FLEXIRENT Finance Solutions

Acronis COMPUTE WITH CONFIDENCE

A.B.T.R.O.N. ENTERPRISES LIMITED

# 9 Tips for a Successful DATA Backup Strategy

*"Backup is your DATA insurance Policy and your policy is only as good as the last backup you can access. Your DATA is valuable, ensure you protect it".*

Carey Duckmanton
Managing Director – A.B.T.R.O.N. Enterprises Ltd

## 1. Offsite – Keep them away from your office

As a minimum the latest backup must be kept somewhere other than your office, in case anything happens to the building/PC/Server e.g. fire, theft, damage. For preference all but the backup media you are using today should be stored offsite. It is not just about protecting your data from a building disaster as we have seen instances where burglars have taken the backup media as well.

## 2. Generational – Make more than one copy

What if you are unable to access your last backup, you need to be able to go back to another therefore it is very important that you have more than one backup copy. It can also be useful to be able to restore file(s) from days/weeks/months ago e.g. some files may change only occasionally (monthly accounting reports) and when they get corrupted/deleted/overwritten etc it can be days/weeks before this is noticed. Additionally the ability to restore files that go back a long way can also assist in any forensic investigation you may need to undertake.

## 3. Complete – Backup ALL Files

Make sure you have everything, not just a bit here and a bit there. In the event that you need to restore your data some implementations of Partial, Incremental or Differential backups can make it difficult to restore a file or set of files and therefore make restores time consuming, costly and sometimes impossible. If you take everything on to one media every time you back-up then it will be easy to find the relevant file, or set of files, to restore and you will know that you have the correct version of the file.

## 4. Frequent – Backup often

A simple rule for Backup Frequency is to make them as frequent as you can easily recreate the data you may lose if you have to restore any lost data from a previous backup. If you were to lose your current data how easy would you be able to re-create the last hour/day/days/week of data changes, ie Accounting system entries, Word and Excel documents, E-Mails received and sent and other files you have been working on (CAD Drawings etc). Answering this dictates the Frequency of your backup.

## 5. Verify It – Make sure the data is on the media

If the backup software has a verify option use it. Although it may take twice as long for the backup process, if the backup Software only thinks it has written to the media or the media has issues you wont be able to restore.

## 6. Check It – Ensure the backup has worked

Every backup that is done needs to be checked to confirm if it has run successfully or not. Most backup systems will provide a log of success or failure, or even E-mail the result. It is very important to check to see that all files selected have been copied to your backup media and if not the backup is re-run or the issue rectified.

## 7. Test It – Make sure you can restore from a backup

Your backups need to be tested occasionally to ensure that you are able to restore files when you need to. There is no point to undertaking a Backup if you are not confident that you can restore your valuable data from that Backup. This should be done at least annually.

## 8. Disaster Recovery – Backup not just your Data

If the computer with all your valuable data on were to go “bang” e.g. virus, windows corruption, fire, theft etc you may be able to get your data from your backup but what about settings, configuration, software installations etc. Rebuilding a system like this can take a long time = Money, so if your backup software offers a Disaster Recovery option it is good practice to undertake one of these backups occasionally, 3 monthly, and test it. Backup Software with Bare Metal Recovery or Hardware Independent Restore is even better – this is where you can restore your entire system to a completely different hardware platform and it will install all your Software, files and settings as they were on the “dead” hardware.

## 9. Accountability – Make someone accountable

It is important that some is responsible for ensuring the Backup is run, checked and media cycled offsite in accordance with your generational pattern. This can be a staff member or your IT department or IT Service provider. In the event you are unable to restore someone needs to be accountable.