# How to back up PGP keys and keyrings

## Q: How to back up PGP keys and keyrings

PGP is no longer being offered on the software grid. Support is being phased out and will discontinue at the end of 2016.

### Answer

PGP stores keys in two files on your hard disk; one for public keys and one for private keys. These files are called keyrings. It is important to keep your PGP private key very secure. If you lose your private keyring, you will be unable to decrypt any information encrypted to the keys on that ring.



### Windows Users

1. Go to C:\Documents and Settings\Administrator\My Documents\PGP directory or whichever directory you specified for your public and private keys when you first installed PGP.
2. Copy your pubring and secring files to a USB device or external hard drive or make a backup copy with TSM.

By default, PGP Desktop automatically creates a backup of your keyring (private and public keys) to the default keyring folder when PGP Desktop is closed. The backup files can then be used to restore your key if your keyring files are accidentally deleted or the files become corrupted.

You may also specify a different location for your backup keying files from within PGP Desktop.

1. Open PGP Desktop by clicking on the icon on your desktop.
2. Select the **Options > Keys** tab.
3. In the Backup selection:
    - Enable / disable the automatic backup of keys
    - Specify the location of your backup keyring files
4. Click **OK** to apply any changes made.

### Mac Users

1. Go to **your user directory > Documents > PGP**.
2. Copy the files located in this folder (PGP Private Keyring.skr and PGP Public Keyring.pkr) to a USB device or external hard drive or make a backup with TSM.

**Additional Information**
More information on PGP can be found on the PGP Desktop page. If you don't find your answer, contact pgp-help@mit.edu.