

GILLWARE DATA SERVICES

PROVIDING FIRST-CLASS DATA BACKUP SOLUTIONS

GILLWARE REMOTE BACKUP

Gillware Data Services software developers had two primary objectives when designing Gillware Remote Backup: 1) ease of use and 2) security of user data through all phases of data transmission and storage.

Gillware Remote Backup uses proven data encryption techniques to ensure that a user's data remains secure during all aspects of the backup process. The backup process begins by encrypting the user's data with an encryption key. The encryption key is unique and is generated automatically during the installation of Gillware Remote Backup. Alternatively, users can choose to generate or purchase their own key. After the data is encrypted, it is transferred over the internet via the SSL protocol to Gillware Data Services servers. The data remains encrypted on Gillware Data Services servers and is only decrypted after being downloaded back to the user's machine.

Gillware Data Services provides two distinct options for the generation and storage of encryption keys.

OPTION 1 [DEFAULT]:

The Gillware Remote Backup software generates a unique encryption key during installation. A copy of the key is automatically forwarded to Gillware Data Services for backup. Gillware Data Services makes two backup copies of the key. One copy is stored off-site in a Gillware Data Services vault. The second copy of the key is sent to the user for their personal storage and use.

OPTION 2:

The Gillware Remote Backup software generates a unique encryption key during installation. A copy of the key is automatically forwarded to Gillware Data Services for backup. Gillware Data Services makes a single copy of the key. This single copy is sent to the user for their personal storage and use. After confirming receipt of the key, Gillware Data Services permanently deletes all copies of the key. It is important to note that this option places sole responsibility of encryption key storage on the user. Gillware Data Services has no means for reproducing the encryption key following its deletion. User's choosing this option are required to sign a release form instructing Gillware Data Services to destroy all copies of their encryption key.

