



We know that security is paramount to our clients — and we've made it our highest priority at CommuniGator to ensure your data is safe around the clock. We devote significant resources to continuously develop our world-class email marketing software for both hosted solutions and on-premise.



Data Center

Our data centre provides 24-hour physical security, redundant electrical generators, redundant data center air conditioners and other back-up equipment designed to keep servers continually up and running. We leave the data center management and security to the experts by working closely with our strategic partner who understand and appreciate the demands of our business. The redundant data center guarantees our customers security, reliability and performance.

- 24/7 management
- Climate-controlled environment
- Locked down environment
- Redundant power supplies
- Resilient WAN connection
- Flexible bandwidth

Data Security

We ensure that your data is kept safe from corruption and that access to it is suitably controlled through our internal security procedures.

- company security policy and procedure
- Data is mirrored and backed up off site
- Private information like passwords all encrypted - 128 bit
- Lose your password it cannot be retrieved, needs to be reset
- Each customer has separate and locked down database, there is no sharing of data in single database
- Never sell, rent or share your personal information on yourselves or your customers with third parties for their promotional use.

Application Security

We host in a secure server environment that uses full hardware firewalling with packet-inspection, virus guard and other advanced technology to prevent interference or access from outside intruders. All our clients are set up with a secure environment that is monitored 24/7 by our strategic managed service partner. The environment is then continually validated in terms of its security by our internal security team and also periodically by a third party penetration team.

- Virtual environment run on VMWARE platform for enhanced resilience
- Load balancing
- secure web development team strategy
- Intrusion detection and prevention
- Periodic penetration tests
- Double firewall for best practice
- Virus protection and managed internet security updates
- Separation of services through web, application, database, delivery, integration and web service servers for total security

Reliability and Backup

All networking components, load balancers, Web servers, and application servers are configured in a redundant configuration. Our fileservers use RAID technology to minimise the risk of file loss. In addition, all data is backed up on a daily rotation to our off-site backup servers.

- Redundancy
- RAID technology
- Daily off site backups

Email Delivery

The email delivery technology we use is supplied by our partner Port25 and is called PowerMTA. PowerMTA is the market's leading email gateway software that makes it easy for senders to adopt the latest authentication specifications (SenderID, SPF, Domain Keys and DKIM) and comply with policies for accountable outbound email delivery. The first MTA solution certified and approved by Goodmail Systems, PowerMTA includes support for Goodmail CertifiedEmail on Windows operating systems. Our choice of PowerMTA comes down to its scalability, delivery speed, best practice in email marketing, intelligent bounce back, complaint management and back off services.

For best deliverability and ownership we encourage all our customers to use their own domain or sub domain for their email marketing.

- Reverse DNS
- SenderID, SPF, Domain Keys, DKIM
- Email delivery software is certified and approved by Goodmail Systems
- Complaint management
- Bounce back management
- Clever ISP back off detection

Customer Integrated Solutions

Any onsite integrated customer applications such as a customer's CRM pass data through encrypted secure web service methods using the secure TRIPLE DES algorithm. Our web application never talks to a customer application, the customer application is forced to request data itself as the most secure method.

The application allows the customer to choose the data that 3rd party applications can send for their email marketing.

- Triple DES encrypted web services
- One way 3rd party communication
- Customer defines shared data

Employees

We take care to reinforce the importance of our services security and privacy among our employees. Our employees are trained and required to safeguard your information and we therefore restrict access to key employees through our intense security procedures.

End of Customer Contract

In the unlikely event that our customers end their contract, we will immediately remove the service availability and physically delete all customer data. All required data such as opt outs and undeliverables are sent back to our customers for their own use.