

Sensitive Information Backup Checklist

No	Procedures	Status	Notes
1	Wipe each previous backup before proceeding with the next one.		
2	Use full backups and never incremental ones.		
3	Be aware that some disk-encryption and partition-encryption software have the quirky requirement that they can only back up the encrypted portion after it has first been decrypted. This means that the backup will be extremely vulnerable. Do not use such encryption software. If your backups do contain unencrypted information that is encrypted on your computer(s), store your backups where they cannot be found by unauthorized third parties.		
4	Use a password to protect the contents of the backup. This provides no protection against a forensic attack, but does protect from casual perusal. Also, use compression, which is usually offered as an option in the backup process, to make glancing at the contents just a bit more difficult.		
5	Always store the backups offsite at a location other than that of the computer that was backed up, preferably at some location not accessible by a potential adversary (business or personal). This will also help you save the data in case of fire at the site of the computer.		
6	Do not ever acknowledge the existence of backups to unauthorized others. Explain the existence of backup software as something you always meant to do but never got around to.		
7	Protect the backups as if they contained the family jewels. They often do.		