Client data protection

Securing personally-owned hardware and media

Version 3.3 January, 2020

Contents

1 Preface

1.1 Background and purpose

This document outlines options and recommendations for adequately securing your client and business information maintained on personally-owned computers and portable data storage devices.

1.1.1 Why is this so important?

The protection and security of client and confidential information should be a priority for everyone. We understand the trust clients place in us depends on our protection of their confidential information.

News reports and complaints to the federal and provincial Privacy Commissioners highlight issues related to computer and portable data storage device theft. Client and personal information on these computers is at risk for identity theft or other inappropriate access and use. These incidents often occur as a result of office or home break-ins, or theft from vehicles or other public places. Such incidents are damaging to the reputation of the company and/or individual involved when client confidence is affected.

It's important to ensure that your business is appropriately protecting the personal data of clients and prospects, and that it is in compliance with all applicable privacy laws (e.g., PIPEDA – Personal Information Protection and Electronic Documents Act).

1.1.2 Greater mobile technology risk

For mobile technology, the risk of theft is even greater. Working away from the “bricks and mortar” office means that you are also working outside of traditional physical security layers. As a result, you should consider reassessing the privacy and security risks associated with working remotely, or traveling with mobile technology that has client information stored on it.

1.1.3 What should I do to protect my clients’ data?

You should take appropriate steps to safeguard confidential information, whether it’s your own, or that of your clients. This document discusses the risks associated with keeping data on computers and portable data storage devices, and offers practical advice on how to reduce these risks. Once you have decided on which steps you will take to implement security measures, all components of that solution (e.g., additional software, system BIOS, operating system upgrades, patches, portable storage device firmware or software) should be kept up-to-date to ensure that your protection solution continues to function as expected.

Implementing some of these options may require significant technical capability. You are encouraged to consult with your technology provider for assistance in completing this process. Also, be sure to properly 'shut down' your machine when it is unattended or being transported. If you only “logoff”, "lock" or leave the device in “standby” or "sleep" mode, any additional security measures could be ineffective. If your computer is lost or stolen and it was not "shut down" or does not have data protected, you may be required to notify those clients whose information was stored on the machine.

1.1.4 What are the benefits?

Appropriately securing the data on your computer(s) and portable data storage devices will help protect client information in the event that your computer(s) or portable data storage devices are lost or stolen. You can confidently assure clients who are concerned about the security of their personal information that you are taking appropriate measures.

1.2 Computer security: the whole picture

There are many factors in a sound technology security policy. This document outlines options for implementing a strategy to deal with **data protection** on **computers, portable data storage devices, and removable media**. A more complete list of other aspects of computer security is provided below.

Physical security — Ensuring computers are located in facilities that are adequately secure and any portable storage devices are stored in a location accessible only to authorized personnel.

Physical device protection (particularly for laptops) — This includes physical protection measures such as security cabling.

Authentication and authorization ID protection — Ensuring all users of a computer confirm their identity and are only authorized to see what they are required to see to fulfill their business role. Ensuring portable storage devices require the user to confirm their identity before accessing data stored on the device.

Idle management — Verifying the state the computer or portable storage device is left in if unattended, and not explicitly secured, for a period.

Computer sharing — Authentication and authorization practices related to regularly sharing a computer across multiple users.

Operating system and key software patch management — Keeping the operating system and other key software suites, such as MS Office, up-to-date with the latest security patches and releases.

Virus protection — Having it installed and active with the latest virus ID files. These products should be running in a "live scan" mode where they are proactively scanning files for viruses, as well as running periodic full scans.

Spyware/malware protection — Having it installed and active with the latest spyware/malware ID files. Some newer portable data storage devices, such as USB flash drives, support onboard malware protection to ensure that malware is not passed from computer to computer.

Network firewall protection — Implementing a hardware, software or combination firewall to protect computers regularly connected to high-speed Internet from outside attack.

Computer data protection — Protecting data saved on the computer from malicious disclosure in the event of computer theft.

Portable data storage and removable media data protection — The same outcome as computer data protection, but extended to data copied from the computer onto removable media such as a CD, DVD, diskette or portable storage devices (i.e., USB flash drives and portable hard drives).

Email/instant messaging protection — Protection from virus/spyware/malware attack initiated through the receipt of infected emails.

Wireless access management (including all types of access, such as 802.11x, Bluetooth and 3G) — Proper configuration and securing of wireless services to ensure that network signals cannot be inappropriately intercepted by others.

Proper data disposal (in the event of a sale or donation) — Ensuring data no longer required has been adequately destroyed so it can't be recovered by others who eventually come in contact with the media.

2 Computer data protection options

Full hard drive encryption is now mandated on all devices that will be interfacing with corporate systems or storing client data. A selection of commercial products, as outlined below, are recommended options to encrypt hard drives.

Encryption uses software installed on the computer to encrypt all data stored locally on the hard drive. It turns current data on the hard drive into an incomprehensible code that can only be viewed by those able to enter the correct password.

Full drive encryption is most often chosen in the industry as an effective way to protect sensitive data on computers that are stolen. The real advantages of this type of solution are:

- Robustness/completeness
- Low administration (once installed and configured) –transparent to the user, except at boot-up
- Does not rely on the user to protect the right information – all data is automatically protected
- Protects temporary files created by software
- Is universally applicable as a solution for multiple, disparate types of computers

It's important to note that all of the options presented below may require you to create, maintain and remember another set of password credentials (other than those you currently use to log on to your computer and/or local area network). For these solutions to be effective, it's important that you create a different password than the one you currently use to access that particular computer.

OS	Option
Windows	BitLocker (included in Windows 7 Ultimate/ Windows 8.1 Pro, and Windows 10 Pro)
Mac	FileVault2 (included in Mac OSX, free)

3 Portable data storage options

Portable data storage devices:

- Are not part of the computer itself, but rather can be made accessible via the computer by attaching them, typically via USB connection
- While attached to a computer, present themselves, and are managed like, another hard drive
- Are compact and convenient enough to easily transport from location to location. These devices typically come in one of two types:
    - **Portable hard drive –** A traditional hard drive technology (similar to that found in your computer) with additional on-board power management and disk controller circuitry to support USB connection to a computer.
    - **Flash memory drives** (i.e., thumb drive, memory key, etc.) **–** Very small, flash-memory based devices with additional on-board power management circuitry that utilizes flash memory to simulate hard drive storage.

3.1 Point-of-purchase questions

When considering the purchase of a portable data storage device, ask the vendor or retailer the following questions:

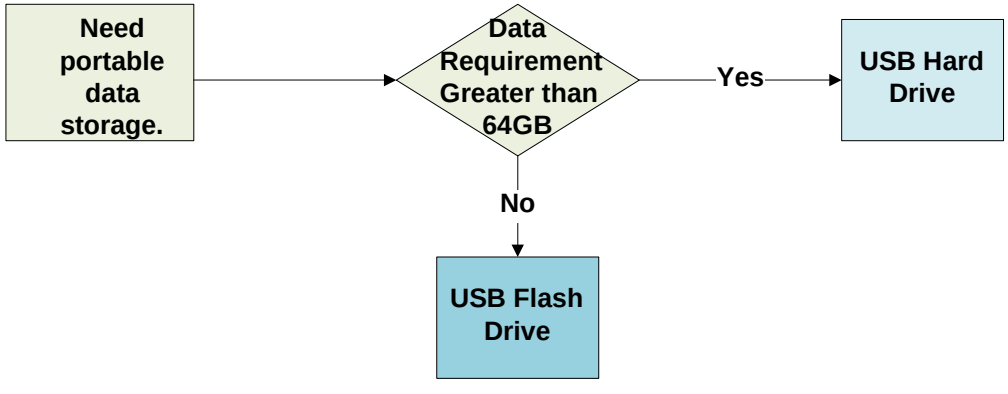
1. **Does the device support encryption of all data stored on it, without the purchase of additional software?**
2. **Is the encryption approach hardware-based?** Typically, hardware encryption of similar cipher strength is substantially more secure than a software alternative.
3. **Does the encryption approach support minimum cipher strength of 256-bit AES (Advanced Encryption Standard)?** Anything less powerful may put your data at unnecessary risk.
4. **How transparent is data encryption management to the user?** Does it encrypt/decrypt data stored on the device without interfering with or requiring explicit management by the device user (other than initial setup and ongoing authorization for access)?
5. **Does the device support the use of a strong password?** Are there any password entry restrictions for the device that would prevent the user from setting up a strong password (minimum 8 characters, combination of letters (mixed case), numbers and symbols) to authorize use?
6. **Does the device support lockdown or self-wipe after a defined number of invalid password attempts?** Some portable storage devices support on-board tracking of a defined number of consecutive invalid password entry attempts, after which the device is either:
    - Locked down from any further unrestricted authorization attempts and/or use, or

- Initiates an (unrecoverable) wipe of all data currently stored on the device, based on the assumption that it has fallen into unauthorized hands.

The most sophisticated of these devices permit users to configure the number of invalid authorization attempts before this security operation is carried out.

7. **Does the vendor provide any central management services or alternative approaches to support authorized device password recovery, should it be forgotten?** Passwords, when not used regularly, can be easily forgotten. In the case of an encrypted portable storage device, if the password is misplaced or forgotten without a recovery alternative, access to data previously stored on the device could be lost forever. Some vendors provide, as part of the purchase of their devices, access to a central management console or telephone support services to assist the registered owner/user of the device in regaining access to data stored on the device in the event of a lost or forgotten password.

3.2 Portable storage device selection



It should be noted that USB flash drives come in sizes of up to 256GB, but the price point beyond 64GB is more expensive and it becomes most economical to purchase a portable hard drive in the 1TB+ range (1 Terabyte (TB) is approximately 1,000GB).

3.3 Encrypted USB flash drive options

If you are considering purchasing a USB flash drive (i.e., thumb drive, jump drive, memory key, etc.), typically in the 1GB to 256GB size range, suitable hardware-encrypted options include:

- **SanDisk Cruzer Professional** http://www.sandisk.com/products/usb/drives/
- **Kingston DataTraveler Secure devices** http://www.kingston.com/us/usb/encrypted_security
- **CE Secure Vault FIPS Flash Drive** https://cmsproducts.com/encrypted-flash-drives/

3.4 Encrypted portable USB drive options

If you are considering purchasing a portable USB drive, typically in the 1TB+ size range, suitable hardware-encrypted options include:

Lenovo ThinkPad USB Portable Secure Hard Drive
https://www.lenovo.com/us/en/accessories-and-monitors/memory-and-storage/c/memory-and-storage?q=%3Aprice-asc%3AfacetAcc-Type%3ASecure+Hard+Drives&uq=&text=#

3.5 Encrypting any portable drive

Many hard drive encryption packages that encrypt your primary drive will also encrypt external drives and USB devices. Windows BitLocker instructions can be found here, and Apple OSX instructions are here.

3.6 Using USB-based portable storage devices safely

USB-based portable storage devices that can be easily connected to different computers introduce the risk of cross-computer virus and/or malware infection, as outlined in the following Public Safety Canada bulletin entitled '*Increased activity of malicious code spreading using removable devices*': http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2008/in08-007-eng.aspx

To minimize the risk of such cross-computer infection, and potentially loss of backup data stored on these devices, it is prudent to follow the first two steps outlined in the bulletin:

1. Disabling the AUTORUN features on all computers using this and other shared portable storage devices.
2. Regularly scanning all data stored on any portable storage device with a reputable antivirus/malware product before accessing any of the files.

4 Removable media options

Storage of data on removable media (i.e., optical CD or DVD) poses unique challenges:

1. The media is mobile, making it easy to misplace, remove or transport with little or no detection.
2. Protection of the data must be accomplished **prior** to writing it to the media, as this media provides no on-board protection capabilities.

The first line of defense is good physical security. Ensure that any removable media that contains backups or copies of sensitive client information is stored in a secure location only accessible by authorized personnel. Physical security does not protect removable media while in transit to a secure storage location, nor is it applicable for items that have been misplaced or inappropriately discarded. To ensure an adequate level of protection, data should be encrypted prior to being written to removable media. This can be accomplished through several approaches:

1. **Document level encryption –** Uses the native features of the tool that creates and manages a particular document type (such as MS Office or a PDF writer) to encrypt the content of the document and assign a password.
2. **Multiple document and/or folder archiving and encryption –** Uses a data archiving tool (such as *WinZip*) to create an encrypted archive that contains multiple files, or even folder(s) of files, and assigns a password for authorized access to the archive.

   Note: With both of the above options, it is important to select an adequately secure encryption technique to ensure that the data encryption is sufficient. For instance, basic MS Office document encryption is not terribly secure. If encryption options are permitted within the product, select at least a 256-bit AES level of encryption and provide a strong password to ensure adequate protection. MS Office 2000+ supports AES encryption, but only at 128bit strength. WinZip supports 256-bit AES encryption natively. For more information about encryption levels available with Microsoft, visit: http://technet.microsoft.com/en-us/library/cc179125(v=office.15).aspx

3. **Commercial endpoint security encryption software –** Many commercial encryption software vendors not only encrypt data stored on the hard drive, but have the capability to extend this encryption to any data written to portable data storage and/or removable media connected to the encrypted computer.
4. **Data backup software –** Most commercial data backup software packages support writing of backed up data to removable media, and encryption of this data prior to placing on the removable media.

Here are some other things worth considering in the secure handling of removable media:

- Properly label removable media to remind yourself of the importance and classification of data stored on discs
- If transporting removable media while traveling, do not pack it in checked luggage. Always keep them in your carry-on bag.

4.1 Options summary

	OPTION 1 Document-level encryption	**OPTION 2** Archive encryption	**OPTION 3** Encryption software	**OPTION 4** Data backup software
Level of protection	**GOOD** (if secure encryption technique chosen)	**EXCELLENT** (if secure encryption technique chosen)	**EXCELLENT**	**EXCELLENT**
Typical costs	**FREE** (features in existing software)	**$30 - $40**	(See section 2 for more information)	**$35 - $90**
Pros	Uses features in existing, familiar software No additional software required	Allows a single password to authorize access to multiple files or folder(s) In addition to encrypting the data, compresses it as well	A single product may be able to achieve both computer and removable media data protection Once logged into the computer encryption and decryption is transparent to the user. Most products support very secure levels of encryption	Most products support very secure levels of encryption Can also be used to regularly backup critical files and configuration on the computer
Cons	Day-to-day inconvenience as authorization is required every time a document is opened Have to manage passwords on a document by document basis • Some software may not support native encryption of its user document types	May require specific archive product to access data Competing archiving products may not be able to open an archive that has custom encryption	Encrypted data on removable media may only be accessible from the computer (running the drive encryption software) where the original write of the data occurred	No benefit over option 3 (and additional software to manage) if pursuing full drive encryption for computer data protection Proprietary backup file data formats require a valid installation of the backup product before the data on the removable media is accessible
Ease of use	**FAIR** Uses a feature in familiar software, but passwords are managed on a file-by-file basis	**GOOD** User must point and click to select files and folders to encrypt	**VERY GOOD** Access to data on removable media is transparent, but only via the computer where the original write of the data occurred	**GOOD** Excellent encryption, but proprietary backup file data formats make access to the data dependent on an installed, configured version of the backup software
Compatibility	**VERY GOOD** Works on all devices that support the file type. Typically this is MS Office, which is widely used.	**GOOD** Works on any device that has the right archiving software.	**POOR** Works only on devices where the content was originally encrypted.	**FAIR** Works only on workstations that support the same backup utility.

5 Appendix A: Glossary of terms

BIOS (Basic input/output system) **–** BIOS refers to the software code stored on firmware ROM chips on the computer motherboard that runs on a computer when it's first powered on. The primary function of the BIOS is to prepare the machine so other software programs stored on various media (such as hard and optical drives) can load, execute and assume control of the computer. This process is known as booting up. BIOS can also be a coded program embedded on a chip that recognizes and controls various devices that make up the computer. In the context of this document, these represent the firmware services available at computer boot time, commonly known as the *setup utility*, that permit you to configure your computer's hardware for correct use.

PIPEDA (Personal Information Protection and Electronic Documents Act) **–** Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business. PIPEDA was passed in 2000 to promote consumer trust in electronic commerce. PIPEDA incorporates and makes mandatory provisions of the Canadian Standards Association's *Model Privacy Code* of 1995. The law gives individuals the right to:

- Know why an organization collects, uses or discloses their personal information
- Expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented
- Know who in the organization is responsible for protecting their personal information
- Expect an organization to protect their personal information by taking appropriate security measures
- Expect the personal information an organization holds about them to be accurate, complete and up-to-date
- Obtain access to their personal information and ask for corrections if necessary
- Register a complaint about how an organization handles their personal information if they feel their privacy rights have not been respected.

The law requires organizations to:

- Obtain consent when they collect, use or disclose personal information
- Supply individuals with a product or a service even if that individual refuses consent for the collection, use or disclosure of personal information, unless that information is essential to the transaction
- Collect information by fair and lawful means
- Have personal information policies that are clear, understandable and readily available