

# Security Technical File

Emailvision takes charge of all of the hosting, exploitation and security of the campaigns that are managed using campaign commander™ in ASP mode.

**Ensuring that customers' data is fully protected, and that access to that data is also secure, is an absolute priority for the Emailvision teams.**

The infrastructure used, called Interactive Mail Centre™, is the very best in the field, and was designed by experts on the basis of the best technologies currently available, adapted to the specific needs of Emailvision.

**This architecture, which is constantly being tested and reinforced, forms part of a global security policy covering:**

- data exchange
- access to data
- security policy and procedures
- physical safety
- Hardware infrastructure
- back-ups

## Data exchange

Emailvision uses various data transfer methods, and makes recommendations for each one in order to reinforce security. The data, of course, remains the exclusive property of Emailvision's customers, and Emailvision undertakes not to authorise any access to it by third parties.

### Real time

Data sent to Emailvision servers by means of secure forms (SSL 128 bits web form submission). Data transfer via a secure Internet protocol (HTTPS). This method is strongly recommended by Emailvision in order to guarantee the secure integration of data into campaign commander™.

### Web

Transfer protocol via FTP or FTPs, providing that the PGP encryption technology is used, along with certain sizes and types of key.

### Virtual Private Network (VPN):

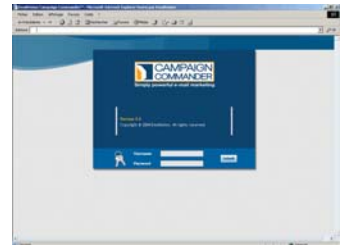
For a permanent secure link, a virtual private network can be set up to protect Internet-based exchange channels.

### e-mail

Transfer of data via e-mail, by encrypting the messages and attachments by PGP technology. Under certain conditions, attachments that are password-protected may be sent, providing that the password is communicated by telephone to prevent any e-mail communication being intercepted.

### Off-Line

Data processing using any kind of medium: CD-ROM, ZIP disks or floppy disks. Files to be protected by a password, to be communicated over the telephone.



## Access to data

### SSL

Access to the campaign commander™ application via a 128-bit secure site.

### encrypted LAN

Exchanges between the campaign commander™ platform and the databases using an encrypted LAN network and several firewalls.

### Password

Strong authentication for all requests for access to campaign commander™ and to databases.

### Blocking

Predictive functions that block passwords after a certain number of incorrect entries.

### Authentication

Customer data only accessible via the campaign commander™ solution. Access rights management using User ID and password, and for each user, the access rights defined according to profile. Each campaign commander™ account exclusively accessible to a restricted list of users.

### Firewall protection

Combination of various firewall technologies to isolate and protect the systems. Customer data protected by a dual independent firewall technology.

### Data preparation

Data preparation work carried out off-line. Data migration for campaign launches using secure VPN tunnels.

## Security policy and procedures

Data hosted by Emailvision within the European Community. Use governed and protected by European laws.

All Emailvision employees sign a charter that sets out the rules for using workstations and Internet, and for internal and external data protection and confidentiality.

Monthly validation and revision of security policies and the protective measures, carried out by the Emailvision Senior Management.

## Physical safety

The equipment used by Emailvision services is housed in high security DataCenters which comply with the most stringent safety and redundancy standards:

- 24X7 CCTV and infrared surveillance
- Physical isolation of hardware systems (locked up and alarm-protected)
- 24X7 Supervision
- Clean room with restricted and controlled access
- Complete UPS support
- Power supply redundancies for the servers
- Emergency diesel electricity generator
- Supervision of electrical supply for each server
- Environmental control: air conditioning and fire detection

## Infrastructure

Redundant architecture for all the systems including the databases, the firewalls, the tracking systems and the application servers.

## Back-ups

Daily back-ups of customer data (campaign history, user profiles and messages) within the Interactive Mail Centre™. Archiving of backups each week on DAT tapes and monthly on CD-ROMs stored in a protected external site.



In addition to the tests carried out by its own security teams, each year Emailvision calls for an external audit of its security architecture, in order to ensure that its security levels remain above the standards of the market. This audit involves a whole series of security, intrusion and reliability tests. Emailvision is regularly subjected to security audits requested by its customers, and passes them with flying colours.

## Barnes & Richardson S.A./N.V.

An Emailvision Company

42 Chaussée de Lasne -1330 Rixensart, Belgium

Tel. +32 (0)2 656 05 97 - Fax +32 (0)2 344 20 86

[www.emailvision.be](http://www.emailvision.be)