ClearCenter Remote Server Backup Privacy and Security Statement

Your data is your data. It is that simple.

This is why ClearCenter designs the storage of your data to best protect it from all intrusions or threats. ClearCenter uses high levels of encryption in both the transmission (RSA 2048-bit public/private key authentication or better for the handshake process and subsequent session key encryption while the data channel is secured with a randomly generated 256-bit AES session key or better and the shared secret key (host key) used for authentication is also a 256-bit AES key) and storage of your data (dm-crypt module which encrypts using a 256-bit AES key). The technology is designed in such a way that only the transmitting ClearOS server can decrypt the data. This key is never stored anywhere by ClearCenter. If a client loses or forgets their volume key, we can not recover their backup data. It is your responsibility to ensure that this key is complex and difficult to compromise as well as it is your responsibility to recall this information. The client key (which is set by the user of this service, located on the server in question, and only revealable by the user or his server) represents the only tangible method for access to the user's data that known to us.

While it is possible for an entity with enough resources to crack any encryption method, ClearCenter has and will take every precaution to ensure that the tightest methods available to us are implemented within best security practices. In the event that a general failure, backdoor, loophole, exploit or other mechanism is discovered, ClearCenter will make every effort to ensure that the failure, backdoor, loophole, exploit or other mechanism is fixed, updated, or repaired. In the event that ClearCenter cannot ensure security of the transmission or storage of your data, ClearCenter will discontinue the service and refund the balance of the remaining service at a pro-rated rate based on the remaining duration of the service term purchased.

All Remote Server Backup data is stored outside of the United States of America. All data centers used by ClearOS for the purposes of Remote Server Backup and customer data are housed in data centers that comply with PCI compliance standards and industry best practices. Encrypted data stored on ClearCenter servers are subject to the local laws of the countries in which that data is stored. This can include any of the following countries (Canada, New Zealand, and the United Kingdom but by default is located in Canada.) If you desire that your RBS data be stored in a country not listed or in a particular country that is listed, please contact ClearCenter. To date, ClearCenter and its related companies has never received any request from any legal authority requesting customer data (encrypted or otherwise) under subpoena or other legal instrument.

Remote Server Backup Privacy and Security Statement version 2.0 (updated 1 January 2014)
David Loper
Vice President of Technology
Representing ClearCenter Corp.