

# 5.6 Managing removable media

---

## What is removable media?

Removable media is storage media which is designed to be removed from a computer. The earliest forms of removable media were paper data storage media like punched cards and tape. They were followed by magnetic tapes and floppy disks which have now largely been replaced by optical disks (including Blu-ray Discs, DVDs and CDs) and memory cards.

Removable media also refers to removable storage devices such as flash devices (memory sticks or USB sticks) and removable hard disk drives.

iPods, PDAs, digital cameras, smartphones, Bluetooth and MP3 music players are other examples of technology that use removable media devices.

The storage capacity of the media depends on the type and age of the removable media. Flash drives and removable hard drives, for example, can store gigabytes of data.

## Uses of removable media

There are two main ways removable media is used:

1. for off-line storage within the office environment or at a storage location
2. to enable data to be copied, moved around or accessed away from the office.

## What are the advantages of using removable media?

Removable media is low cost, portable and simple, allowing people to copy, store and carry large quantities of data easily between locations. Employees can share information easily and access it from a variety of locations, which can increase the organisation's productivity.

## What are the risks associated with using removable media?

There are a number of risks associated with the use of removable media.

- The ability to transfer information quickly, huge storage capacities and the portability of the media means that users can copy or remove corporate data from the organisation quickly and with less chance of being detected. This puts the confidentiality, integrity and availability of corporate information at risk.
- Devices are easily lost, misplaced or stolen and the data often has no access controls. This can cause public embarrassment and may cause the organisation to breach legislation e.g. privacy legislation.
- Removable media devices can open pathways in the organisation for viruses, malware and inappropriate content which can lead to business disruption and public embarrassment.
- Information 'silos' are perpetuated. The information held on removable media is not available to the whole organisation.
- Records are often copied multiple times onto different removable media, and it is unclear what information is original and what is duplicated.

- It is difficult to apply disposal decisions to the information on removable media. This often results in the over-retention of corporate information, which is costly and raises additional risks for the organisation.
- Locating and retrieving corporate information for discovery orders or *Government Information (Public Access) Act* requests is complex, as removable media must also be searched.
- Using removable media as the primary location for information and records can mean the data is not backed up regularly and changes made to the data on removable media may not be reflected in the online data (thus creating two versions of information or records).

### **Additional risks associated with using removable media for the long term storage of records**

Removable media is increasingly being used by organisations for longer term storage of digital records. This presents some additional risks to those described above:

- The longevity of CDs, DVDs and USB sticks is questionable. If they are not stored with optimal temperature and humidity they may degrade quickly.
- Removable media is easily damaged. For example, CDs and DVDs can be easily scratched and magnetic media can be affected by magnetic fields.
- There is no centralised backup for removable media.
- Often the labelling of the media is haphazard and inconsistent, which can cause problems with retrieval and reuse of the information.
- If encrypted or password protected, the encryption keys or passwords may be lost over time, rendering the data inaccessible.
- Removable media is often overlooked during migrations and may become obsolete; 'out of sight, out of mind.'

#### **The perils of using removable media**

##### **Scenario**

An organisation was moving and staff members were clearing out some old cupboards. Three floppy disks were found in the back of the cupboard. These were labelled Part 1, Part 2, Part 3, but there was no other identifying information. No disk drives were available in the organisation to read the data, so the staff members threw the disks into a dustbin.

Later it was discovered that the disks contained vital corporate information that was not backed up and was not available elsewhere.

##### **Reported incidents from the United Kingdom:**

- In January 2009, a health worker in Lancashire lost a memory stick containing the medical details of more than 6,000 prisoners and ex-prisoners. The data was encrypted, but the password had been written on a note attached to the stick.
- In September 2008, discs were taken from a secure area at the RAF Innsworth in Gloucestershire. The discs contained 500 highly sensitive files containing vetting information for personnel including names, addresses, bank account details and information about extra-marital affairs, debts and drug use.
- In August 2008, a Home Office contractor admitted losing a computer memory stick containing information on 84,000 prisoners in England and Wales. It also held personal details of about 10,000 prolific offenders.

- In July 2008, the Ministry of Defence confirmed that 121 computer memory sticks and 747 laptops have been lost or stolen in the past four years. Five of the memory sticks contained secret data.
- In November 2007, HM Revenue and Customs (HMRC) lost two computer discs containing unencrypted child benefit records, including the personal details of 25 million people. They were sent via internal mail to the National Audit Office and never arrived.

### **Is removable media suitable for the storage of backups?**

Removable media is generally suitable for storing backed up information as it is a copy of digital information intended to be kept for disaster recovery purposes for a short time only. Security measures should still be in place for backups.

### **Measures that should be in place to protect information on removable media**

While it is a good idea to discourage staff from transferring or keeping digital information on removable media, it can be difficult to prevent users from bringing devices and media into the corporate environment. Therefore, efforts should be centred on managing the risks associated with the use of removable media.

Measures that can be taken by the organisation include:

1. Including the risks of removable media in organisational risk assessments so that the risks are clearly delineated and treatment measures identified and implemented.
2. Creating policies and procedures for the management of removable media and integrating these into the organisation's security framework and training programs. Policies and procedures should include topics such as the use of non-corporate removable media on corporate machines, the type of information that can be stored on removable media and what can't, the removal of information from removable media when no longer needed, required approvals, use of encryption or password protection and physical security. They should be communicated to and acknowledged by users so their responsibilities are well understood.
3. Identifying what information is particularly sensitive, confidential or private in the organisation and ensuring that this has strong access controls. Employees who handle this information need to be fully aware of the risks of removable media, when it is inappropriate to use these devices and if it is used, what security measures are required.
4. If appropriate, implementing physical security solutions to prevent removable media being used. For example, logging the amount of data that a user downloads or configuring computers to restrict or prevent the use of devices such as flash drives.
5. Implementing access controls to protect information on removable media. For example, introducing password protection and locking of data after a number of password attempts or encryption software that is easy to use and that will work on a range of devices and removable media.
6. Periodically auditing and testing to ensure the effectiveness of controls.

### **Additional protection needed for long term preservation**

With regard to ensuring the long term preservation of valuable digital information measures can also include:

1. Outlining policy decisions regarding the use of removable media for storing records in the organisation's records management policy. **State Records**

**strongly recommends that removable media is used as a last resort only and advises that long term or archival records should be stored on networked servers or online spinning disc storage systems.**

2. If removable media must be used for long term preservation, specifying in records management procedures the environmental conditions they should be stored in, handling requirements, copies required for disaster management purposes, metadata requirements, any access controls required, de-encryption requirements, monitoring requirements and refreshment, replication or migration schedules.
3. Ensure that responsibilities are assigned for the management, regular monitoring and safeguarding of removable media used for long term preservation.
4. Physically labelling any removable media used for storing digital records to indicate what it contains, even if the storage is only expected to be short term.

### Further advice

For further information on the protection and handling of removable media, see:

- National Archives of Australia, *How do I protect and handle optical discs?* Available at: <http://www.naa.gov.au/records-management/secure-and-store/physical-preservation/faq/optical-disks.aspx>
- National Archives of Australia, *How do I protect and handle magnetic media?* Available at: <http://www.naa.gov.au/records-management/secure-and-store/physical-preservation/faq/magnetic-tape.aspx>

### Acknowledgements

Ahlberg, Magnus 'Addressing the risks of removable media', *Continuity Central*, 11 March 2005, available at: <http://www.continuitycentral.com/feature0184.htm>

BBC news, *Previous cases of missing data*, available at: [http://news.bbc.co.uk/2/hi/uk\\_news/7449927.stm](http://news.bbc.co.uk/2/hi/uk_news/7449927.stm)

Rostern, John, 'Dangerous devices: the huge storage capacity of computer-removable media poses a considerable threat to sensitive corporate data', *Internal Auditor*, October 2005, available at: [http://findarticles.com/p/articles/mi\\_m4153/is\\_5\\_62/ai\\_n15756369/?tag=content:col1](http://findarticles.com/p/articles/mi_m4153/is_5_62/ai_n15756369/?tag=content:col1)

Tharp, Tom, 'The unique benefits and risks of USB mass storage devices', *ISACA Journal*, Volume 2, 2007, available at: <http://www.isaca.org/Journal/Past-Issues/2007/Volume-2/Pages/The-Unique-Benefits-and-Risks-of-USB-Mass-Storage-Devices1.aspx>

Wikipedia, *Removable media*, 31 August 2010, available at: [http://en.wikipedia.org/wiki/Removable\\_media](http://en.wikipedia.org/wiki/Removable_media)