Radar data security and disaster recovery policies

Radar data security and disaster recovery policies

Security

Introduction
At Radar we understand how valuable your data is and how imperative it is to protect that data for you. Data is our stock in trade and we never underestimate its power or importance.

Data Processing
Radar utilises a managed service in a purpose built data centre for all sensitive data processing.

Our services are managed by Dudobi.

Data Protection Act
In the UK, Radar is registered and fully compliant under the Data Protection Act.

Data at Radar
Our backup and retention needs are also provided by Dudobi.

Contingency Plan
Radar's managed service provides a remote mirrored site, which means we are able to provide a continuous, uninterrupted service to our clients.

Data at/for client
All data for client to be supplied on CD/DVD-ROM, external hard drive (EHD) or via secure FTP transfer, zipped and password protected following update or selections. This CD/DVD/EHD will serve as first line of backup for the client

Alternatively data can be re-supplied from the main database from Radar's hosted server within 24 hours of failure, should the situation demand it

Database interrogations made on Radar equipment and e-mailed through to client will automatically be backed-up according to Radar's standard back-up procedure

Data security

Radar ensures that security is in place on all computer equipment that data is stored upon. This includes:

- All desktop computers, laptop computers, and servers require user name and password to gain access

- When Radar take laptops or netbooks off site, they do not hold any sensitive client data on them so that if lost or stolen, they pose no security risk

- All computers are only used either standalone or behind a hardware and software based firewall

- Any external access to the system is only provided to essential staff and agents

- External agents only have access to their own secure FTP site

- No generic guest FTP site is available

- External access requires a user name and password to be provided

- All passwords are amended on a monthly basis

- All passwords are complex and contain a combination of mixed case characters, numbers and special characters

- No password may be a real word

- Anti-virus software operates on all desktop computers, laptop computers, netbooks and servers

- Any sensitive data sent by email, CD or DVD will be contained within an encrypted zip file

- All retired hardware has their disk drives either scrambled or physically destroyed

More information about our data security is available on demand