## **Efficient Backup System Procedure**

# Introduction

A system backup is the process of backing up the operating system, files and system-specific useful/essential data. Backup is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost. System backup primarily ensures that not only the user data in a system is saved, but also the system's state or operational condition. This helps in restoring the system to the last saved state along with all the selected backup data. Generally, the system backup is performed through backup software and the end file (system backup) generated through this process is known as the system snapshot/image. Moreover, in a networked/enterprise environment, the system backup file/snapshot/image is routinely uploaded and updated on an enterprise local/remote storage server. A System Backup involves all of the system files, boot files, and program files. Backing up both the system and boot files can ensure that the operating system works normally when we restore the operating system. If only one of them has been backed up, the operating system may not work normally after [system restoring.](https://www.backup-utility.com/features/system-restore.html?hot=true) Therefore, it is necessary for us to know what the system partition and the boot partition.

* **System partition:** the partition that installs the operating system, applications, and saves your personal files. That is the so-called C Drive. System files require relatively more space. For example, the system files of Windows 7 require at least 8 GB.
* **Boot partition:** the partition that stores boot files, including boot.ini, ntldr, bcd, winload.exe, etc. Boot files require relatively less space, generally less than 200MB.Before the introduction of Windows 7, the earlier operating systems such as Windows XP, Vista, as well as Windows Server 2003, had the system and boot partitions combined together. That is to say, the boot partition was a system partition and the system partition was a boot partition. Thus, with those earlier operating systems, we just need to backup one partition during system backup. In Windows 7 and later operating systems, the system partition and boot partition are usually separated. The System partition is the C Drive that can be accessed normally, while the boot partition is a 200MB or bigger partition, named "System Reserved Partition". The boot partition usually does not have a drive letter, and we cannot access it in Windows Explorer. When backing up Windows 7/8/8.1/10 OS, we should backup these two partitions to complete a system backup.

**Procedures: Computer Systems Backup**

The head of Computer/Information Systems is responsible for ensuring that this policy is carried out. Exceptions to the standard computer backup procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

1. A full or incremental systems backup will be performed with sufficient frequency so that the entire system and all data from the end of the school the prior day can be completely restored, if necessary. Each backup should be maintained for an entire month.
2. Data to be backed up include the following information:
3. User data stored on the hard drive.
4. System state data
5. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. The last full backup of the month will be saved as archival records.
7. Monthly backups will be saved for one year, at which time the media will be recycled or destroyed.
8. Incremental backups of new data will be performed daily. Incremental backups will be retained for sufficient time to restore data for at least a week, at which time the media will be recycled or destroyed.
9. Periodic tests of the backups will be performed to determine if files can be restored.

* The testing should be conducted quarterly.
* The tests should be personally monitored by an auditor, and the auditor’s report of their findings should be maintained for 5 years.
* Testing should be conducted on clean servers, and all servers should be restored at the same time.
* Applications testing of the restored servers should be conducted and the results included in the auditor’s report.

1. All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
2. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.

**Needed of a Regular System Backup**

In general, when the operating system has been used for a period of time, most users would face the problem of system crash, as well as many other disk problems that prevent the system from working normally. In such cases, reinstalling the operating system is one available solution. As known to many people, OS reinstallation is time-consuming. It requires at least half an hour at a time. And then it can take many hours to install various drivers and applications. To save a lot of time and effort, we can do a complete backup of the system (usually C Drive) immediately after the installation of a new operating system and some commonly-used applications. It is wise to do a full system backup at intervals no matter how old the computer is. Thus, if there is any system problem, the system can be restored to the previous normal state quickly with the backup image file.

**Ubuntu operating system**

Ubuntu, a Linux distribution based on Debian architecture, is an open source software platform which sun everywhere from smartphone, tablet, personal computer, network server and cloud. There are hundreds of different Linux distributions out in the world, and many are free of charge and have communities our users who provide each other with guidance and support. A Linux distribution is a version of the operating system that contain Linux kernel. Ubuntu is one of the most popular Linux distributions and it is published by Canonical Ltd. It is a free operating system and it is easy to get a copy by downloading the OS directly from its website. A default installation of Ubuntu convers a broad scope of software such as Firefox, Library Office, Transmission, games, etc. Ubuntu is suitable for both PC and server se and current release supports Intel x86 (IBM compatible PC), AMD64 (x86-64), ARMv7, ARMv8 (ARM64), IBM POWER8, IBM Series (zEC12/zEC13), and PowerPC architectures.

# Overview on backing up Ubuntu partition

Routine backup is an effective way of protect data against data loss, and backup should be done in time once there is big change to your data. Thus it is necessary to create a backup for your Ubuntu partition. As Windows user, it is familiar to backup Windows operating system, as we can backup Windows partition with the built-in tool or third-party system backup software. Likewise, we can backup Ubuntu partition using either built-in tool or Ubuntu backup software. As we all know, many users would like to dual boot Ubuntu with Windows, thus we can also backup Ubuntu partition under Windows environment or Ubuntu. Before we start the backup process, you should decide where to store the backup data. it is not recommended to save backup file on the same hard drive or partition with original data. If you are a home user and small business, you can prepare a hard drive to store backup data, which is safe enough and cost-effective. Also, you can keep more than one backup copy on different hard drives in case of any unexpected issue.

# Backup Ubuntu partition using the pre-installed Deja Dup

Deja Dup is a backup tool which comes pre-installed with most Ubuntu releases. It enables users to backup Ubuntu as well as restore system from backup. This section will show you how to backup Ubuntu partition with this tool step by step. You should note that this method takes Ubuntu 14.04 LTS as example, and it is may not work on all Ubuntu version. Now let’s start making the backup.

1. Open the backup tool by pressing Windows key and typing “Backups” in searching box. Then click the Backup icon.
2. Select “Folder to use” option on the Backup window. You can use +/- button to make changes based on your requirement and then go to next step.
3. Select “Folder to ignore” option. By this step you can decide which folder you do not want to backup. For example, folders “rubbish bin” “Downloads” are set to be ignored by default, and you ignore more folders by clicking “+”.
4. Select “Storage location” option. You should decide where to store backup data. You can select hard drive from drop-down menu.
5. Select “Scheduling” option. If there are many files to be backed up, you can set the backup regularly. If you just want to make a one-time backup, you can turn off schedules.
6. Click “Overview” option and click “Backup Now” button. Then a screen with a progress bar will pop up and show the backup process.

**Step 1. Click the backup system application and go to the system backup.**

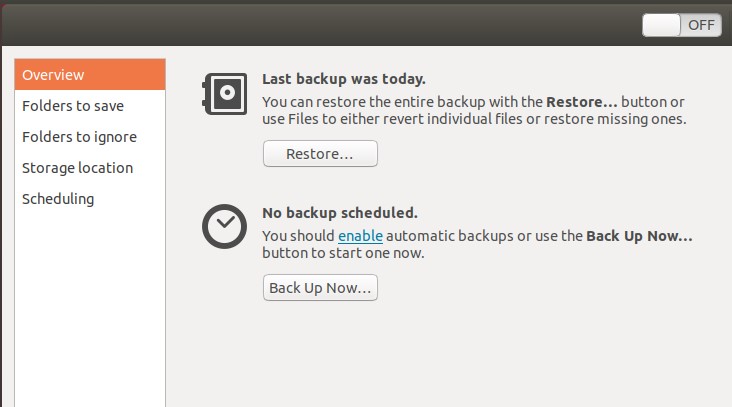


Figure: System Backup.

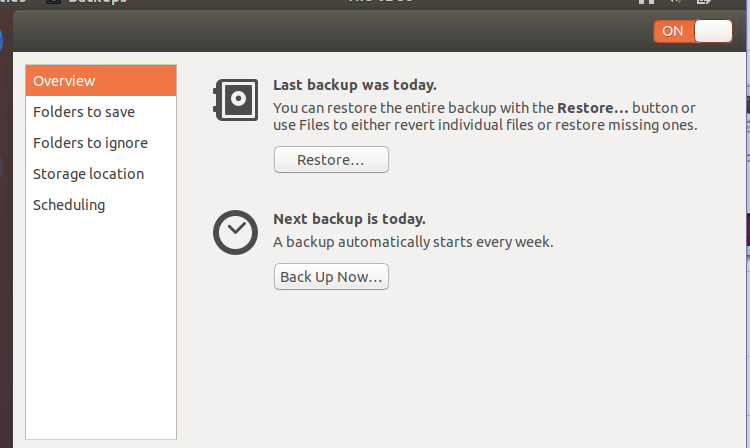


Figure: System Backup.

Step 2. Click the folder save application and then save any documents.

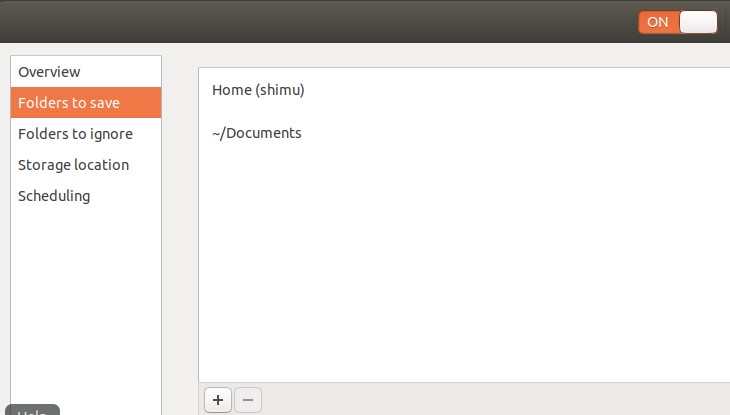


Figure: Select Folders to save.

Step 3. Click the folder ignore application and go to documents to trash or backup.

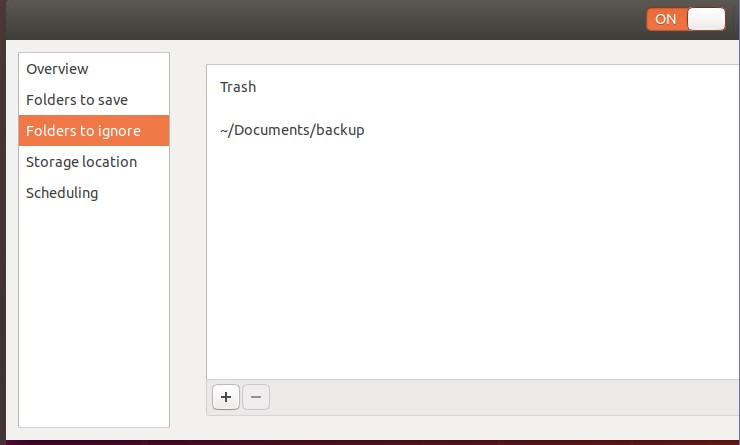


Figure: Select Folders to ignore.

Step 4. Backup Storage Options.

You will also need to think about where to store your backups. Here again, you have more than one option.

1. You can back up your data to local or USB disks. This option is best for backing up individual files and hardware. It is not ideal for networks. If the drive is destroyed, you will lose your backup.
2. Network Attached Storage (NAS) and Storage Area Networks (SAN) are also options. These are ideal for storing data for your network. They make for easy recovery network data recovery in most situations. The exception is if your hardware or office is destroyed.
3. Backing data up to tapes may be appealing to some companies. The tapes would be shipped to a secure location for storage. This keeps your data safe. The downsides are that you will have to wait for tapes to arrive to restore your data. They are best suited for restoring your whole system, not individual files.
4. Cloud storage is increasingly popular. You will need an internet connection to send your data to the cloud. There are options available to help you transmit a significant amount of data. You will be able to access your data from anywhere, but not without an internet connection.

To decide which option is best, you will need to consider two metrics, RTO and RPO. The first is your Recovery Point Objective or RPO. That is the maximum time you are willing to lose data on your systems.

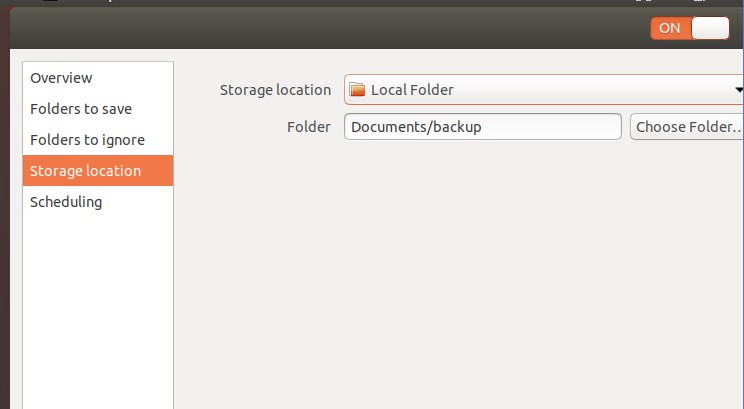


Figure: Select Storage location.

Step 5: Click the scheduling application and go to automatic backup with on/off.

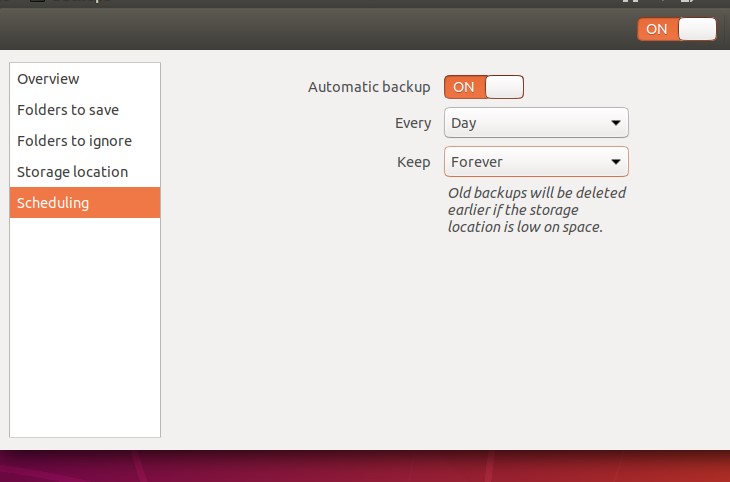


Figure: Select Scheduling.

Step 6: Click the backup now.

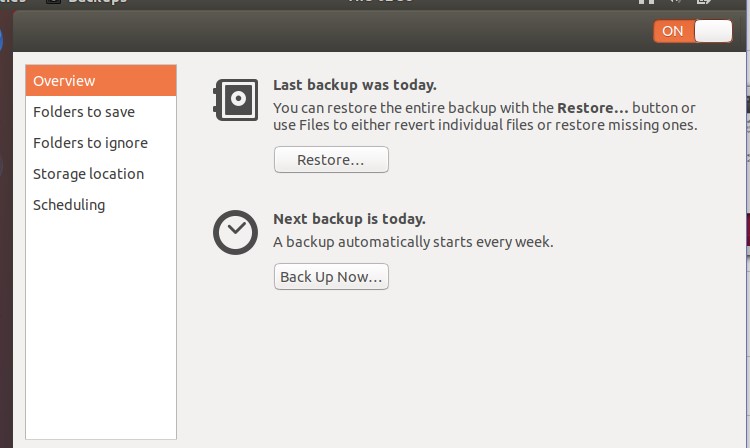


Figure: Back up Now.

Step 7: For the encryption data or file, encryption password is needed.

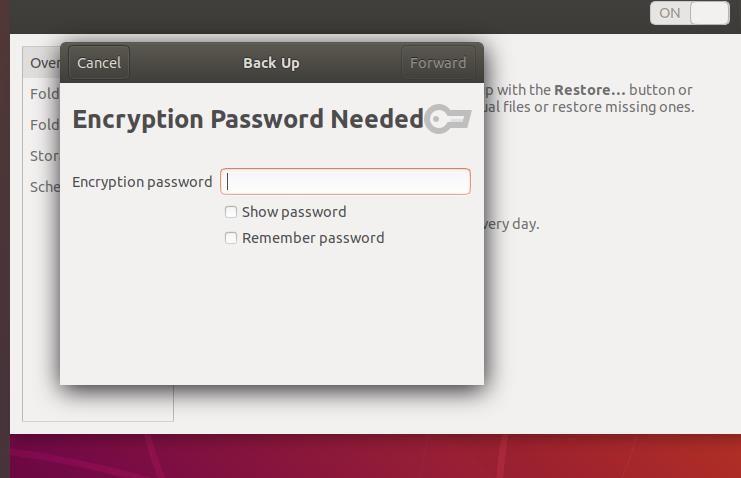


Figure: Enter Encryption authentication password.

Step 8: Backup system completed.

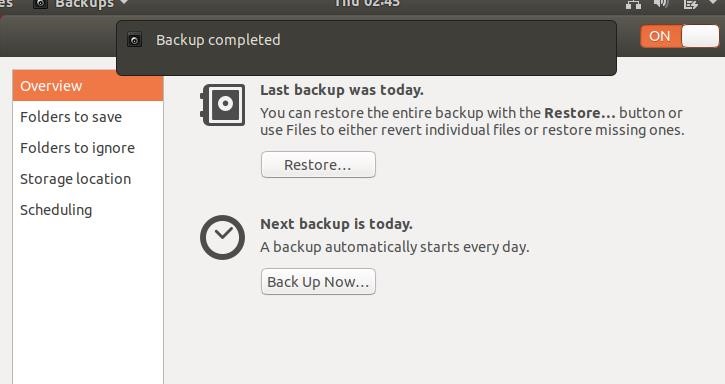


Figure: Backup completed.

## **Overview of Windows 7 Full Backup**

A system backup is a process of backing up the operating system, files, and system-specific useful/essential data. Backup is a process in which the state, files, and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost. As we all know, Windows 10's newest update is coming out. In order to avoid Windows 10 data loss, we need to make a full backup of Windows 10. Backups help ensure that your system and files aren't permanently lost or damaged. Follow the two methods below to make a full backup of Windows 10/8/7.

## **Method 1. Backup to Make a Full Backup**

Backup Free has more than enough features for personal use. The program can perform system, disk/partition, and file backups either manually or automatically through [scheduled backups](https://www.easeus.com/backup-utility/schedule-backup.html). You're able to make full, [differential and incremental backups](https://www.easeus.com/backup-utility/differential-backup-vs-incremental-backup.html). If you want to control over your backups, start downloading the [free Windows backup software](https://www.easeus.com/backup-software/tb-free.html) and make a full backup.

**1.** Windows 10 backup software and then choose the "System Backup" option.

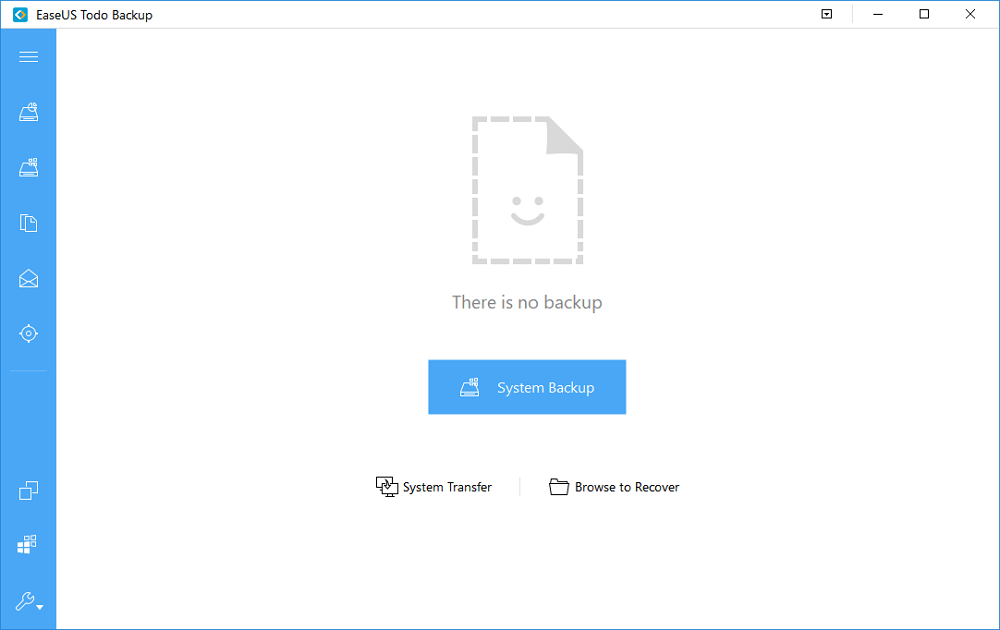
[](https://www.easeus.com/images/en/screenshot/todo-backup/guide/easeus-todo-backup.png)

Figure: System backup.

**2.** The software will then automatically recognize your operating system. And what you need to do here is to perfect the Destination, Plan name, and Description.

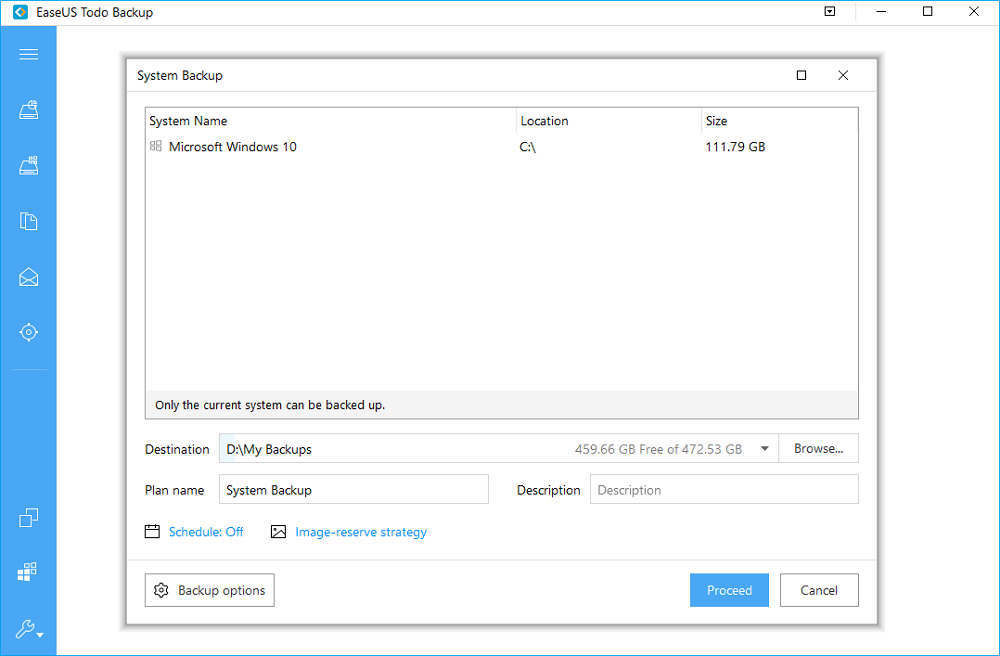
[](https://www.easeus.com/images/en/screenshot/todo-backup/guide/windows-10-system-backup.png)

Figure: System backup proceed.

**Note:**

* Destination - Click the folder icon to modify your backup destination.
* Plan name and Description - An accurate plan name and appropriate description can help you find the needed image file easily.
* You'd better create the backup file to an external storage device or in some other drives. If not, there may be a risk of the backup file getting corrupted or destroyed.

**3.** Click **Proceed** to start Windows 10 system backup.

**Tip:**It is pretty easy to recover the system image. Just open the software again and click the "Recovery" option of the image, and then you can restore the system. If you need a detailed instruction, please refer to [system recovery](https://www.easeus.com/support/todo-backup/system-recovery.html).

**Method 2. Create a System Image of Windows 7 With the Built-in Tool**

In this Windows 10 guide, we will also walk you through the steps to create a full backup, including all your settings, apps, and files, using the built-in system image tool. However, the steps are a little bit difficult compared with using a free tool to back up the system. Read on to create a system backup of Windows 10 using the built-in system image tool.

1. Click on Start and click Control Panel then choose Backup and Restore (Windows 7) Windows

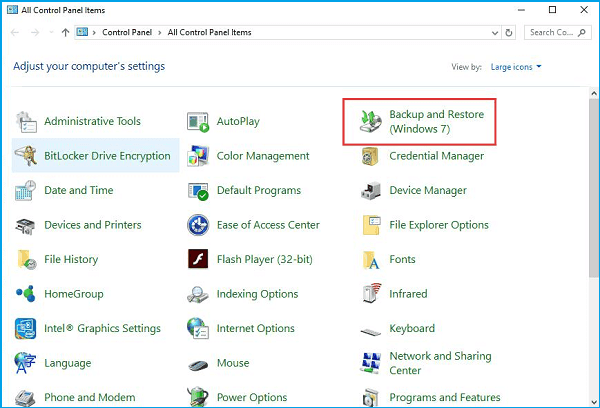


Figure: Backup & Restore windows.

2. On the left pane, click the Create a system image.

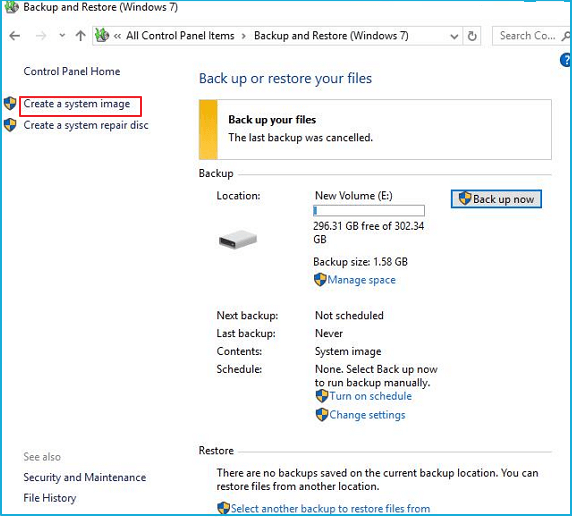


Figure: System image.

3. Select the location to save the Windows 7 user profile backup and click “Next” to continue. You'd better save the backup on an external storage device so that you can transfer it to other computers.

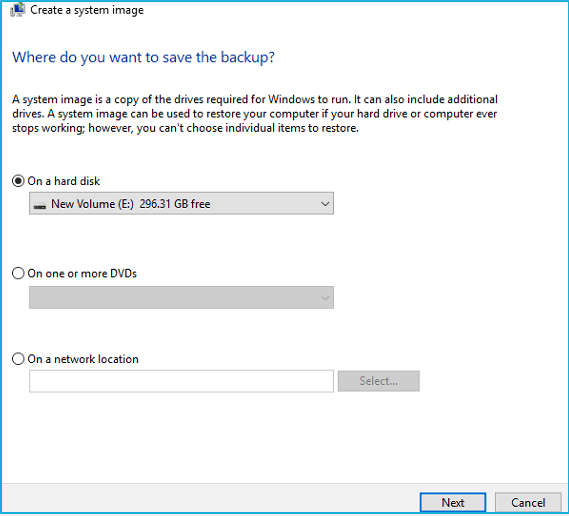


Figure: Location on the drive.

Once you completed these steps, the wizard will proceed to create a full backup of your system, including everything that is stored on the main drive, as well as the system reserved partition. After the backup is done, you'll be prompted to create a system repair disc to access the recovery options if your computer is unable to boot.

Quick access: You can always create a repair disc by clicking the Create a system repair disc link within the Backup and Restore (Windows 7) settings page.

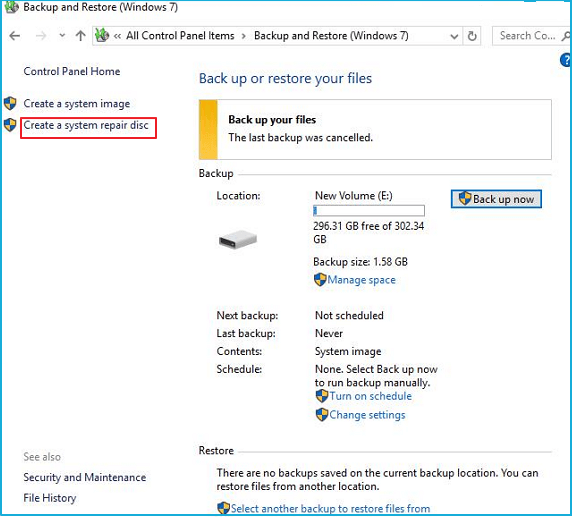


Figure: Create a system repair disc.

## **How to Restore the System Image Backup of Windows 10**

Now that you have the backup of your Windows 10, and a system repair disc, you may also want to know the way to restore the system image of it, just read more to learn the steps:

1. Connect the external drive with the system image backup to your device.

2. Connect the disk that contains the system repair files (or USB bootable drive with the Windows 10 installation files) to your device.

3. Reboot your computer. Press F2 and choose boot from USB.

4. On the "Windows Setup" page, click the Next button.

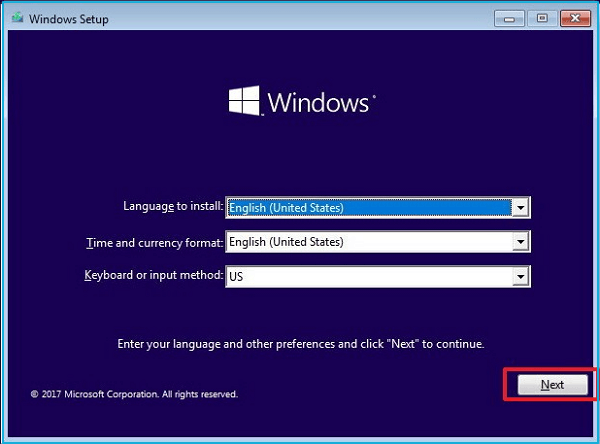


Figure: Windows Setup.

5. Click the Repair your computer link located at the bottom-left corner. Then Click the Troubleshoot option.

6. Click the System Image Recovery option.

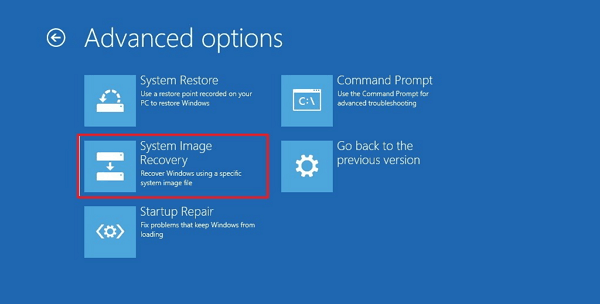


Figure: System image recovery options.

7. Choose the target OS. (In this case, Windows 10.)

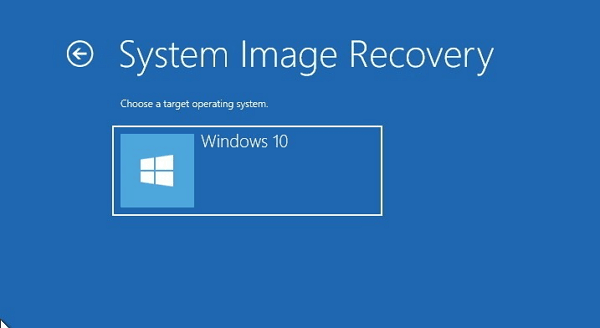


Figure: System image recovery.

8. On the "Re-image your computer" page, select the Use the latest available system image option and click Next.

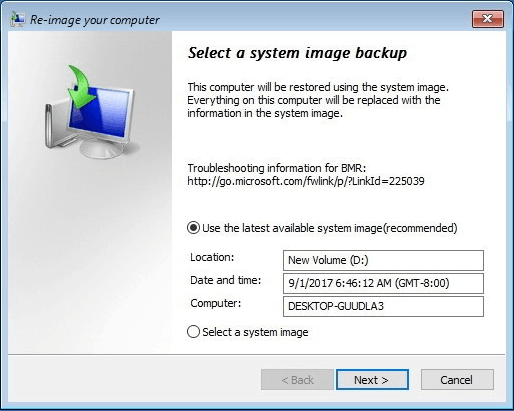


Figure: Re-image our computer.

If you're restoring a full back up to a new drive, you can also select the Format and repartition disks option. (Use this option carefully, as it will erase any existing partitions and disks on your computer.) Then click Next.

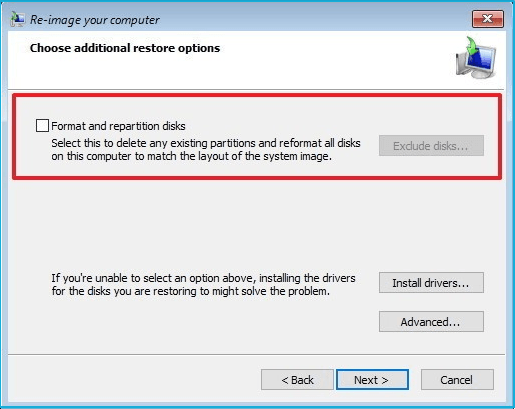


Figure: Additional restore options.

9. Click Finish, and click Yes to confirm that the backup will replace the data on the drive.

## **The Conclusion to the Whole Page**

Method 1 is an easy and free method to help you make a full backup of your system. If you want to back up system easily, using a free backup software is indeed easy and fast. Method 2 is a little bit difficult. If you have enough time and patience, the second method is a nice choice.

**The Components of Efficient Backup procedures**

Before you create your backup strategy, you should know what to include. Let us break down some of the backup strategy best practices:

1. **Cost.** You will need a **data backup plan** that you can afford. It is a good idea to think beyond dollars. Keep the potential expense of a breach or loss in mind. Then, weigh that against the projected cost of your backup system. That will help guide you.
2. **To store copies of our data.** Some companies prefer cloud-based backup. Others like to have a physical backup. The most cautious companies use multiple backup sources. That way, if one backup fails they have another in place.
3. **Data risks.** Every company must think about malware and phishing attacks. However, those might not be the only risks you face. A company in an area that is prone to flooding must consider water damage. Having an off-site backup and data storage solution would be wise.
4. **Back up our data.** Some companies generate data quickly. In such cases, a daily backup may not be sufficient. Hourly backups may be needed. For other companies whose data is rarely updated, a once-weekly backup may be enough.
5. **Responsible for our backup planning.** Employee training is essential to an effective file backup strategy. You need knowledgeable people you can rely on to keep things running.

**Rules for effective data backup procedures**

1. **Set consistent policies**

Your procedure should encourage, if not demand, consistent backup policies across all the servers and backup devices in your enterprise. This isn't always possible, especially in the case of mixed backup devices, such as backing up the data center with a disk library and using cloud backup for remote offices. In general, policies are low-level criteria, usually set within backup software, and data backup procedures are the higher-level constructs that determine policies. Thus, in backup, procedures manage policies. So, for our purposes, "backup policy" refers to the rules that control the actual backup. These are usually enforced by the software under the term policy management. Data backup procedures are the methods used to set policies.

1. **Make sure the policies are clear and as easy to implement as possible**

A policy that isn't consistently followed because it's confusing isn't much better than having no policy at all. Ideally, everyone should understand the policy and why it exists. That means putting the justification in writing. Backups involve critical data. Staff should recognize the importance of the data as well as the backup and recovery process. Data backup procedures shouldn't just sit on the shelf -- organizations should consistently update them and review them with staff.

### **3. Establish metrics**

An effective procedure has clear, measurable and appropriate ways of checking to see that the policies are being followed. Modern backup software with automatic policy management features helps considerably. Testing data backup procedures, just like testing overall recovery plans, is key to an organization's knowledge that it can follow the policies appropriately in a data loss event.

### **4. Strive to take the human out of the loop**

A good policy takes people out of the backup process as much as possible, because of machines are simply more reliable. It usually isn't possible or feasible to completely eliminate humans from the process for economic or other reasons, but minimizing their influence should be a procedural goal. Your organization should have confidence in its backup software, whether it's taking differential, incremental or full backups, whether hourly, daily or weekly. However, staff should consistently check that backups are working.

### **5. Collect ongoing feedback**

Effective data backup procedures create policies that are responsive to the real world. That means you need to make an effort to find out from the people in the trenches how well the policies are actually working. Ideally, this is more than a passive effort. Storage administrators should actively seek opinions from the people affected by the stakeholders, especially the people who are doing the work.

### **6. Get buy-in**

You've heard it before: Get buy-in from the people doing the work. However, it's especially important here because many backup and restore failures have human error as a root cause. In addition, media failures -- another common reason for back up issues -- are often a direct result of human error. And human error is notoriously influenced by the human's commitment to the process.To be blunt, if you don't have buy-in, then you're going to have a much higher rate of failed backups. This is a particular problem with backups at remote locations, when the people doing the backups don't belong to the storage organization and running backups is an auxiliary job.

### **7. Make it easy to change policies as technology and needs change**

The purpose of data backup procedures is to make it easy to establish good policies. Good policies are those that reflect and adapt to the real needs of the organization. A slow, inflexible and overly bureaucratic policy-setting procedure will hinder rather than help this goal.

# Conclusion

Backing up our data is an essential task that needs to be performed regularly. Setting up an automated backup task with Sync Back only takes a few minutes. Once done, you'll have peace of mind that your data is safe. Don’t wait until a disaster occurs and live to regret it when your data are lost.

**References:**

* <https://searchdatabackup.techtarget.com/tip/Effective-data-backups-Seven-rules-to-follow>.
* <https://phoenixnap.com/blog/data-backup-strategy-guide-business>.
* <https://blog.leaseweb.com/2019/02/14/backup-storage-options/>.
* https://www.easeus.com/backup-recovery/how-to-make-a-full-backup-of-windows-10.html