DATA SECURITY ADVICE
FOR RESEARCHERS & THE
McMASTER RESEARCH ETHICS BOARD

Revised – February 2016

Table of Contents

A. SOME GENERAL POINTS TO CONSIDER ABOUT DATA SECURITY

New data security issues are constantly emerging. When in doubt, always contact UTS for advice at extension 24357. Keeping data secure is important so that the researcher can access the data when needed (data availability), so that the data are not altered (data integrity), and so that the confidentiality of the data is preserved (data confidentiality).

To maintain data's confidentiality, integrity, and availability, researchers should consider three different data security demands. In all three cases, security issues arise when personal information is present in the data.

Data in motion: This is best described as the transmission/sending of electronic information via tools like e-mail in the form of attachments or in the body of the e-mail message.
Advice for protecting data in motion – Encrypt, encrypt, encrypt!!! Also use secure socket layers and Virtual Private Network. See Glossary.

Data at rest: This is best described by the storage of information in both electronic and paper form. In the case of electronic data, the types of devices used to store information can be a computer's hard-drive, USB key, server, and CD/DVD to name a few. In the case of data in paper form, we tend to store in filing cabinets, in a desk drawer, or on a desk in a locked office. Advice for protecting data at rest – encrypt, back-up, and secure data.

Destruction of electronic data: This is best described as securely destroying all data on any physical device such as a computer hard disk drive, or a USB drive, in such a way that the data cannot be recovered.
Advice for data destruction – The US Department of Defense's method to securely destroy data is known as "DoD7". It recommends assigning a random date to the file, then writing over the original computer code with 0's, or 1's, or random 1's and 0's, then basically doing it all over again seven times. (Please refer to http://www.thefreecountry.com/security/securedelete.shtml for a complete list of free tools to use.
Or destroy the hard drive physically, by breaking it into pieces with a hammer.

B. TIPS FOR PROTECTING DATA IN MOTION

1. Encrypted file system (EFS): For example, for those individuals using Microsoft Windows 2000, XP, Vista, Windows 7; Windows 8.1 and Windows 10. Microsoft introduced a built-in utility called Encrypted File System (EFS) and BitLocker (Windows 7), that will allow you to encrypt a directory or your entire hard-drive. However, there is a caveat: Before using utilities such as these a word of caution; if not used properly all of the information you have stored may be lost forever. As such, before proceeding it is best to speak with your IT security expert for more information. In addition, Macintosh users will likely have different utilities. **Call UTS at 24357** and ask for further details about this. .

2. Storing and transporting data using a USB Key (i.e., jump drive, flash drive, data key and other mobile devices)

- If you misplace your USB key before encrypting the information, and someone finds the USB key – the information will be exposed.
- If you intend to use a USB key to store information here is some information you should keep in mind.
- USB keys contain encryption software. There are also additional programs that can be used to encrypt USB keys. Here are two examples:
    - **VeraCrypt is an open source secure encryption tool that is recommended. It is easy to use as well as very secure. https://veracrypt.codeplex.com/ AEScrypt is another free and open source option: i. Another option, not totally free, is Sophos Safeguard.** Secure Access (http://kb.sandisk.com/app/answers/detail/a_id/2399/session/L2F2LzEvdGltZS8xNDEwODA5MTg4L3NpZC9YcTRxLXQybQ%3D%3D)
- If you decided to encrypt your information and you forget your password/passphrase to unlock it, there is a good chance it could be lost forever.
- Because of how inexpensive USB keys have become, hackers have started using them to distribute computer viruses by strategically distributing them in parking lots outside companies enticing an unsuspecting helpful individual to place it in their computer to find out who lost the key. Don't be enticed!
- In light of new information as of 2010, using built-in encryption on USB keys is not advised.
- A product called "Iron Key" is more expensive than the average USB key but everything stored on it is automatically encrypted www.ironkey.com/ . **However,** US Military-grade USB key such as "Iron Key", could actually be problematic in certain sensitive locales. Generally, when traveling to or through the United States or other countries with strong national security concerns, researchers are advised to check those countries' importation rules regarding bringing in, traveling with or taking out encryption software. Call UTS at Extension 24357 for more advice about these issues prior purchase and your departure.

3. Creating Better Passwords:
Researchers should consult the UTS website or Ext. 24357 for instructions on how to create better passwords and how and where to store passwords.
http://www.mcmaster.ca/uts/macid/passwd.html
A quick tip: DO NOT create a file on your computer entitled "Passwords" or similar words. Web crawlers (i.e., a computer program that browses the World Wide Web in a methodical, automated manner) look for these kinds of file names and are a dead giveaway.

4. On-line surveys and Data Interception:
A) LimeSurvey – the McMaster Research Ethics Board offers a free instance of LimeSurvey. Data is kept on secure McMaster servers. It uses SSL. http://reo.mcmaster.ca/limesurvey

B) FluidSurveys is a Canadian online survey provider http://FluidSurveys.com recently purchased by SurveyMonkey. However, the data is collected and stored in servers in Canada. It offers very similar functions and pricing structures and is a Canadian alternative to the popular US online survey providers. Before using an online survey provider you could ask them these kinds of questions.
Some questions to ask the sales and service people at online survey companies:

- Where is the survey service located? USA or Canada or elsewhere? (If data is held on a server in the US or US subsidiary in Canada it is subject to the USA Patriot Act).
- Who owns the survey service?
- Who owns the data?
- Do they use SSL (https) for surveys (a secure from of data transmission??
- Do they capture personal information other than that explicitly provided by the user?
- Does the researcher see the IP address of the respondent? If yes how easy is it to be turned off?
- How is personal information provided by the user stored?
- How is data transferred to the researcher?
- How is data protected on the server? Backups?
- Who has access to their backups?
- After the data are transferred to the researcher, how/when are they destroyed on the company's servers?

5. Sending emails securely when off campus or abroad:

Internet Cafes and Keyloggers:

- Be aware that there could be hardware and software-based keyloggers. A keylogger is a program or a hardware device that captures or monitors every keystroke made on a keyboard. A hardware-based keylogger is easily detected by inspecting where the computer's keyboard and mouse are plugged into the computer. If the cable is not directly connected to the computer, but rather into another device that, in turn, is plugged into the computer; there is a good chance this is a keylogger. On the other hand, a software-based keylogger is a program that records all keystrokes and stores them for later retrieval and you can't detect it visually.

- The existence of a keylogger hardware device/program installed on a public/kiosk computer is highly likely; as such it is highly recommended you refrain from using them

- If you must use a public/kiosk computer, never access any website that requires you to enter a username/password, and never enter any personally identifiable information while you are using it.

- Information is available on the Internet to assist you to do safe logins from Internet cafes. Click this link to read a useful article by Cormac Herley and Dinei Florencio entitled: How To Login From an Internet Cafe Without Worrying About Keyloggers

Which email account to use?

- It is best to use your McMaster account rather than other popular free accounts like gmail and hotmail that may not have the same level of security that the University provides.
- MacMail uses a secure socket layer (SSL) that encrypts the communication path. If you do not know how to access your MacMail account go to: https://macmail.mcmaster.ca/
- A quick tip: Once you've sent the email, you should delete the email from your "sent" folder if it is not on a secure computer.
- If sending research data over the internet using e-mail, consider setting up a free encrypted e-mail application such as GnuPG www.gnupg.org/ on your laptop or desktop.
- Be aware of who manages the e-mail service that you use. MacMail is owned by McMaster versus "Hotmail" and "Gmail" which are both owned and operated in the United States. See further discussion in the section below.

6. Emailing data back to McMaster while conducting research off-campus or abroad

Note: Please refer to the previous section regarding "Internet Cafes and Keyloggers".

- If you are a McMaster researcher (faculty, student or staff) conducting research off-campus or abroad and the only service available to transmit your data back to McMaster is email, then be sure to use your McMaster email account.
- All faculty, students and staff can obtain a Virtual Private Network (VPN) account from UTS. http://www.mcmaster.ca/uts/network/vpn/ VPN is a good way to work away from one's desk at McMaster while at home because it provides a secure tunnel that protects your transmission of data while it is in transit from the IP address you are using to a drive back at the university. If you have questions about VPN contact the UTS service desk 24357.
- Graduate and undergraduate students may need to request permission to access a drive at their home departments where they can send your data for safekeeping against theft, loss, corruption or confiscation.
- Given the varying levels of sensitivity of data and risk to study participants more sophisticated data security measures can be created on a case by case basis. Please leave enough time for you and UTS personnel to work out the best strategy well in advance of your departure to conduct research.

7. "Wireless" or "Wired" Connection?

- To reduce the risk whilst working from home, setup a secure password protected wireless network. Make sure that you take the time to set up your connection securely. Be reminded that levels of security can change so follow the vendor supplied installation guide to set up your wireless router security. If you require assistance contact UTS for advice at Ext. 24357.
- From hotels whilst traveling on business or conducting research, use Virtual Protocol Network (VPN) to protect data transmission back to McMaster.

- When using Wireless from an Internet Café one should use a VPN to protect data transmission back to McMaster.

8. Security Issues related to Online Survey Research

- On-line surveys go out and come back on to the Internet. Wherever there is a server there is someone administering the server and they may have access. Thus researchers should read the agreement carefully and ask questions about security.
- Survey Monkey is a common on-line survey. The basic free package now has a SSL option The option in Survey Monkey to use SSL which encrypts data being sent across the Internet – reduces the probability to intercept and reassemble to being very unlikely.
- If the server is in the USA or is on the server of a U.S. subsidiary in Canada, then the USA Patriot Act permits snooping by U.S. Homeland Security without probable cause or a warrant.
- Canada is not impervious to government surveillance. CSIS can conduct surveillance but there is more legal protection.
- Keeping a separate (hard copy) identity key is important in research. If information might be of interest to governments, or electronic data is very sensitive, extra data security measures should be undertaken such as encrypting the key. It is vital to strip off identifiers as quickly as possible.

Maintaining Server Security:

- If researchers have a server, they along with their staff and graduate students need to be trained on how to secure their server. Call UTS (Ext 24357) to learn how to secure servers with appropriate passwords and other procedures.

C. TIPS FOR PROTECTIONG DATA AT REST

9. Servers:

- Measures to reduce risk include: restricting server access, installing security updates, configuring properly, installing anti-virus (see below for access to software), coding web applications to OWASP guidelines (see Glossary). Refer graduate students or research staff to this if they are responsible for the maintenance of a project's server.
- Encrypt sensitive information.
- You need to ensure that the physical security of data is also ensured in your office or lab. Don't share swipe entry keys with people, lock doors where servers are physically housed and don't leave passwords in "stickies" near your computer.
  - See the UTS website for their more detailed Best Practices guide on server security
  - http://www.mcmaster.ca/uts/security/ITsecurity/standards/server-security.html

10. Anti-virus software protection:

- All McMaster faculty, staff and students have access to Trendmicro for campus and home computers. Go to the UTS website: https://antivirus.mcmaster.ca/ or contact the help desk at X 24357.
- Because Windows, Macintosh and other non-Windows computing environments may have built in protections it is important to be familiarized with these features.

11. Conducting research on or recruiting participants through chat-rooms, discussion lists and face book/second life etc.

Researchers and research ethics boards continue to struggle with understanding what constitutes "public" and "private" when it comes to research on and recruiting through discussion lists, support groups, chat-rooms, Facebook etc. This form of technology is continually evolving and new options or applications may pose new challenges to the researcher, the participant and the research ethics board. Here are some points for researchers to consider.

- Consult your ethics board when in doubt and to work out how to a strategy that works for your study
- Your data may not be permanently accessible
- Your data may not be accurate or representative due to anonymous online participation.
- See the Queen's University guidelines document in the references section at the end of this document.

12. SECURITY BREACHES – Steps for an Incident response

If it appears that there has been an electronic security breach:

- Seek assistance from McMaster Security Department (**Emergency number dial 88**) (General number Ext. **24281**). McMaster Security works with the local police.
- Turn off computer –**DO NOT** try to remedy the problem.
- Call University Technology Services **(UTS) at ext. 24357**.
- Call the Research Ethics Board to determine if participants need to be informed of the security breach of research data.

13. Other sources of information to help you with you data security questions:

- If you have further questions, contact the UTS staff, ask for education and training for yourself or research staff at uts@mcmaster.ca or call the UTS service desk ext. 24357
- Also consult the IT Security web pages of UTS for a variety of information and to keep up with ongoing changes.: http://www.mcmaster.ca/uts/ITsecurity/

D. TIPS FOR SECURELY DESTROYING DATA

14. Decommissioning computers and clearing off data:

- Sensitive files and research materials should be removed from the computer prior to disposal
- Formatted hard disks may contain recoverable residual data
- If disposing a computer, examine affordable disposal services.
  If transferring ownership of computer, low-level hard-drive cleansing is required.
- Consult UTS for advice on removing sensitive data
- **See UTS advice for hard disk disposal**

http://www.mcmaster.ca/uts/security/ITsecurity/best-practices/disposal.html

- The US Department of Defense's method to securely destroy data is known as "DoD7". It recommends assigning a random date to the file, then writing over the original computer code with 0's, or 1's, or random 1's and 0's, then basically doing it all over again seven times. (Please refer to http://www.thefreecountry.com/security/securedelete.shtml for a complete list of free tools to use.
- Or destroy the hard drive physically, by breaking it into pieces with a hammer.

E. Glossary of Abbreviations and Terms

Cache: a cache is a temporary storage area where frequently accessed data can be stored for rapid access. Once the data is stored in the cache, future use can be made by accessing the cached copy rather than re-fetching or re-computing the original data, so that the average access time is shorter.

Data sniffer: A sniffer is a type of software that grabs all of the traffic flowing into and out of a computer attached to a network.

Encryption: the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature.

Keylogger: A keylogger is a program or a hardware device that captures or monitors every keystroke made on a keyboard.

OWASP: The Open Web Application Security Project (OWASP) is a not-for-profit worldwide charitable organization focused on improving the security of application software.
http://www.owasp.org/index.php/Main_Page

SSL: Secure Socket Layers are cryptographic protocols that provide secure communications on the Internet for such activities as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

USB Key: also known as a data key, jump drive, etc.

VPN: Virtual Private Network

Web crawler: A Web crawler is a computer program that browses the World Wide Web in a methodical, automated manner.

F. References:

Herley,C. and Florencio,D.
How To Login From an Internet Cafe Without Worrying About Keyloggers.
Microsoft Research, Redmond. Accessed from the Internet, December 15, 2009
http://cups.cs.cmu.edu/soups/2006/posters/herley-poster_abstract.pdf

Queen's University General Research Ethics Board
2008 Draft Exemption Policy: Research Ethics Review of Projects Involving Digital Data Collection (October 3, 2008 version)

http://www.queensu.ca/urs/sites/webpublish.queensu.ca.urswww/files/files/QueensDigitalDataPolicy.pdf