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.