5 tips for protecting your data when working remotely

As the number of remote workers continuously rises, ensuring data protection can prove challenging. Organisations have the added pressure of maintaining business continuity whilst adhering to data protection regulations. Strain is added for those dealing with highly sensitive information shared within a large organisation or with third parties. How can organisations protect data from attacks and human error, as well as manage access to confidential information?

Here are iStorage's five tips:

1 Keep a safe back up of sensitive information
- protect against ransomware

All important files should be regularly and securely backed up. Backing up valuable data onto a PIN-authenticated, hardware encrypted USB flash drive or HDD/SSD ensures business continuity in the event of a hard drive crash, lost or stolen computer and ransomware attack.

Using an encrypted drive for backing up data is essential. For ultimate protection, the selected drive should preferably have an on-device crypto-chip offering real-time AES-XTS 256-bit hardware encryption with a FIPS PUB 197 validated encryption algorithm. As a result, if the encrypted device, such as a USB flash drive or hard disk drive, is lost or stolen, it will not result in a data breach and the exposure of confidential client or company data.

2 Transport files securely

Securely carry work home with you using a PIN protected, encrypted USB flash drive or HDD/SSD. In the worst-case scenario of the drive getting lost or stolen when employees transport files or work out of the office, an encrypted drive as described above will allow organisations to avoid the risk of their data being compromised.

Moreover, 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. Another feature worth considering is 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.

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 read only (write protect) will ensure the data is not modified and means viruses cannot be brought into the company infrastructure.

3 Encrypt data stored in the cloud

The cloud is often the preferred option for remote working. However, cloud security is a common major concern, meaning most businesses will hesitate to store any highly confidential information in the cloud. Is there a way around this issue?

To ensure data privacy when faced with common threats, such as DDoS and malware attacks, data must be encrypted in transit and at rest. Data encryption renders stored and transmitted data unreadable and unusable in the event of theft or inadvertent data leakage.

Encryption cannot be dependent on the cloud service provider (CSP). With server-side encryption, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff. It is therefore 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. Having your own key management system will not only give you more control of encryption keys but it's also more convenient for those using a multi-cloud solution.

An ideal solution to control the encryption key is to quite literally remove it from the cloud and physically store the encrypted encryption key within a PIN-authenticated USB module, such as the iStorage cloudAshur. The module will not store any data. Rather, it will act as a key to encrypt data and access any data in the cloud. It can thus be used to securely encrypt confidential data stored in the cloud, on a local computer or network drive, sent via email or sent using a file sharing service.

4 Ensure authorised access to data

Using specific software, such as iStorage KeyWriter, all critical security parameters between the primary encryption module and as many secondary encryption modules as required can be copied, including the randomly generated encryption key and all PINs. Only those with a copy of the encryption key will be able to decrypt the shared data. This allows for secure and instant collaboration in the cloud between authorised users, regardless of location.

Businesses need a clear procedure that all staff follow to uphold adherence to data protection regulations, even more so with the rise of remote workers. Multi-factor authentication 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.

5 Manage access to data remotely

Handing authorised staff an encryption module, such as the cloudAshur, will contribute to reducing the risk of data loss due to human error. Still, this does not entirely eliminate the possibility of such an occurrence. For example, an individual may lose the encryption module or be dismissed and keep the device. This is where central management is needed.

Those responsible for cloud and data security in the organisation should be able to monitor file activity, set geo-fencing and time fencing restrictions, encrypt file names and disable users' access to the data remotely. This will go a long way in eliminating security risks in the cloud and help managers have full visibility and administration of sensitive data and user access.

These measures will contribute to maintaining business continuity, upholding compliance to data protection regulations and eliminating any complexity of remote working.

At iStorage, we can assist organisations with remote workers to: (1) safely transport and back up data using our datAshur or diskAshur range, and (2) securely share and manage data in the cloud using our cloudAshur solution.

To discover the ideal solution for your business, please

Get in touch

iStorage®