USB Flash Drive Policy for use with clients

CYBERCO

Client USB Flash Drive Policy:

You must only use company issued CyberCo USB flash drives. Flash drives will be password protected. Drives for external use will contain antivirus software. When transporting any sensitive data, the flash drive must also be fully encrypted.

If you do not know where a USB flash drive has come from, you must never use it in company networked workstations. You can take any USB flash drive you are uncertain about to reception.

The reception staff have a standalone machine. They can help you test any flash drives. Antivirus software will be up to date to check for malware and viruses.

Similarly, if you find a company USB drive that does not belong to you, take it straight to Reception. The reception staff will try to reunite it with its owner.

All USB flash drives from third party vendors or clients should be fully scanned before use. It is safe to use a company laptop to scan these as auto-play is set to off. You can also get these scanned by the reception staff.

If your USB flash drive is either lost or stolen, you must immediately report it to the Data Security Officer. They will aim to help you recover the drive and assess if there has been a data breach.

Under no circumstances should you ever use a personal USB flash drive on any work device.

Reception keeps a set of spare USB flash drives; you can borrow one of these at any time. Reception staff will ask you what you will use it for, so that they can issue the appropriate flash drive.

Activate the antivirus software on your flash drive before using it with an external device. This includes devices belonging to clients, providers or external contractors. The antivirus scan must be completed before you transfer any files.

[This policy was reviewed on 08/23/2023 and is set to be reviewed on 02/23/2024.]