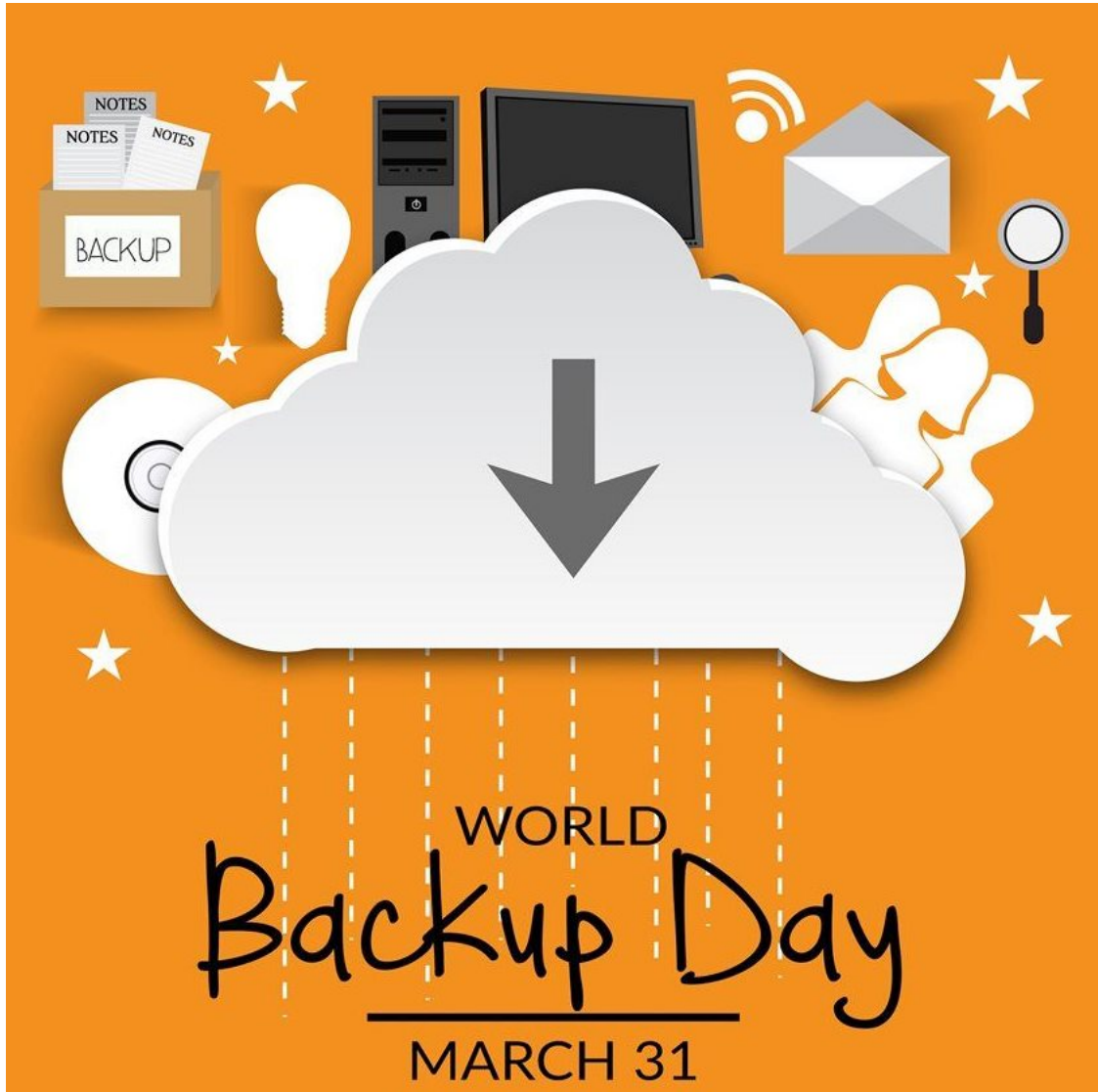


Backup your data...now!

31 March is World Backup Day and serves as a reminder to all businesses and individuals to make sure that all-important files and documents are backed-up.



With the implementation of The Protection of Personal Information (PoPI) Act 2013, many businesses realised the importance of data protection and started implementing structures and policies to ensure the requirements of the Act were adhered to.

“Even though backing up our computers and phones should be a regular task that is carried out and should fall part of any data protection policy, many SMEs don’t have systems in place,” says Anne-Marie Pretorius, managing director at Bizmod.

The World Backup Day [website](#) conveys some scary statistics, stating that 30% of people have never backed-up their files, one in 10 computers are infected with a virus each month and 113 cell phones are stolen or lost every minute.

Pretorius says that the statistics don't surprise her at all, and she would predict that in South Africa the numbers were even higher. "Many managers or business owners are either unaware of the necessity for a backup solution or they assume that their employees or IT support have taken care of this element."

Importance of data protection

As businesses have, and continue to, create a culture of data protection amongst their employees to comply with the PoPI Act, so should backing up of data form part of this process. Customers rely on businesses to protect and keep their information safe and this also includes ensuring that information they have shared is always available and accessible by the right parties.

"In the same way as organisations need to address employee behaviour to reduce the risk that it poses to the protection of personal information so too does behaviour play an integral role in understanding the importance of backing up information on all platforms," says Pretorius.

Here are a few key elements in adjusting behaviour in an organisation to meet data protection requirements:

- Management commitment and support is vital to instil a data protection culture to direct employee behaviour.
- The protection of data policy needs to be compiled with input and agreement from all relevant departments, ensuring acceptance of the policy and user accountability.
- Training encompassing all elements of information protection should be undertaken.
- People are often naturally resistant to change and so weaving change management into the process will aid employee buy-in.

For more, visit: <https://www.bizcommunity.com>