USB and Flash drive security policy best practices checklist

USB Flash Drives have gained popularity due to their huge data storage capacity, simplicity of use and portability

WinEncrypt

USB Flash Drive Security Policy – Best Practices Checklist

USB Flash Drives have gained popularity due to their huge data storage capacity, simplicity of use and portability. The problem with mobile devices, however, is their proneness to theft and thereby vulnerability to data theft. The use of USB Flash Drives might simplify life but unless adequate security measures are taken, the organization is left vulnerable to not only the threat of data loss but of legal action from the affected parties.

Fortunately, there are some easy steps that can ensure the safety of all portable devices. A security policy being adopted by an organization means that all its staff members are obligated to follow the basic steps required to ensure safety of their laptops and USB Flash Drives. Some of the best practices for formulating a USB Flash Drive Security Policy include:

☐ Ensure that your USB flash drive encrypts the data as soon as it is stored in the device with the full disk encryption feature. This will not only restrict the use of the drive to computers that have compatible encryption software but also help avoid unauthorized access to data.

☐ The data stored on a USB flash drive should be put through regular audit trial.

☐ Organizations should circulate notices to all the mobile device users to restrict the use of USB flash drives at particular places.

☐ Every organization should have a security policy regarding personal storage devices, including USB flash drives, which should be a part of the disaster management policy.

☐ There should be a centrally managed database for all portable storage devices issued by the company to keep a track of the use of these devices inside and outside network accessibility.

☐ Make all USB flash drives password protected in order to thwart unauthorized access of the confidential data.

☐ USB flash drives also come with biometric finger print identification software that helps recognize the legitimate user. The software scans finger prints, authenticates the user and only then allows him/her to access the data.

☐ Another simple measure that users of portable storage devices can implement is to chain the device so that it does not get lost during outdoor use.

With advance technology solutions for data storage available, the use of the USB flash drive and other portable devices is only going to increase. The main reason for the increasing demand is that these devices are fairly durable, owing to the absence of internal moving

components. As long as legitimate users comply with the basic security practices and safeguard their company's data, the USB flash drive can be a real asset to business.