# HOW CAN YOU BACK UP YOUR DATA SECURELY?

iStorage®

Sales and general enquires
Tel: +44 (0) 20 8991 6260
E-mail: info@istorage-uk.com

# EVERY ONE HAS AT SOME POINT LOST DATA.

**It could have been a stolen phone, a lost USB flash drive or a result of a computer crash.**

## WHAT EXACTLY IS DATA ENCRYPTION?

Backing up your data, that is, copying or archiving files, will give you the assurance of being able to restore lost data.

Personally identifiable information (PII), payment card details, intellectual property (IP) and email fall under an umbrella of highly valuable data sought after by cybercriminals.

Therefore, it is best to encrypt any data you want to keep confidential. Data can be backed up using a USB or HDD/SSD drive and can also be stored in the cloud.

Encryption can, in some ways, be likened to a padlock on a suitcase.

Without a padlock, you run the risk of anyone being able to open the suitcase and view or steal your belongings, especially when making stopovers.

With a padlock, the suitcase is securely closed wherever it travels and can only be opened by those with a key or a copy. Similarly, encrypting data will keep it confidential, even if it should fall in the wrong hands.

# HOW TO SECURE DATA IN THE CLOUD

If the data is stored in the cloud, control of the encryption key is important.

Although most cloud service providers will encrypt their customers' data, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff – much like leaving your house key under the doormat that half the neighbourhood knows about.

Moreover, if a hacker obtains the user's credentials, the breach will go unnoticed to the cloud service provider as they won't be able to decipher between a legitimate user from an attacker.

By encrypting the data yourself, you have full and secure control of the encrypted encryption key, which will ensure the data is kept confidential even if the cloud account is hacked.

Keeping the encryption key away from the cloud increases the number of security measures from just one authentication, the cloud account login, to as much as five-factor authentication.


# BACKING UP DATA IN THE MOST SECURE WAY POSSIBLE

In the worst-case scenario of a lost or stolen USB flash drive, hard drive or solid state drive, an encrypted PIN protected USB or HDD/SSD drive will negate the risk of your data being compromised.
Additionally, backing up valuable data onto an encrypted, PIN-authenticated drive can save you the trouble of losing access to important information during a ransomware attack, allowing you to quickly restore your data so that you're back up and running.

If the drives are only accessible by entering a unique 7-15-digit PIN, it will prevent unauthorised access to the data stored on the drive. With brute force limitation, if the PIN is entered incorrectly a designated number of times, all data previously stored in the drive is deleted and the drive is reset to factory default settings.

When power to the USB port is turned off, or if the drive is unplugged from the host device or after a predetermined period of inactivity, the drive should automatically lock to prevent unauthorised access.

Using a drive that can also be configured as a read only (write protect) will ensure the data is not modified.

Data is becoming increasingly valuable. Businesses and individuals alike should take the utmost precautions to protect their data.

Backing up data into the cloud or to an encrypted PIN protected USB or HDD/SSD drive will protect your data from being accessed or viewed by unauthorised persons and will ensure your data isn't lost forever.