MARCH 2018

SECURITY OVERVIEW

MaxContact

SECURITY OVERVIEW

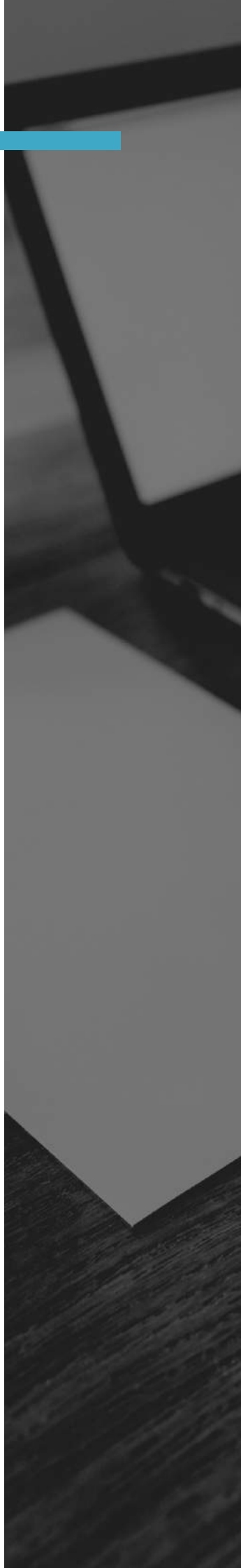
"Security is at the forefront of everything we do. MaxContact understand that software, infrastructure, people and processes all have to be in-line in order to achieve the highest level of security standards; therefore, you can be sure your data is in safe hands."

Ben Booth - Operations Director

PRODUCT

MaxContact always takes a security first approach when designing and developing our software. We have implemented industry standard development practices, coupled with multi layer architecture security, This is why we are one of the most trusted suppliers to industries regulated by OFCOM, FCA, PCI-DSS and GDPR.

- We use SSL only (HTTPS, TLS 1.3). This means your data is protected over the internet using encryption.
- We regularly review our data security.
- We use tokens for authentication.
- Our software is designed with security at every level.
- You cannot use any API, or page, without prior authentication (login).
- We secure the data, so that individuals only see what they are allowed to inside the API layers.
- We use database injections to make sure that every request that goes near the database is secure from SQL Injection attacks.
- Code reviews are completed before every software release.
- data is encrypted at every level (at least AES 256 bit)
- We use a reduce risk surface area approach at every level of the product and infrastructure



INTERNAL POLICIES

We know people are the number one reason for data breaches.

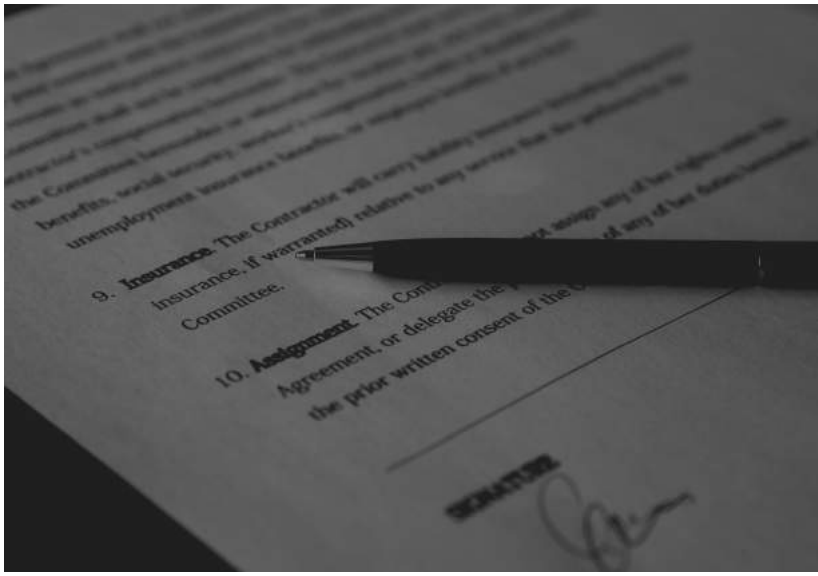
We have very strict internal information security policies and procedures in place to control, restrict and monitor data access. These include:

- Restricted access to servers
- Additional restricted access to databases
- Individual user account access
- Logging and auditing of all data access
- Screen recording of data access
- Elevated permissions only when required

We carry out regular reviews of compliance procedures and policies alongside training courses for staff, with regular refreshers.

No data is stored on site, instead it is all stored in our Microsoft AZURE hosted infrastructure. This partnership lends itself to the policies and ethos of our company. We believe that restriction of access to data is the best course of action for reducing breaches.

All data communication within the company is done compliantly. We use audited storage in conjunction with automatic clear down procedures, to remove human error as an element.



OUR GOALS

- Reduce the surface area of risk i.e. Remove access if it's not required
- All access is logged and audited
- Staff awareness of regulatory and internal policies and procedures
- Director level understanding of security importance
- Utilising technology to remove the element of human error
- Advanced alerting of data access anomalies
- Security is at the forefront of everything we do

INFRASTRUCTURE

HOSTING

Our Microsoft AZURE hosted platform gives enterprise level compliance and security as standard. With encrypted storage, and dedicated, audited storage areas for each client, all data stored is secured and audited.

SECURITY.
COMPLIANCE.
RESILIENCE.

DATABASE

Databases are where the data is stored, so it goes without saying that the security surrounding the databases needs to reflect this.

All customer databases are individual per client, so data leakage is not possible. Each database has its own unique encryption to AES 256 standard. Database backups go to a secure, encrypted location, and each database has its own unique encryption key where access is audited and logged.

Database access is restricted to senior staff only, with the exception of escalated privilege request access, which is time sensitive and expires. This supports our ethos that not having access in the first place infinitely reduces the risk of data breaches.

.

- Data encryption
- Data replication is only conducted within our own infrastructure, and uses encrypted streams to transfer data into a secure backup databases for DR
- No shared databases
- Unique certificates and password policies for every database
- Restricted access with full auditing
- Patch update policies
- AZURE IaaS
- IP Whitelisting