



## Frequently Asked Questions about Encryption Keys

### 1. What is encryption?

Encryption is basically the process of taking a computer data file and systematically scrambling the contents of the file so that it cannot be easily read by unauthorized persons. The Dr.Backup remote backup client software makes an encrypted copy of all data files it backs up from your PC -- and transmits this secure data to our backup storage servers. At no time is unencrypted data ever sent across the Internet.

### 2. What is an encryption key?

An encryption key is a specific series of letters and/or numbers which can be used to scramble and de-scramble the contents of an encrypted data file. A file which has been encrypted cannot be read without this key. For this reason, it is very important that the owner of the encrypted data carefully safeguard the value of their encryption key.

### 3. What is my Dr.Backup encryption key?

When you installed the remote backup client software, a completely random encryption key was generated for you automatically. The client software offered you the opportunity to record this secret key on a floppy diskette when you performed the installation.

### 4. I didn't create a recovery diskette with my encryption key when I installed my software. How can I do it now?

Refer to the Quick Start User Guide for instructions on how to use the remote backup client software to access the encryption key management screen. On the dialog box where you set your encryption key, you will see the option "Create Key Disk." Select this option and insert your diskette when prompted. A complete recovery diskette will be created. Store this diskette in a safe place away from your computer.

### 5. I don't have a diskette drive on my computer. How do I save my encryption key?

For users of computers without a diskette drive, the Dr.Backup Quick Start User Guide recommends that you manually set the encryption key to a known phrase which will not be forgotten, but cannot be easily guessed. Refer to the Quick Start User Guide for instructions on how to change the encryption key from a random value to a private code you specify.

**Note:** The 4-digit password used to log into the Dr.Backup website is NOT your secret encryption code.

### 6. I've lost a data file and I need to recover it back from the Dr.Backup storage servers. What do I do next?

If you have been performing regular data backups, your data file is likely safe and secure on our remote offsite storage server. Use the remote backup client software and select the Restore option from the main menu. You should be able to locate the name of the file you lost and electronically retrieve it from the remote storage server.



**Dr.Backup**<sup>™</sup>  
remote backup service

**7. I've had a hardware failure on my PC and I can no longer use it. I need to recover my critical data files and move them to a new PC/server. What do I do now?**

You will need to reinstall the Dr.Backup client software on the new PC using the "disaster recovery" installation option. To successfully complete this process, you will need the recovery diskette you created when you first installed the software. Alternatively, if you do not have this diskette, you can manually key in the information required for recovery – provided that you know your secret encryption key.

Please contact Dr.Backup customer support for assistance prior to attempting a disaster recovery installation.

**8. I've experienced a disaster and the employee who had the recovery diskette has left the company. Nobody can find the diskette and we never manually set the encryption key to a known value. How can we get our data back?**

Dr.Backup customer service personnel can provide you with your account name and password information. However, the critical missing piece is your encryption key. Unfortunately, for security purposes, Dr.Backup personnel are not permitted to maintain records of your secret encryption key.

This means that while your data is likely safe and secure on our servers, because it is in encrypted format, it is of little use without the encryption key. You must recover the encryption key in order to recover your data from our servers.

---

Remote Backup Systems (RBS) of Collierville, Tennessee does offer an emergency encryption key-recovery service. With your consent, they will attempt to "crack" your secret encryption key. Dr.Backup offers no guarantee that RBS will be able to recover your encryption key.

If you have experienced a data disaster and do not have your encryption key, you may contact Remote Backup Systems directly to inquire about this service from them. Please identify yourself as a client of Dr.Backup and provide them with our customer support number, 301-604-5534.

As of June 2004, the current list price for the RBS encryption key recovery service is US \$500.

***Remote Backup Systems, Inc.***

319 Poplar View Lane West

Suite 1

Collierville, TN 38017

Phone: 901-850-9920

Toll Free: 800-945-4491

Fax: 901-854-7411