SOP: Safe Data Use Outside of the VU

Digital transfers/Data sharing

For data that are transferred or shared digitally outside of the VU, only approved services should be used. NEVER use Dropbox, WeTransfer, Google Drive or your private/non-VU e-mail for sending data. Sending date to private e-mail addresses should also be avoided whenever possible because once data is on an external server, such as gmail's servers, the VU no longer has control of that data.

The best options for transferring/sharing data are SurfFileSender and SurfDrive, and data should be encrypted prior to sending. The de-encryption password must be shared with the receiver via another route, for example, calling the receiver to provide the password verbally. SurfFileSender automatically includes an expiry date on the link to the shared files, which you can adjust as needed. You can include an expiry date on a shared file in SurfDrive and this should always be included if the person who has been granted access should only have access to the files for a specified period of time. The VU is also introducing ZIVVER, which can be added as an extension in Microsoft Outlook. It functions similarly to SurfFileSender, but requires fewer steps to activate. It can also detect potentially high risk e-mails that need to be protected. Unfortunately, the ZIVVER extension is not available on the Apple version of Outlook; for Mac users you can use the app via SURFconnext. For all, potential ZIVVER users, make sure to update your user profile after you have activated your account otherwise your VUnet ID will appear as the name of the sender. If you find that the standard VU options do not meet your requirements, contact IT voor Onderzoek (itvo.ucit@vu.nl) or UCIT for advice.

Lastly, bear in mind that there is currently a LOT of discussion about the anonymity of certain types of data collected from humans. Clearly certain data types are much lower risk for re-identification than others (e.g. reaction times, kinematics), but many in the legal world still see these data as NOT anonymous. We are working hard to get clarity on the issue. As of early 2019, it is advised to take at least some measures to protect even what you would consider low risk data if it has been collected from humans. This means if you are sending data to a student, you can send it to their VU e-mail address so that the data remain on internal servers. If this is your choice advise your student that they should turn off any e-mail forwarding from their VU-address to their private e-mail. Alternatively, if a private e-mail is the only option for the receipt of data, it is still a good idea to use a service such as ZIVVER or SurfFileSender in the event that the e-mail is sent to the wrong address.

Portable Devices

Portable devices are any easily transported devices that can be used to collect and store data. They include USB sticks, external hard drives, laptops, tablets, smartphones, DVDs, CDs and cameras. For many research projects, data must be collected remotely and physically returned to the VU using a portable device. Because these devices are portable, they are easy to lose or worse, they can be easily stolen. Therefore, it is essential that extra care be taken when using these devices.

USB Sticks/External Hard Drives/Flash Drives

There are a few variants of secure portable drives. In general, there are two main types: hardware encrypted drives and software encrypted drives.

For a variety of reasons, software encrypted drives may be slightly less secure than hardware drives. These drives can also be taxing on computer resources during encryption and decryption, and they only function with specific software that may not be available on all operating systems (e.g. BitLocker is a commonly used software encryption tool, but it only works with Windows). Software encrypted drives are cheaper than hardware encrypted drives and they usually have recovery systems to recover encrypted data, although these systems often need to be set up prior to use of the drive.

Hardware encrypted drives may be password protected by a password chosen by the user or with a PIN number that is entered onto a keypad on the device. These drives work on all operating systems after the password or PIN is entered. Hardware encrypted drives use less resources on your operating system during encryption and

decryption, but they are much more expensive than software encrypted drives and data stored on these devices can be much harder to recover if the device fails.

To decide which type of portable drive to use:

1. Complete a data classification (FGB research data officer can provide a template; this document is not currently available on VUnet) or review an existing data classification that has been previously completed for your research data.
2. If your data do **not** have a **high level of confidentiality risk**, but the **risks to the availability and integrity of the data are high**, use a software encrypted drive (note that this will limit the use of the drive on certain operating systems). Make sure to setup recovery options and back-up the data on an approved VU storage option.
3. If your data have a **high level of confidentiality risk**, it is advisable to use a hardware encrypted drive with 256-bit encryption. Back-up the data on an approved VU storage option. For particularly sensitive files, it is also possible to further encrypt such files for example as encrypted ZIP files (see below "DVDs/CDs").
    a. Data with a high level of confidentiality risk can range from benign videos of children playing to interviews with abuse victims. Clearly there is a lot of variation in that level of risk. If the data are classified as high-risk regarding confidentiality because it's clearly easy to identify participants, but the nature of the data is relatively benign, software encrypted drives are still a reasonable option for securing such data. Additionally, if other measures are in place to protect the data on the drive, such as pseudonymization, software encryption may again be appropriate. However, if the data can clearly cause someone harm or distress if leaked and the participants are easily identifiable (directly or indirectly), the data should be stored on hardware encrypted drives.
    b. Software encrypted drives are only as secure as your computer is. If your computer is infected with malware or other malicious software, a hacker can easily access and crack the encryption on a software encrypted drive through brute force. Therefore, make sure to have virus and malware scanners active on your computer.

VU Laptops

Although laptops are an option for VU research workspaces, their use must be limited because of the increased risk for data breaches. Therefore, researchers should consider whether a laptop is absolutely necessary to carry out their function and supervisors should only approve requests for laptop workspaces when the use of a laptop is essential for the researcher's work. Laptops should be secured during their use in the office (e.g. using Kensington cables) and locked in a desk drawer or cabinet at the end of the day or when not in use.

When using laptops, the first consideration should be whether data need to be physically stored on the laptop. Whenever possible, data should be stored on an approved VU storage option and if it is necessary to access the data remotely, Citrix should be used. The VU storage options are not only safer in terms of security, but they are also regularly backed-up to prevent data loss. The same cannot be said about data stored on the laptop hard drive. If data must absolutely be stored on a laptop, they should be backed-up on a VU storage option.

In addition to using VU storage options for data storage, VU laptops should be encrypted. Although VU laptops require passwords to log in, thieves can still remove the hard drive from the computer to access all of the stored files. Even if you are working with VU storage options, some data may be cached to the hard drive and accessible if the hard drive is not encrypted. To prevent this, you must encrypt your laptop's hard drive. The best option for hard drive encryption is Full Disk Encryption. This type of encryption decrypts your hard drive whenever you log in to your laptop and automatically encrypts it when you lock or sign off of your laptop, therefore making the hard disk encryption a part of the login process. VU provided computers are already equipped with encryption software (more information can be found on VUnet, as well as on the University of Edinburgh website). VU-IT supports BitLocker for Windows users and FileVault for Mac users. BitLocker is already installed on green and orange workplaces: on Windows 7 workspaces it must be activated by the user; on Windows 10, it is already active. Some Windows configurations do not support BitLocker (see "Availability" in the hyperlink); check with UCIT if uncertain. If using BitLocker, it is possible to add a requirement that a PIN must be entered and/or a hardware encrypted USB-flash drive must be inserted in order to decrypt the hard drive; the choice depends on the privacy risk of the data and the risk of harm to the data subjects if there is a breach. Windows users should

also activate the recovery option in BitLocker when encryption is activated to help prevent data loss or corruption.

Tablets/Smartphones/iPods

Apple products produced from 2013 onwards are encrypted when they are locked by the user. All Android products running 5.0 and up can also be encrypted when locked, but the user needs to activate this encryption. Although encryption is activated when these devices are locked, anyone can unlock them unless the user activates a PIN code or biometric scan (finger print or iris scan) for locking and unlocking the device. A PIN code or biometric scan should always be used for these products if sensitive data is going to be collected on them.

Public Wi-Fi

It is discouraged to connect VU devices to public Wi-Fi (e.g. on trains, in a café, at the airport) because of potential security risks. Only use secure Wi-Fi such as eduRoam and if it is absolutely necessary to use public Wi-Fi, activate a VPN, such as eduVPN.

DVDs/CDs

Sometimes data will be burnt to a DVD/CD to allow for data transfer. If the files on the DVD/CD are sensitive they should be encrypted at the file level using, for example, VeraCrypt. DVDs or CDs should only be used to transfer data; after the data are securely stored on a VU storage option, the DVD/CD should be destroyed.

Tips on Passwords

It is important to choose strong passwords when encrypting data, but it is also important that the passwords are not easily forgotten. Tips on choosing and managing passwords can be found here. Some simple tips for strong passwords are to make them long (15 characters or more) and to include capital and lower-case letters, as well as numbers and special characters. To help with remembering passwords, use passphrases instead and replace letters with numbers and characters that are logical replacements **TO YOU** (i.e. not necessarily to someone else). For example, you could replace the letter Y with a 4 because when a 4 is open at the top is looks a bit like a capital Y. A safe and memorable passphrase could be: 1_l0Ve_+He_fGb!

Encryption in the Long Term

It is important to note that encryption standards change with time. Standards for encryption change because as computers become more powerful it becomes easier to break older encryption methods. If encrypted files will be stored for long periods of time, it is important to re-assess regularly whether the encryption used still meets current standards. If data will be encrypted and stored for more than 5 years, it is necessary to nominate an individual who will monitor whether the encryption must be updated; updates are necessary whenever an encryption standard has been cracked or shown to be vulnerable. UCIT can help with this assessment.

Cameras

There is no method for encrypting digital cameras and although SD cards can be encrypted, they cannot be used in a camera if encryption has been activated and there is no way to de-encrypt the data using a camera. The safest and most convenient option when physically transferring data recorded on a camera is to remove the SD card and store it in a mini locked safe.

Tips for video recordings

Researchers can choose between iPads/iPods or cameras for recording video data. In general, iPads should be used because a PIN code can be activated to lock and encrypt the device, which is not feasible for camera SD cards. Cameras are only superior to iPads with regards to zooming options and light capture in dark environments. If these features are not important, researchers and their assistants must use iPads with a PIN for video

recordings. If zooming and light capture are essential to the research project, a mini safe must be used for storing SD cards during transport, **particularly** if researchers are transporting the cameras via public transportation.

TO3 Borrowing Service

The TO3 helpdesk for the FGB has a number of portable devices that can be borrowed for short-term use by FGB researchers. The online reservation system can be accessed via the TO3 webpage. Some equipment available for borrowing are:

- A small selection of hardware encrypted USB-sticks, as well as regular USB-sticks
- A small selection of external hard drives
- ~60-70 Windows laptops
    - In general, these laptops should only be used to collect data with medium to low privacy risks (i.e. **NO** names, contact information, audiovisual data, birthdates, 6-digit postal codes, other highly specific information nor free text). Because these laptops are intended for short-term use by many different users, it is not feasible to require individual login credentials for every user. Full disk encryption of the hard drive is also not feasible for these laptops.
    - If TO3 laptops must be used for collection of higher risk data, the data files should either be encrypted with VeraCrypt or stored on an encrypted USB- or external hard drive rather than the laptop hard drive. In these cases, these data must be backed up to a secure VU-network as soon as possible.
- ~150 iPads and iPods
    - iPads and iPods are provided without any PIN codes however the user can activate his or her own PIN codes on these devices. PIN codes should always be activated whenever these devices are used to record audiovisual data.
        - Prior to activating a PIN code on any loaned device, consult with the TO3 technician, from whom you loan the device, about the use of a PIN. If the PIN is forgotten, the device may be rendered unusable.
    - Other forms of research with these devices may not be feasible if a PIN is required to lock and unlock the device throughout the data collection process (e.g. if 30 devices are being used simultaneously in a classroom). The researcher must weigh how complicated the use of a PIN will be against the risk of subject re-identification in the data, the potential harms re-identification could have on data subjects and the risk of the devices being lost or stolen. If researchers absolutely cannot complete their project with PIN encrypted devices, but there are risks to the privacy of the subjects, then in such a case, these devices should not be transported via public transit. If researchers and their assistants have absolutely no other option than to travel via public transportation, then they must be cognizant at all times of where the data are. They should not put the devices under their seat or in a luggage storage area. They should be able to see the devices at all times and preferable have a hand on the devices at all times.

Returning portable devices after use

When you no longer need the device loaned by the VU or TO3, it is important to **permanently** remove all of your files from the device as per the instructions from TO3. Any files that are important for research, particularly for archiving, should already be stored on a VU storage option.

Analog data (paper notes, bodily materials, cassette recordings, photographs etc)

Not all data are stored digitally; analog data may also be sensitive and these data should still be transported securely and with care. The safest option for storing these materials is in a locked briefcase or a portable locked safe (see “Cameras” section). If these measures are absolutely not possible, it is strongly recommended not to use public transportation for travelling to and from the data collection site, particularly if the data are very sensitive. Obviously public transportation is often the only option for many researchers and research assistants, therefore, if public transportation must be used, make sure to review the tips below on physically transporting data in a safe manner.

General Tips for Physically Transporting Data

Whether data are physically locked away or locked with encryption, both methods only function to slow hackers and thieves down. Locked and encrypted data are not 100% safe therefore users always need to take extra care to not lose these items.

- Whenever possible, and especially when working with highly sensitive data, try to find an alternative to public transportation. Obviously, this is not always feasible, therefore, when transporting data on public transportation stay alert and aware, and always keep track of your devices.
- Don't throw your encrypted device into the bottom of a giant bag. Know where it is at all times.
- Just like they say on the train, always check that you have all of your belongings before you depart.
- Be aware of your surroundings and situations where pickpockets could steal your devices (i.e. don't bring your research USB-stick to the Pride Parade).
- Whenever possible, immediately transfer the data from the research site to the VU. If this is not possible find a safe location to store the data (e.g. your house) until you can transfer the data to secure VU servers. Basically, don't carry around research data on your person during your free time.

Support for Complex Cases

TO3 Helpdesk: Provides FGB specific advice and solutions for data collection and transport options
Research Data Officer: Provides advice for weighing privacy risks against data utility, and data management tips to improve security
IT voor Onderzoek and Domain Team Solution Architects (contact via Annemieke Schoonenboom, FGB IT Relation and Information Manager): Help to determine appropriate storage and data transfer options based on data classification levels
UCIT: Provides general VU solutions; most devices for long-term use can be ordered via UCIT

References and additional readings

VU Code of conduct for computer and network use
Wiltshire, S. (2017, Sept 12). *Hardware Encryption vs. Software Encryption: The Simple Guide*. Retrieved 6 August 2018, from: https://www.ontrack.com/blog/2017/09/12/hardware-encryption-software-encryption/.
Pettitt, M. (2017). *Encryption at rest: Not the panacea to data protection* [White paper]. Retrieved 6 August 2018, from NCC group: https://www.nccgroup.trust/uk/our-research/encryption-at-rest-not-the-panacea-to-data-protection/.