

Creating a Backup Process

The 3-2-1 Rule

The basis of all backup plans revolves around the 3-2-1 rule.

- 3 copies of your data
- 2 of the copies are on different devices on-site
- 1 copy is 'off-site'

In a perfect world this would mean that your `Thesis.docx` exists on your computer, on your external backup drive, and on a cloud drive (gdrive, onedrive etc). How far you want to go with this rule is part of your planning.

Create a plan

What needs to be backed up?

Go back to the [previous page](#) to see the scary list of things that people have lost over the years, and think about what you have that you care about.

Generally bulky things like games and the OS itself do not need to be backed up, redownload/reinstall these things after recovering your environment.

For this reason we discourage the use of image based backups when an image is not explicitly needed. By minimizing the size of your backups you can complete your backup/restore process quicker and for cheaper.

How often does your data change?

Determine how often your data is going to change. Your wedding photos will never change, but the thesis you are working on will change quite often.

When things change more often you need to decide how much time/work you can lose in a disaster. If you cannot afford to lose more than a few hours you need to run your backups much more often than is losing a full day was OK.

With all backups you need to also decide if you need version history. This is how many copies of backups you keep, like a timeline. If you overwrite your old backup every time you make a new one then you will be in big trouble if there is an error in your only backup.

Where will the data be backed up to?

Critical data should fully follow the 3-2-1 rule while less critical can be more lax.

The simplest method most users start with is backing up to a local external hard drive. Replacing data infrequently. This is fine for unchanging data or less critical data.

More comprehensive backup procedures should be automatic. These can use network attached storage (NAS) solutions, scripts or applications to manage the backup creation, frequency, and version control. "Personal Cloud" based solutions such as Nextcloud can check most of these boxes.

To gain a full 3-2-1 scope you can push backups of your NAS to an offsite solution such as AWS S3 or Backblaze.

Revision #9

Created Thu, Nov 26, 2020 5:12 AM by [PipeltToDevNull](#)

Updated Tue, Dec 29, 2020 5:54 PM by [PipeltToDevNull](#)