoices for the account. Pro users can browse folders and share to any of your users or to their contacts who don't need a licence to download (normally your employees). Associate users can only use your service to share files back to your Pro Users - great for external partners who need to regularly feed data into your organisation. Jailed users are jailed to the Projects Shared With Me folder. They are not able to use the Share Form or otherwise share files outside of the designated workflow. Read more about Roles and permissions.
3	How are user passwords stored in the system?	Passwords are individually salted and stored in a database, encrypted one way.

4	Does your organisation have a documented password policy? If YES, describe the controls (e.g. minimum length, complexity, expiration period).	Yes. ISMS OP 30 - Password Management Policy: The following are general recommendations for creating a Strong Password. A Strong Password should: • Be at least 8 characters in length • Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z) • Have at least one numeric character (e.g. 0-9) • Have at least one special character (e.g. ~!@#$%^&*()_-+=) A Strong Password should not: • Spell a word or series of words that can be found in a standard dictionary • Spell a word with a number added to the beginning and the end • Be based on any personal information such as user id, family name, pet, birthday, etc. With the optional Extended Authentication module, customers can set a password policy, including: Users can / cannot change their passwords, must change their passwords on the first login, must periodically change their passwords, must use strong passwords.

5	Can we request a custom password policy to be applied to Customer users?	Yes, the administrator of FTP-Stream account can set a password policy for his/her account to specify complexity requirements and rotation periods for his users' passwords. It provides a possibility to allow users change their passwords, to set a number of failed login attempts, to set the minimum password length, to force password change on the first login or after a specified period and to specify password construction requirements. The following options are available for configuring the password policy:  **User password policy** Allow users to change passwords ☑ Password change forced on first login □ Password change forced every (days) 0 Notify user on password expiry No notification Lockout after (failed attempts) 0 Force strong passwords □ Quatrix supports strong passwords.

<table>
<tr>
<td>6</td>
<td>What is the password reset process?</td>
<td>There are several ways of changing the password in FTP-Stream and Quatrix:
<table>
<tr><th>Admin</th><th>User</th><th>Backoffice Admin</th></tr>
<tr><td>resets his own password;
sends password reset links to his users</td><td>changes his own password.</td><td>resets password upon customer's request.</td></tr>
</table>
The user or admin can change their password on the Login page. Follow these steps:
1. Go to the Login page of your account and click the Forgot password link.
2. Enter your email to get instructions on how to reset your password.
3. Click the Password reset button in the email.
• Password reset link is valid for 24 hours after the first request. All further requests use the same link.
• After 24 hours the link is invalidated and a user has to generate a new link.
1. The Reset password page opens where you should type in and confirm your new password.
2. You can log in to your account with the new password.</td>
</tr>
</table>

7	Does the solution support multi-factor authentication?	Yes, all Maytech's file sharing products offer Two-Factor Authentication (2FA) as an additional module. Administrators can elect to have their 2FA codes sent in one of two ways: 1. Download and install the Google Authenticator, Duo Mobile, Authy, or Windows Phone Authenticator app for your phone or tablet. An installed app implements TOTP security tokens from RFC 6238 in a mobile app. It provides a 6 digit one-time password which users must enter alongside their user name and password every time they log in to their account. 2. SMS During account login an SMS is sent to the user's designated phone number with a one-time use code which is 6 digits long. This code must be entered as well as the user name and password during login.
8	Do Maytech provide audit and monitoring of access to the system and data?	Yes. Comprehensive audits logs are available and all user activity is tracked.
9	How does the solution authenticate users to prevent unauthorized access?	Username and strong password, and 2FA.
10	Within the application, and the supporting infrastructure, describe how administrator actions are logged and recorded, including details of how long these audit logs are stored for.	Where Maytech are instructed to access any data (regardless of whether it is personal data or otherwise), all such access is logged with information identifying the Maytech's personnel accessing the data and setting out the date and time of access. Access logs are maintained for 12 months and can be downloaded and stored by the Customer at that time.

11	What is your review processes, manual or automated, for event and application logs generated within the solution?	Maytech's approach to log management is controlled by ISMS OP 22 - Logging and Audit Trails Policy. Maytech conduct an ongoing collection and retention of a record of user activities on or with Maytech, including: • Log-in attempts. • Password changes. • File creations, changes and/or deletions. All audit entries are time-stamped with entries recorded as GMT dates and times. Clock synchronisation is uniform on all servers to ensure timestamps are consistent across all logs to avoid any time discrepancies which may cause issues for any subsequent forensic activities. All logs are reviewed periodically (minimum at least monthly) to identify any unauthorized access to the systems. Retention of audit files is for at least 12 months.
12	If required, what methods and formats are available for a Customer to export a copy of data?	The account owner has access to all the data, so can take a copy of it at any time.

3 Physical & Netwok Security

1	Does Maytech's platform have adequate hardware/software monitoring that is in place to ensure issues compromising system performance, availability, integrity or security are alerted for remedial action? What proactive/protective monitoring tools, processes and audits (i.e. details of security/ system health checks, penetration tests, scanning, audit and control of key architectural components etc.) are used?	Maytech's services are very extensively monitored, we have more than 125 checks in place. These include low level system health such as: • Weekly vulnerability tests (McAfee) • Weekly PCI conformance tests (McAfee) • Network conditions • Load • Database response times • Storage IO performance And high-level tests – for example: • Can a test user login • Time to authenticate • Time to get file listing • File transactions – upload, download, rename, delete.
2	What kind of alerting for the monitoring is available: SMS, email, etc?	Our systems are extensively monitored alerting our NOC on a range of conditions, but this is not a service we share with customers.
3	How do you monitor the security of your infrastructure?	Firewalls, weekly external vulnerability scanning (McAfee) daily internal vulnerability scanning (Vuls) and Annual Penetration Testing.
4	Detail any DDoS protection in place for the service.	Maytech's platform is protected by a suitable firewall infrastructure with Intrusion Detection System /Intrusion Protection System, DOS/DDoS protection, antivirus filtering, access control and auditing. The service is monitored by over 125 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 DDoS attack.

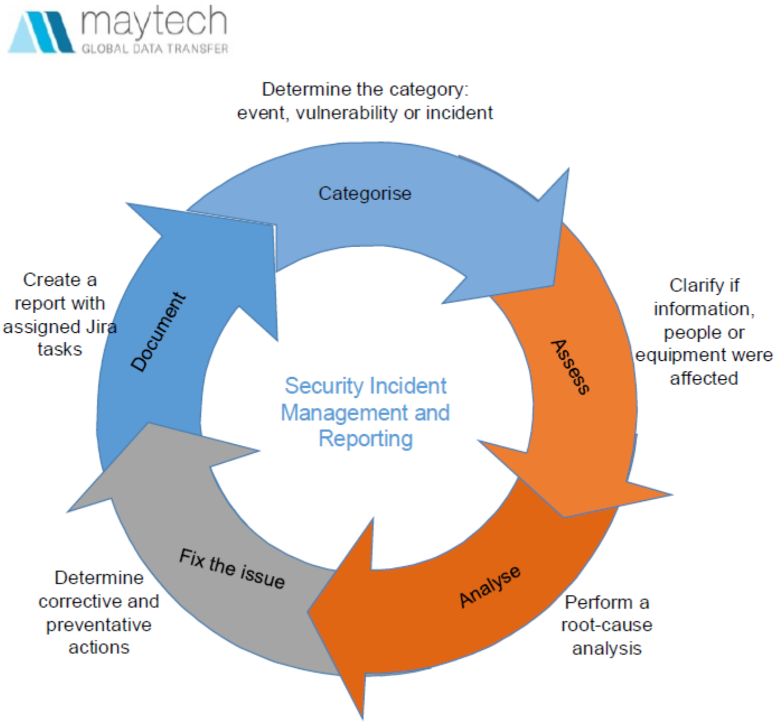
5	What boundary protection architecture and governance regarding protective monitoring is used? Is Maytech's platform protected by a suitable firewall infrastructure with Intrusion Detection System /Intrusion Protection System, DOS/DDoS protection, antivirus filtering, access control and auditing?	The Maytech's 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 a lockout of offending IP on the firewall.
6	Are Intrusion Detection Systems (IDS) installed either on network or hosts? If yes, describe the solution used and the management/monitoring process.	Maytech have comprehensive IDPS systems that scan traffic for and recognises intrusion attempts and automatically blocks offending IPs on the firewall.
7	Does your Internet gateway provide website filtering to block compromised sites and provide malware protection?	Yes.
8	Does Maytech's platform have any performance constraints and maximum loading for the system?	Maytech's platform is a cloud service that handles hundreds of requests per second. Server load is constantly monitored at our NOC. It is our policy to ensure no part of the system is loaded above specified industry standard trigger points. Our systems are architected for seamless scaling.
9	Do Maytech have any system hardening policies and controls in place?	System hardening is governed by ISMS OP 11 - Systems Security and Network Management Policy and tightens system security by limiting the number of users, setting password policies, and creating access control lists. Unnecessary services are disabled to make the system more secure and to provide better performance. All ports, other than those required for the provision of service are closed.
10	Are there any patch management policies and controls in place?	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. Patch installation failures are monitored.

11	Does Maytech's platform components have active anti-virus installed and maintained? What anti-virus and/or anti-malware controls are in place?	We may provide virus checking, content filtering (spam control) and other similar supplementary services in connection with, or as part of, the services. We will use our best endeavours to provide these supplementary services with reasonable skill and care but we give no other warranty in regard to these supplementary services and, in particular, we do not guarantee that they will be totally effective. It is essential for the protection of your data and systems that you install and routinely maintain your own virus checking and other security services and that you regard the protection available from us as no more than the first line of defence. All files uploaded are scanned using ClamAV to inspect uploaded files.
12	What antivirus software is installed on both servers and workstations? What are scanning and signature update schedules?	Maytech do not use any Microsoft products in production, as such our production systems are not susceptible to Windows malware. We do offer a virus scan service which uses ClamAV to inspect uploaded files. All staff PCs run McAfee antivirus.
13	Is the application/solution subject to regular third-party penetration testing? How frequently such tests take place?	The service is subjected to an annual IT Security Health Check (ITSHC) by a CHECK / CREST approved vendor and a management report and residual risk statement are available for all interested parties upon request and a signed NDA. 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 Her Majesty's Government and other UK public sector bodies. Vulnerability scanning: Daily scanning for over 40,000 vulnerabilities and weekly PCI scanning using McAfee, an Approved Scanning Vendor (ASV).
14	Which company, or companies, is used for penetration testing?	Maytech alternative third party security companies on a regular basis. Please contact us for specific details for a current year.

4 Compliance

1	Do you have any relevant certifications in relation to Information Security Standards that are held by your organisation (such as ISO 27001, PCI DSS, etc.)?	Yes. Maytech's Information Security Management Systems are ISO 27001 certified. Our certificate number is 10009780 and the certificate is available on request. Maytech's products are PCI-DSS compliant and our annual PCI-DSS SAQ (level D) and Attestation of Compliance are available on request. Maytech's services are also GDPR and HIPAA compliant.
2	Have your information security controls been assessed by an external auditor or certification body?	Yes. Maytech are audited twice a year by Lloyd's Register Quality Assurance — one of the leading business assurance providers in the world.
3	Can you fully disclose the scope under which Information Security was achieved?	Scope of Applicability: Information Security relating to the design, development, support and provisioning of Maytech's SaaS hosted services. Statement of applicability can be provided upon Customer's request.
4	Do you have the independently conducted third-party security control assessment, such as SOC 2/SOC 1 reports?	Yes, for data centres. Maytech do not have a SOC 2 report. Our information security management systems are instead ISO 27001 certified, and audited twice a year by Lloyd's Register Quality Assurance, one of the leading global business assurance providers. 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 with its origin in a British standard, SOC 2 is created and governed by the American Institute of Certified Public Accountants, AICPA.

5	Is your service suitable for Government data?	Maytech's government service and associated infrastructure is dedicated to public sector customers and is accessible from the internet. It is suitable for UK public sector customers with data sensitivity levels up to OFFICIAL and including OFFICIAL SENSITIVE. These categories represent up to 85% of data created or processed by the UK public sector. Maytech is a registered G-CLoud supplier (Service ID no: 110486484775596) and further information can be found on UK government Digital Marketplace.
6	When were written security policies last updated?	Policies are reviewed during monthly ISMS mgmt meetings and updated regularly, as necessitated or identified within review / training, as part of Maytech's Continual Improvement program.
7	Do you have a documented information security policy or program? If YES, what is covered by written information security policies?	Yes ISMS 01. This document provides a policy and framework of the main requirements of ISO 27001 that Maytech adheres to, in order to ensure that the company remains compliant. Our ISMS documentation includes regulatory obligations, all potential risk factors, policy & procedures, internal checking methods, recording, analysis and review which determines a proposed action.

8	Do you have any incident response programs in place?	All reports of information security weaknesses/incidents or events relating to any of Maytech's information assets are within the scope of:  maytech GLOBAL DATA TRANSFER Determine the category: event, vulnerability or incident Categorise Clarify if information, people or equipment were affected Assess Security Incident Management and Reporting Analyse Perform a root-cause analysis Fix the issue Determine corrective and preventative actions Document Create a report with assigned Jira tasks If the incident results in unauthorised access to customer data we will inform the Customer within one hour on what actions have been taken and what controls are put into place to prevent any repeat incidents. Users are not allowed to continue working after identifying a possible weakness/incident or information security event which affects their activities.
9	Are your information security controls regularly assessed by an internal audit team? If so, please describe and provide their findings.	Yes, we conduct thorough internal audits which cover core aspects of the ISMS throughout the year. Results available on request.

5 Confidentiality & Privacy

1	How do Maytech ensure my privacy?	Maytech are committed to protecting the privacy and security of your personal information. The Privacy Notice describes how we collect and use personal information about you in accordance with data protection law.
2	How long do Maytech keep customer data?	Maytech retain customer data for 28 days after it is deleted. We do not keep persistent backups of customer data.
3	Do you store or process any personal information?	Maytech offer secure, compliant, simple cloud file sharing and data storage of Customer's electronic files. Customers at all times are in control of their data. Further details can be found on Maytech's Guide to GDPR Compliant File Sharing page.
4	Does data belong to the Customer at all times?	Yes.
5	Do Maytech have a disciplinary policy or corrective action procedures in place for addressing data privacy violations?	Yes, ISMS OP 33 Disciplinary policy. Maytech believe that the fairest way to resolve issues with staff conduct or performance is to have a well structured disciplinary procedure.