



Hotsite Back-Up Privacy and Security Statement

Hotsite Back-Up™ is committed to ensuring the security of your information. To prevent unauthorized access or disclosure, maintain data accuracy, and ensure the appropriate use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect from your electronic backups.

In addition, Hotsite Back-Up™ will not sell, rent, or lease your personally identifiable information to any third parties. So, for example, we do not sell your email addresses or your name and personal demographic information to mass marketers.

Data encryption, or scrambling, as it is sometimes known, is a method of securing sensitive data so that it is not viewable by unauthorized users. All data that is sent to us is encrypted before it leaves the machine on which it resides within your office. Each user must specify a secret key which is used to encrypt the data.

We use 448 bit encryption, which to our knowledge, is virtually unbreakable. However, with your explicit permission, Hotsite Back-Up™ has option to recover your data without your secret key. That option can be disabled at any time, if you prefer. You may have already done this by answering **"NO"** to the question regarding this when you signed up. When this option is disabled, absolutely no one besides you (not even Hotsite Back-Up™) is able to recover the data for this account. **IF THIS OPTION IS SET TO "NO" AND YOUR SECRET KEY IS LOST OR FORGOTTEN, YOUR DATA CANNOT EVER BE RECOVERED.**

It is our policy to respect the privacy of our customers. Therefore, Hotsite Back-Up™ will not monitor, edit, or disclose the contents of a customer's private data unless required to do so by law or in the good faith belief that such action is necessary to: (1) conform to the edicts of the law or comply with legal process served on Hotsite Back-Up™; (2) protect and defend the rights or property of Hotsite Back-Up™; or (3) act under exigent circumstances to protect the personal safety of its customers or the public.

While we use encryption to protect sensitive information online, we also do everything in our power to protect user information off-line. All of our users' information, not just the sensitive information mentioned above is kept in a restricted access area. Only team members who need the information to perform a specific job (for example billing or customer service) are granted access to personally identifiable information. Our team members work in a highly secure computing environment. Furthermore, ALL team members are kept up-to-date on our security and privacy practices.

Physical security to our computing equipment includes, but is not limited to:

- Card key access monitoring system with cameras in key zones
- Closed circuit video surveillance recorded locally and fed to 24x7 monitored network operations center (NOC)
- Reporting of trouble and alarm signals to local site and NOC and to our senior management
- 24x7 monitoring by dedicated security teams
- Vehicle entrance barriers
- Secure loading bays
- Strict policies on handling customer packages

Please feel free to contact us regarding any questions about our privacy and security measures and policies.