IS YOUR BUSINESS DUE FOR A SEASONAL I.T. HEALTH CHECK?

#1 Check All Your User Accounts

Check all your user accounts, licences and subscriptions. Are there people who have left the business in recent months? Are their email addresses still important to the business? Do the right people have visibility of these? Do you need to keep the licences and the subscriptions in their name? Or do you need to transfer them to other users?

If no one actively uses an email account – delete it. These are potential security risks.

#2 Backups

Have a good look at your backup history. When was your last backup and are your systems running smoothly?

If you notice any irregularities, you should talk to your IT support provider to assess your set up and address any issues.

When did you last complete a test restore?

#3 Hardware and Infrastructure

Have a good look at your infrastructure and inventory. Make a list of all the devices that have not run reliably in the past few months. Make sure you discuss the list with your team and plan to replace these. The cost of not planning accordingly is simply too high to ignore.

Dispose what you don't use, but do so responsibly. Recycle everything you can.

#4 Wiring

Check all the cabling. Messy wiring can lead to issues, accidental unplugging causing unnecessary downtime and data loss. Some checks to the wiring are required for compliance with existing regulations.

Make sure your IT provider has assessed, tested, cleaned up where necessary and documented all actions taken.

#5 Software

Do you still have legacy applications installed on your workstations that are not in use anymore? They can add unnecessary overheads, create conflicts, prevent updates to be installed and even become a security treat.

Identify these and discuss the list with your team as some may be used very infrequently but can still be crucial to some aspects of your business operations. Then remove from your system.

#6 Archive or Delete Old User Data

Same goes for all old "My Documents" folders on the server associated with users that are no longer with the business.

Review and delete archive on removable storage then delete from the server. Do the same with the stored email folders for closed employee accounts.

This will decrease the size of your company's back up. With cloud licensing a licence is required for disabled accounts.

#7 Shadow I.T.

Do your staff use applications like Dropbox or Google Drive that are not part of your company approved toolbox? Using duplicate services by some parts of the business can create serious issues down the track with multiple data copies, compliance and even client data breaches.

Evaluate the situation and work with your IT providers to ensure the job can be done without associated risk of shadow IT issues.

#8 Unstructured data

Through daily use and human factors data can be copied and saved in the wrong places. Do you have sensitive data saved in folders that are properly protected? Do you have data duplicated on private devices? How your team will know where to find the final version of each document? Do you have file naming convention in place? Is your team up to speed with the company's processes and access permission rules?

Discuss, document any changes and share. Complete a security audit on folders accessible on the network.

#9 Run updates on all devices

Check all - OS, applications, security.

Good IT service providers will make sure that you are up-to-date with all of these on all your devices. If you do not have an agreement in place that covers these, make sure all your staff check for updates and run these right now and make sure they continue to do so on a regular basis.

This is vital step to protect your business and your clients' data.

BUSINESS I.T.

If you haven't done an "IT health check" in a long time and you feel your systems do not perform as you need them to, you can ring us on **0800 248 277** or email **helpdesk@businessit.co.nz** and talk to our experts about our network audit packages.