Queensland Law Society®

QLS Guide: Removable data storage best practice for law firms

A quick reference guide

March 2019

USB Storage device – best practice guide

Note: This is a draft guide for the management and use of USB drives by law firms. It may be used and modified without restriction provided authorship is attributed. Compliance with this guide does not guarantee that loss or damage will be avoided. Each organisation should design and implement policies based on their individual circumstances using appropriately qualified professional advice.

What is the issue?

USB drives are small, cheap and ubiquitous. They are also dangerous from a data security perspective, being a common factor in data loss reported worldwide. (US figures indicate that device loss is the second most prevalent cause of reportable incidents in the healthcare sector (here), and has been for many years).

As many as 7,000,000 pages of text can fit on a single 1Terabyte drive, and copied data is often left on the device once the need for it to be there has passed. If USB drives are used without control, they can be easily lost, and accurately identifying the data contained may be very difficult.

USB drives are also very easy for a hostile insider or outsider to misuse. A device containing attack software can be inserted whilst standing at the reception counter. A departing employee might copy vast amounts of confidential material. The list of potential scenarios is a long one. None of these risks can be eliminated altogether, but some basic policies can improve the situation significantly.

The primary risks

Policies should address three main areas of concern:

- USB devices can be used to copy large volumes of data which is then removed from the organisations' control. Copying the data may be for legitimate or malicious purposes.
- USB devices are easily stolen or lost.
- USB devices may be infected with malware which can infect the network even if no files on the drive are opened.

Encryption

Encrypted data is scrambled so that it cannot be easily read without a missing string of characters, called a Key. Even if it is lost or stolen, strongly encrypted data is safe from casual intrusion. The specifics are complicated, but the take away message is that simple, robust encryption is a mainstay of any information security strategy.

In most cases encryption using basic software (such as the Bitlocker program included with Windows Pro or Enterprise) should be sufficient. Implementation can be as easy as "right clicking" a USB drive and assigning the password. For a range of other alternatives for use with physical drives see: here. For cloud encryption see: here.

There are many different encryption standards in use, the "gold standard" in 2019 being AES-256 (the higher the number on the end the more secure the data is, but the slower it will be to process).

As the most likely threat is not a highly targeted attack by a pro-hacker, but a casual look from someone who finds it on the bus, the best form of encryption is the one that your staff will actually use. To ensure that they know the importance of encryption and how to use it, training should be given.

Certified/managed USB devices

For high security applications, or compliance with contractually mandated standards such as ISO 27001, certified encryption might be required. One of the most recognised certification standards is FIPS. A FIPS-2 device (certification levels go from 1 – 3) is the minimum required by many US government agencies for storing organisation data.

The next level of protection is the use of centrally managed USB devices where the policies are enforced automatically and administered by the firm's IT department. This is usually deployed as a part of a more general endpoint management system.

Policy design and implementation

Like any policy, a rule is useless unless everyone in the firm is told about the risk and why the measures are in place. The rule must apply to everyone, be known to everyone and explained.

Even the most senior partner needs to follow the protocol for it to be effective.

No private USB devices should be connected to the firm network under any circumstances. This policy should be express, and communicated on induction and as part of ongoing training.

Preventing hostile parties misusing USB ports

Unused USB ports on all network-connected devices accessible in public areas (such as desktop computers, laptops, screens) should be disabled and fitted with a lock.

Insider misuse of USB ports is less easy to manage. Spare ports can be disabled (the method varies slightly depending upon operating system version) but this does not prevent someone unplugging a device and using that port.

Ensuring the network logs data events, and ensuring that staff cannot access data they do not need is the most practical way to manage hostile insiders. More comprehensive threat detection systems can also identify unusual activity on the network, but these are not common in smaller organisations.

Please see the Annexure for a draft USB policy. This should be tailored to your organisation's requirements.

Note: Third party hardware and software referred to in this document has not been independently reviewed or tested by QLS, and is not warranted to be fit for purpose in any individual organisation's computing environment. Firms should rely upon their own professional advice prior to purchasing hardware or software.

Enquiries: David Bowles
Direct line: 3842 5937