eMarketeer
Information Security Policy

Version	Date
1.1	2018-05-03

eMarketeer Information Security Policy

eMarketeer AB hereafter called “eMarketeer” is a leading actor within the development of SaaS-service (software as a service) hereafter called “the Service” within e-marketing. eMarketeer provides tools to automate the distribution of information, response and follow-up processes to optimize customer communication and customer service.

Personnel Security
Responsibility and roles of relevant personnel, both staff and contracted is described. A background check of all candidates for positions in eMarketeer is conducted in accordance with relevant laws as well as regulatory and business requirements. A competence plan is in place to ensure the necessary knowledge and awareness regarding security and vulnerabilities among the employees.

NDAs are signed by all employees, temporary staff, contractors or others who may become aware of information that needs protection.

Physical and Environmental Security
Areas that contain information and communication equipment and information requiring protection are secure. Secure areas are protected by appropriate entry controls to ensure that only authorized personnel to has access. Secure areas are properly secured against environmental damage caused by fire, water, dust, and similar influences.

Encryption
eMarketeer uses internationally recognized cryptographic methods to protect information stored on our site.

Access Control
Only authorized personnel are given access to eMarketeers systems based on work responsibilities. All system and system access should - as a minimum - be authenticated using personal user identities and passwords. All users must have unique user identities and passwords. Two-factor authentication is enforced on all critical systems.

To prevent unauthorized access and/or use of the Service, eMarketeer uses secure login via HTTPS (Hypertext Transfer Protocol Secure), a protocol for encrypted transport of data via the HTTP protocol as well as personal user credentials and acceptance of end user license agreement for all users.

Access to all information systems shall be authorized, based on the "need to know" principle and regulated by the position or role of the individual.

Secure Development
eMarketeer applies a Security by Design – principle. All application code is developed with an end-to-end focus on security. New versions are tested by dedicated test personnel and subject to extensive external testing (beta-tests). Different tests are performed: feature-, integration-, performance- and load/stress-tests. Both automated- and manual testing is applied.

The systems being developed for eMarketeer have clear security requirements, including the validation of data, security of code before production setting, and any use of cryptography. Structured methods like agile, scrum, etc. are used to control all parts of the development process.

All changes in the production environment follow current procedures. Dedicated test and development environments are used to test all changes, such as bug fixes and new releases before deployment to production. Independent test personnel regularly test new functionality.

All software is tested and formally accepted by an internal owner and the operator before the software is transferred to the production environment.

Before putting any new changes into production, a code review, threat & risk assessment, and a security code review are performed. If no security issues are discovered the functionality is implemented into the existing eMarketeer application. Penetration tests are also systematically performed and documented.

eMarketeer is using an independent security advisor - Watchcom AS, with the goal of developing secure applications and services. Watchcom assists eMarketeer with security assessments, application security testing, penetration testing, and consultancy.

Security measures in eMarketeer applications

Hosting

eMarketeer uses AWS for all storage and processing of data.

Encryption

Different security measures are used to protect our customers' personal information both when it is accessed by the customer and when stored on AWS. These measures include the use of encrypted communication between our servers and any clients accessing our site using Secure Socket Layer (SSL).

Personnel Security

Access to eMarketeer office and facilities is controlled using an access control system within the building.
Personnel responsible for system administration, such as designers, developers, and system administrators are checked for qualifications. This is done through interviews, tests, and verification of references. Personnel is provided appropriate training to ensure that they are highly qualified to fulfill their job responsibilities.

Physical and Environmental Security

All data are stored on secured servers located in AWS centers in Europe. See https://aws.amazon.com/security/ for more information.

Application Security

Cookies

Cookies are used to store information on user hard disk and contains information about your web browser version, Internet IP address, Operating System, language and similar technical information. eMarketeer will not work without user acceptance of the use of cookies.

Operational Procedures and Responsibilities

Scheduled outage is notified at least 24 hours in advance. System status and any scheduled downtime are presented at http://status.emarketeer.com/

The service capacities and performance are continuously monitored to foresee the need for upgrades of servers and infrastructure. The upgrade and patch management policy (schedule) is minimizing operational impact on the customers. Patches of system critical issues are done as soon as possible.

Service availability
eMarketeer has the goal of keeping the application service up and running “24x7x365”. However, system maintenance might lead to short periods of unavailability. System maintenance is performed on a regular basis to provide our customers with the best performance, security, and stability. The maintenance schedule is aiming to minimize disruption to normal business hours’ operation.

Currently, eMarketeer is using the following maintenance schedule (all times are CET +1):

· **System Maintenance**: Operating system patching, updates, reconfiguration of software to backend systems. This is scheduled for every second week on Fridays between 00:00 and 06:00.

· **Emergency patching**: «Emergency patching» might also occur. I.e. serious security updates, etc.
These updates are normally installed after normal working hours, approx. 18:00.

Downtime for the individual customer will vary depending on the type of change/update. Normally a user will experience a short loss of connection (a few seconds) and thereafter an automatic login will normally take place. Downtime will rarely exceed 30 minutes.
All scheduled maintenance is clearly posted on the login screen of each user at least 24 hours in advance. Critical fixes may be posted on the login screen of each user with minimum 24 hours’ notice if required to
maintain service stability.

Backup
All data have a 30 days “point in time” backup. This means that a Restore can be made from any specific date/time within the last 30 days. In addition, a monthly backup is taken and stored for 12 months.

Access Control to services provided by eMarketeer

Any unauthorized access to the eMarketeer site is automatically blocked by a firewall. Secure Socket Layer (SSL) encryption and user authentication protects information and ensures that only users within the customer’s organization can access data.

Access to personal information

Users can at any time login in with their username/password on our site, access personal information and update contact details.

Access to data stored in eMarketeer applications
Users can be created with different access levels within the account. It is Customer's responsibility to choose the appropriate level of access for each user and to protect information internally.

User Access Management
User access is managed by the Customer. The Customer is responsible for assigning the appropriate rights to individual users. User authentication is done through a username/password combination. The Customer can create users with different access levels (according to the role/right system)

There is no central password policy enforced by eMarketeer. The customer should set their own password policy according to the company password policy. The user/Customer is responsible for keeping the username/password safe.

Termination
The Customer is responsible for overall user management including removing users. When the agreement between the Customer and eMarketeer is terminated/expired, the access to the application is closed. The customer can require all data to be exported in a generic format. Referred also in the chapter below regarding Deactivation / Exit.

Business Continuity Management
eMarketeer has established a disaster recovery plan. The production environment is set up with redundancy to provide high availability in the case of failures and to be able to handle high peaks of traffic to our site.

Deactivation / Exit

When the Customer's subscription to eMarketeer services is terminated or expire, the account will be deactivated and no longer accessible. After 30 days, all data belonging to the Customer will be removed from eMarketeer servers and data center facilities. Backups remain available according to backup procedures.

Contact Info

Please feel free to direct any questions and comments regarding this security policy of eMarketeer to our Data Protection Officer on email privacy@emarketeer.com.