

Data Storage and Backup

First some terminology...

- Original Data
- Operation Data
- Backup
- Archive



1

Why Bother?




hardware failure
 natural disasters
 software or media faults
 virus infection or malicious hacking
 power failure
 human error
 results validation

Server hardware/software failure
 data requests / FOIA/ Lawsuits / legal
 requirement
 funder mandates
 Format obsolescence
 Loss of financial stability



2



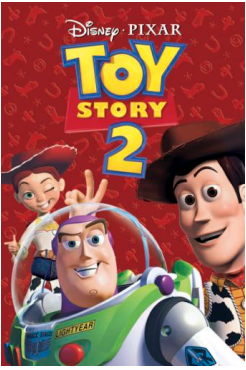
NEWS ▾ VIDEO ▾ WEATHER

PhD student offering \$5,000 reward after car thief steals all his research

CTV Montreal

Published Wednesday, November 29, 2017 10:43PM EST

"The thief stole a backpack containing his laptop, a notebook, and a thumb drive with all his backup material... With all his work gone, he will likely have to head back to the lab and redo experiments, delaying graduation by months."




Audit: Baltimore Data Losses Due to Insufficient Backups

A recently released report states that information was lost after only being saved on local servers. The lack of available data hampered the ongoing recovery efforts and raised questions about protocols.

BY LUCAS ROPEK / SEPTEMBER 30, 2019

<https://www.govtech.com/security/Audit-Baltimore-Data-Losses-Due-to-Insufficient-Backups.html>



Myspace accidentally lost all the music uploaded from its first 12 years in a server migration, losing over 50 million songs from 14 million artists.

Hello Austin,

Yes, this is true. Due to a server migration files were corrupted and unable to be transferred over to our updated site. There is no way to recover the lost data.

Thanks,

Myspace

3

3-2-1

3 copies of your data on
2 types of storage media with
1 copy off-site

4

Storage Media

- Desktop and Laptop Computers
- Campus servers
- Commercial Cloud Backup
- External hard drives
- Optical Storage (CD, DVD)
- Paper
(original notebooks, printouts of spreadsheets, text files)



5

Your Content in our Services

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

6

Storage Media (cont.)

1. Test Your Storage Media Regularly
2. Beware of Early Hardware Failures
3. Determine the Life of Your Hard Drives
4. Routinely Inspect and Replace Data Discs
5. Handle and Store Your Media With Care



7

Backup vs Archive

6. Multimedia (e.g., photo, video, audio) backup is more challenging, in part because transcriptions and captioning can be important for interpretation, discovery, and accessibility.



8

What about the Originals?

7. Finally, consider the short- and long-term security of the originals: specimens, samples, documents and data sheets, photographs, or other physical items.

- Campus Office
- Lab or Museum/Herbarium
- Departmental Office
- Commercial storage facility
- Home
- Library



9

Make a plan. Write it down.

- what needs to be prepared and for how long
- where backups are located
- who can access backups and how contacted
- how often data should be backed up
- what kind of backups are performed
- who is responsible for performing the backups
- hardware and software used for performing backups
- how / how often to check if backups is successful
- the media are used to backup data
- a list of any data that are *not* archived or backed up



10

Backup Strategies

Backup your data at regular (optimized) frequencies

Make it easy to follow your plan

Automate

*Remember: synced computer and cloud drive are **not** independent copies*



11

Restricted Data

- Know if your data require extra protection
- Take steps to ensure the security of Restricted data



12

And finally....

ensure your data will be readable by many systems & for many years

**USE OPEN
(non-proprietary)
DATA FORMATS**