Data Storage, Security and Back-Up Policy

1. Data Storage and Security Measures

1.1. Customer Data saved in CoolCare is stored securely behind an industry-standard firewall.
1.2. Using SSL Encryption, all data accessed is securely encrypted before it is sent over the internet, then decrypted once it reaches the customer, to prevent interception of data during transmission.
1.3. Data is backed up both locally at CoolCare's server centre for quick restore, and remotely off-site in a separate UK data centre, should a disaster strike the primary building.
1.4. The primary CoolCare server centre is located in CoolCare's Head Office.
1.5. The remote off-site data centre is at an undisclosed UK-based location, known only to CoolCare Ltd.'s senior technical team and directors.
1.6. Both the primary and remote server centres are in secure and locked rooms with a security code to prevent physical access to the server hardware.
1.7. A limited number of CoolCare personnel have access to the primary server centre.
1.8. Remote access to the server is not possible without an administrator-level password.
1.9. The servers are virtual and stored on load-balanced, replicated hardware, which can be hot-swapped in the event of hardware failure.
1.10. CoolCare utilises a 100Mbps leased line internet connection, CoolCare also has a 100Mbps backup radio-broadband connection for failover.

2. Data Access

2.1. CoolCare stores and processes data on behalf its Customers who input data into CoolCare, including Protected Data.
    2.1.1.1. CoolCare does not collect Customer Data which has been input into CoolCare
    2.1.1.2. The Customer shall comply with Data Protection Legislation in connection with the collection and processing of Customer Data
    2.1.1.3. Only authorised Customers, who adhere to CoolCare's terms and conditions for use of CoolCare's services, will be given access to CoolCare.
2.2. It is the Customer's responsibility to manage their users' access; permission levels and passwords effectively to prevent unpermitted remote access to Customer Data.
2.3. CoolCare does not access, amend or delete Customer Data without prior consent from the Customer and will only do so in pursuit of meeting CoolCare's legal obligations to our Customer in the delivery and improvement of our product and services.
2.4. CoolCare's administrators may access Customer Data upon authorised requests from the Customer for the purposes of, but not exclusive to:
    2.4.1.1. Troubleshooting and support
    2.4.1.2. Training
    2.4.1.3. Demonstration of functionality
    2.4.1.4. Data recovery
    2.4.1.5. Deletion of data
    2.4.1.6. Testing

2.4.2. It is the Customer's responsibility to inform CoolCare of which individuals or users are authorised on behalf of the customer to allow CoolCare administrators to access, amend or delete Customer Data.

2.4.3. CoolCare will take all reasonable efforts to verify whether an individual or user is authorised to consent on behalf of the Customer for CoolCare administrators to access, amend or delete data prior to taking any action.

2.4.4. CoolCare shall not be liable for the access to, amendment or deletion of such data on the basis of consent from individuals acting on behalf of the Customer who are not duly authorised.

2.5. CoolCare employees will act in accordance with CoolCare's Privacy and Data Protection Policy at all times.

3. Backup

a) Full backups of all CoolCare data are performed every 24 hours and are retained for 30 days.
b) The backups process begins at 2am, customers will be able to use CoolCare as normal while backups are processing.
c) Should data-recovery be required, the most recent and thorough backup will be used for recovery purposes, unless otherwise requested by the customer.
d) All reasonable efforts will be made by CoolCare to prevent any data loss.
e) CoolCare Ltd. will inform customers whenever data recovery takes place and the date and time the data has been recovered to.
f) If data is irrecoverably lost following data recovery, it is the Customer's responsibility to reinput any lost data.