IronTree

Select a Backup Solution CHECKLIST

"make an informed decision"

by IronTree

Backup Solution CHECKLIST

IronTree

Technological advances and their pervasive spread amongst the global business community have resulted in the fact that, almost without exception, even small commercial enterprises rely on a technology infrastructure in one form or another.

It follows that data is an irreplaceable element that could cripple or destroy a business if lost. Because technology is continuously advancing and evolving, it can be difficult to keep track of best practices when it comes to your backup
solution. As such, we have developed two handy checklists:

- Evaluating your current backup solution
- Making an informed decision on a new backup solution

Evaluating your current backup solution

Ensure that your business has a backup routine that includes the following elements:

☑ Backup process should be automated.
A fully automated backup routine scheduled at regular user defined frequencies, preferably at least daily. Corporate backup facilities should not be reliant on an individual to initiate the process.

☑ Backup should be off-site.
Good corporate governance dictates that your data should be backed up to a secure, off-site location. Keeping your backup files on a central server or other on-site hard drive is extremely risky. If the backup PC or server
crashes or is stolen then all the information will be lost.

☑ Backup should sequentially catalogue past backups.
Data backups should contain incremental changes to the relevant data files. This facilitates the storage and cataloguing of sequential copies of the data stored at the offsite data centre. This facility ensures that, in the case of data corruption, it's possible to restore the data to a "pre-corrupted" version
of the data.

☑ The correct data needs to be backed up.
Correct and valid data must be selected for backup in the first place. It goes without saying that data that was not selected for backup will not be able to be restored.

☑ Backup selections should be regularly checked.
Data selections must be regularly checked and updated to include new or changed data.

☑ Backup must include files currently in use.
The data backup routine must be able to backup open files. Most commonly used backup procedures (simple copying of data to alternative media/hard drives) are not able to backup files that are open, for instance when an application is in use or has not been closed before the backup initiates.

Email | Info@irontree.co.za
Website | www.irontree.co.za
Phone | 087 943 2278
Fax | 086 530 4443
Address | IronTree Internet Services CC, Unit 1, Westlake Square, Westlake, Cape Town

☑ Backup should be securely encrypted.
Data should be encrypted and password protected prior to being transmitted to the data storage platform. If one stores data on a memory stick or portable hard drive, it's likely that the data is not encrypted but is merely copied in its native format. Consequently, anyone with access to the backup media would have access to the information contained thereon.

☑ Backup reports should be automatically triggered.
Daily automated reports should be generated confirming the success (or failure) of the back-up process.

☑ Data must be stored in a safe place.
The off-site data centre must be a legitimate, secure, authentic data centre at a known physical location. The most secure data centres include facilities belonging to the major connectivity corporations, for example Vodacom, Internet Solutions, MTN etc. Legitimate online backup providers almost always rent "rack space" at data centres in this category and locate their storage platforms in these extremely secure environments.

☑ Backup solution must be redundant.
The data storage platform must be designed for redundancy. It's likely that, at some point in time, a technology component will fail, be this a hard drive, power supply or other critical component. It's crucial that the storage platform architecture allows for failure of critical components – or entire servers – without any risk of your data being lost.

☑ Data must be easy to recover.
Data must be accessible for easy recovery 24/7/365. If the volume of data required to be restored is large and may take excessive time to download, it's important that:

• The data centre is a local facility – this facilitates the physical delivery of required data if necessary.
• There is a local contact centre with agents who can assist with data restoration if required.

☑ Recovery testing must take place.
Test restore exercises should be conducted on a regular basis.

Making an informed decision on a new backup solution

Ask potential vendors the following questions:

☑ Once our backup is set up, do we need to do anything further?
It is important that backup does not rely on human intervention, as everyone makes the occassional mistake.
Where does our data backup reside? Data must be backed up to a secure and legitimate data centre.

☑ Do you keep previous versions of our backup?
It sometimes takes a few days to notice that data has been corrupted. If there is only a single backup of your data, then even if you recover your data it will still be corrupted. You need to be able to roll back to an older version of your data.

☑ Can you backup files that are currently being used?
Many backup solutions skip files that are currently being used (the files are marked as 'open'), but these are often the most important files.

Email | Info@irontree.co.za
Website | www.irontree.co.za
Phone | 087 943 2278
Fax | 086 530 4443
Address | IronTree Internet Services CC, Unit 1, Westlake Square, Westlake, Cape Town

☑ How well is our data encrypted?
Most providers encrypt your data. However, it is important that it is encrypted before it gets transmitted from the host computer to the data centre.

☑ How redundant is your backup solution?
It's not a case of if technology will fail, it's more a case of when technology will fail – your provider should plan for this.

☑ Is the process to recover data simple?
Losing your data is an extremely stressful scenario. Best practices dictates that data is stored at a locally based data centre and also that you can speak to someone in your own time zone and language if assistance is required.

☑ Will your provider lock you into an extended contract?
Legitimate service providers contract their services on a monthly subscription basis with a 30 or 60 day notice period.

How IronTree can assist you?

We backup and protect business data, so when disaster strikes (theft, corruption and viruses, natural disaster), we simply restore your data and your business can keep on running.

IronTree is a leading provider of secure online backup solutions to the South African business community. Established in 2007, IronTree partners with recognised software vendors including Sage Pastel, IQ Retail, QuickBooks, Sage VIP payroll and others.

Sign up for a free trial by completing the online application form here: https://www.irontree.co.za/html/register.jsp

Email | Info@irontree.co.za
Website | www.irontree.co.za
Phone | 087 943 2278
Fax | 086 530 4443
Address | IronTree Internet Services CC, Unit 1, Westlake Square, Westlake, Cape Town