iStorage®

Speedy sharing of data without compromising data protection

With the global rise of remote workers, delivery and postal services are busier than ever.

The burst of online shopping puts delivery services under greater strain, including FedEx, Amazon and UPS that have warned customers of potential delays.
In addition to increasing demand, widespread airline cancellations can also pose a significant operational impact on the scheduled distribution of mail.

When sharing sensitive information, some may opt for secure postal delivery. More likely though, in the digital age, if someone wants to share a highly confidential document, they will probably either email it, use a file sharing service or share it in the cloud. How secure are these methods?
Needless to say, there are far too many vulnerabilities to mention.

Studies reveal that cloud misconfigurations exposed over 33 billion records in two years.
If it's not hacks or technical issues, the other common cause of data leakage is human error. According to a study by IBM, 24 per cent of data breaches are caused by human error.

A secure alternative would be to post an encrypted USB. If postal services are delayed though, you may need to wait a while. In response to the prevalent concerns over data protection in the cloud, iStorage developed the revolutionary, patented cloudAshur, as a solution to encrypt, share and manage data stored in the cloud.

cloudAshur can also be used to encrypt data stored on your network or local drive, email attachments as well as data shared via file sharing services.

Seal your data before you send – always encrypt!

A recent study found that an alarming 43 per cent of cloud databases are not encrypted.
To ensure data privacy when faced with common threats, such as DDoS and malware attacks, data must be encrypted in transit and at rest.
Encryption cannot be dependent on the cloud service provider.

With server-side encryption, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff. Therefore, it is best for organisations to individually encrypt data stored in the public cloud. The user needs full and secure control of the encryption key in order to ensure the data is kept confidential even if the cloud account is hacked.

With cloudAshur, you have full control as you physically store the encrypted encryption key within a PIN-authenticated, AES-XTS 256-bit hardware encrypted USB module.
The module does not store any data. Rather, it acts as a key to encrypt and decrypt data stored in the cloud, on your network or local drive, email attachments as well as data shared via file sharing services.

Make sure only those authorised can see your censored letters

If your data ends up in the wrong hands, there is no guarantee the data will return to sender.
With cloudAshur, each authorised user will have a clone of the cloudAshur encryption module.

Using the iStorage KeyWriter software, all critical security parameters are copied, including the randomly generated encryption key and all PINs, between the Master cloudAshur module and as many Secondary cloudAshur modules as required. This allows secure and instant collaboration in the cloud, on a network drive, between authorised users, as well securely sharing encrypted files via email and file transfer services.

It also allows for multi-factor authentication, which is a highly recommended best practice for data protection compliance. If a hacker obtains the cloud user's credentials, the breach will go unnoticed to the cloud service provider as it won't be able to decipher between a legitimate user from an attacker.

On the other hand, the cloudAshur encryption module increases security measures to an unprecedented five-factor authentication, as the encryption key is kept away from the cloud.

The post office of electronic data

Using iStorage's Remote Management Console, those responsible for cloud and data security in the organisation can manage and monitor cloudAshur devices centrally.
Administrators can temporarily disable or reset cloudAshur encryption modules, restrict file types, monitor users' log files, display user's location, as well as enable geo-fencing and time-fencing restrictions.

The cloudAshur solution, which works with all the main cloud providers, allows users to encrypt data in the most secure way possible, share encrypted data with authorised users in real-time, and manage and monitor cloudAshur devices centrally.

cloudAshur can also be used to encrypt data stored on a PC/Mac or local network, as well as encrypt data shared via email or file sharing software services.

There is no need to disrupt business continuity and productivity waiting for mail to be delivered.
Neither is there a need to ever compromise data protection, risking data breach fines, adverse publicity and even job losses, by insecurely sharing data electronically.

With cloudAshur, you can share files in seconds, safe in the knowledge it is kept confidential in the most secure way possible.

iStorage®

Tel: +44 (0) 20 8991 6260 | www.istorage-uk.com | e-mail: info@istorage-uk.com