RESEARCH DATA MANAGEMENT

Guidelines for Information Security

VRIJE UNIVERSITEIT AMSTERDAM
Information Technology

STATUS draft for pilot training research data management for PhD's
VERSION: 0.2

AUTHOR N. van Deursen, Information Security Officer
ASSIGNED BY
DATE 1.11.2017

DISTRIBUTION

VERSION HISTORY

VERSION NUMBER	DATE	AUTHOR	REMARK
0.1	5-10-2017	N. van Deursen	
0.2	1-11-2017	N. van Deursen	Updated after review

TABLE OF CONTENTS

1. INTRODUCTION

The Research Data Management - Information Security Guidelines pertain to researchers and research team members who obtain, access or generate research data, regardless of whether the data is associated with funding or not. These guidelines help researchers understand the sensitivity of the data they are collecting and develop appropriate data protection plans, know the appropriate mediums and places to store data, understand how and when to dispose of data, prepare their research data for public use, understand how to keep research data secure while traveling, and what to do in the event of theft, loss, or unauthorized use of confidential research data. These guidelines can also be used as part of the data management planning process in conjunction with other (future) guidelines, such as privacy and ethics policies.

2. RESPONSIBILITIES

Researchers are expected to be proactive in the protection of research data. The guidelines in this document are intended to help researchers understand when and how to use the most effective and efficient methods for storing and analyzing confidential research data so that those data are adequately protected from theft, loss or unauthorized use.

If your data is (privacy) sensitive, you do not want any unauthorized person to access it. In the Netherlands, the collection of non-anonymous data for scientific research is subject to the Law Protection Personal Data (Wet Bescherming Persoonsgegevens). This law regulates all relevant aspects of informed consent, data collection, storage, protection, retention and destruction of personal data. Medical research data falls under the law Medical scientific research (Wet Medisch wetenschappelijk onderzoek).

Beware that in 2018 new European legislation for personal data will be issued. The VU is working towards compliance with this new regulation.

3. INFORMATION SECURITY AT DIFFERENT STAGES IN YOUR RESEARCH

3.1. AT THE START: CLASSIFY YOUR DATA

Ask yourself the following questions:

- Are you collecting personal data (name, email address, IP address, phone number, geolocation data, photographs of people, and so on?
- Is your research classified as confidential by your faculty or grant provider?
- Could your research lead to public outrage or media coverage? Examples are research into environmental, political, or ethical issues.
- Do you use chemicals that, if misused, could harm people?

If any of these apply, you should think about protected storage of your data and reports and who you can share it with.

The following table indicates how your data might be classified:

Vrije Universiteit Amsterdam Information Risk Classifications			
	Low Risk	**Moderate Risk**	**High Risk**
Confidentiality	• The data is intended for public disclosure. • The loss of confidentiality of the data would have no adverse impact on your research goals, safety, budget or reputation. • Benign information about individually identifiable people.	• The data should be available only to a specific group. • The loss of confidentiality of the data could have a mildly adverse impact on your research goals, safety, budget, or reputation of your research group, faculty or the VU. • The data contains sensitive information about individually identifiable people.	• The data should be available only to a specific group. • Protection is required by law/regulation. • VU is required to report to the Information Commissioner's office (Autoriteit Persoonsgegevens) and to the individuals if the data is inappropriately accessed. • The loss of confidentiality of the data would have a significant adverse impact on your research goals, safety, budget or reputation of your research group, faculty or the VU.
Integrity	• Some errors in your data or analysis are acceptable.	• Some errors are sometimes acceptable and it would have a mildly adverse impact on your research goals, safety, budget, or reputation of your research group, faculty or the VU.	• Errors in data or calculations are unacceptable, as it would have a significant adverse impact on your research goals, safety, health, budget or reputation of your research group, faculty or the VU.
Availability	• Loss of the data is no problem as it can easily be reproduced or the process can be postponed. • The data can be unavailable up to 1 week	• Recovery of data after data loss should not take longer than a week and it would have a mildly adverse impact on your research goals, safety, budget, or reputation of your research group, faculty or the VU. • The data can be unavailable up to 1 day.	• Loss of data is a disaster and is not allowed to happen at any time, as it would have a significant adverse impact on your research goals, safety, health, budget or reputation of your research group, faculty or the VU. • The data can be unavailable for 1 hour only.
Examples			
Confidentiality	• VUnet ID • Information available on the VU websites without VU-net ID authentication. • Some research data (at data owner's discretion), such as a survey about reading habits/an experiment on pattern recognition.	• Unpublished research data (at data owner's discretion) • Student records and admission applications • Staff employment applications, personnel files, benefits, salary, personal contact information • Engineering, design and operational information regarding VU infrastructure • Project administration • Non-public contracts and policies/manuals	• Patient records • credit card numbers/ bank account details • social security number • passport/driver's licence number • health information/ehealth app • intellectual property • crime records, court cases, • data on sexual behaviour/ illegal drug use • passwords • big data analysis
Integrity	• Research data (at data owner's discretion)	• Qualitative and quantitative research data (at data owner's discretion)	• Analytics that support management decisions • biomedical research • high risk chemical experiments
Availability	• Publicly available and easily accessible dataset, software, hardware.	• Data, software, hardware that is replaceable within a short timeframe.	• Patient life support systems • (real time) big data analytics • Almost finished thesis or finished but unpublished work that will take many hours to redo if lost.

3.2. DATA COLLECTION STAGE

3.2.1. SURVEY TOOLS

When you buy a license for a survey tool, or if you use free online survey tools, make sure to read the Terms & Conditions. The T&C should tell you:

- where the provider stores your data (is it stored in Europe?)
- will they use our data for commercial activities?
- is the personal data of your respondents well protected?

The VU supports Qualtrics, and this tool has been approved to collect and process personal data under the VU license (not approved to collect personal identifiable data with a consumer or student license).

3.2.2. VOICE RECORDINGS

- Where possible the name of the interviewee must not be recorded in the audio file.
- Where possible an encrypted device must be used for recording eg an Apple iOS device such as an iPod touch, iPhone or iPad with activated device encryption. Where high quality audio, twin microphones and more than one recording device (eg for backup) are required, and the device is not encrypted, data must be downloaded to an encrypted device as soon as possible.
- The device used to make the recording must never be left unattended and must be locked away securely when not in use.
- Transcription of the voice recordings must be done in a secure environment.
- The identity of the participant must be anonymised in the transcript unless explicit consent has been obtained to maintain their identity.
- Transcripts must be securely stored.
- Transcripts or voice recordings held outside of the approved University systems must be stored on an encrypted device for temporary storage only. They must be transferred to University systems and deleted from temporary storage as soon as possible.

3.2.3. RECEIVING DATA FROM THIRD PARTIES

- Don’t ask anyone to send confidential files of files with personal data by email.
- Should you receive confidential or personal data by email, transfer the data to a secure medium as listed in 3.4.
- Suggest your third party to deliver the files with Surffilesender (with encryption).
- Suggest your third party to upload the files on Surfdrive.
- Investigate the possibility to access the data on the supplier’s systems, using a secure connection.
- Portable media (external hard disks, USB sticks, recorders, and so on) should be stored in a locked cabinet and destroyed when no longer needed.

3.3. STORE YOUR DATA APPROPRIATELY DURING RESEARCH

Not all ICT facilities provided by the VU are suitable to store high risk data. The following table shows what services are advised for different risk types.

Approved Data Storage											
	Personal Device	VU-network H:	VU-network G:	VU-network project folder	Google Apps VU	VU SQL database*	SURF drive	EDU groups	Portable data storage	Secure USB with PIN	Scistor/ Scicloud
Personal use											
To store your personal files	√	√	X	X			√				
Business use											
Low risk data	X	√	√	√	√	√*	√	√	√	√	√
Medium availability risk data	X	X	√	√	√	√*	√	√	√	√	√
High availability risk data	X	X	X	X	X	√*	√*	X	X	X	√
Medium confidentiality risk data	X	X	√	√	X	√*	√*	√*	X	√	√
High confidentiality risk data	X	X	√*	√*	X	√*	√*	X	X	√	√
Available from:	IT	IT	IT	IT	IT	IT	SURF	SURF			IT

* = requires additional security controls, such as management of user access rights, antivirus & encryption on workstations

Should you require additional software which is not listed on the IT software pages, contact the IT servicedesk.

3.4. PREVENT DATA SHARING OR DATA LOSS

You might not want others to use and have access to your data before you explicitly decide to grant this. Please remember the following tips:

- Do not provide others with your login credentials.
- Automatically lock your computer during a break.
- Do not leave unsecured copies of your data lying around.
- Have a strong password.
- Encrypt your data.
- Encrypt your device.
- Do not use free public WIFI.
- Use Eduroam where available, see: www.eduroam.org/where/
- Create backups of your files. Especially when your require high availability.
- Do not use free cloud storage solutions such as Dropbox for work related to the VU.
- Be aware of social engineering: no reliable organization will ever call you and ask for your login credentials.
- Be aware of SPAM and phishing emails: do not click on suspicious links.
- If necessary, ensure that physical access to your office or research facilities is granted only to people who have a need to be there.
- Do not connect any unsecure devices to the VU network.
- Store paper files with personal data in a locked cabinet.

For more information: VUNET or cybersaveyourself.nl

3.5. WHY CAN'T I USE FREE CLOUD STORAGE SUCH AS DROPBOX OR ONEDRIVE?

Here are some general risks of putting your data into cloud solutions such as Dropbox:

1. The data will most likely sit outside the European Economic Area, so will not be covered by EU data protection laws, and if it resides in the US will become subject to the US law and may be accessed or removed without your knowledge or consent.
2. You put data into it at your own risk, with no safeguards about the continuing existence of the data and no guarantee that the access rights you set will be maintained.
3. The data may be altered or corrupted without your knowledge, and you won't have any way of getting uncorrupted copies back.
4. During your employment contract with the VU, your work is the intellectual property of the VU. There is no possibility for the VU IT department to retrieve files from your personal cloud storage in case you should leave the VU, fall ill, or if you lose your password. This could lead to data loss for the VU.
5. There is no guarantee of data availability (i.e. if the files are accidentally deleted there's no backup. There is also no guarantee of the service continuing to exist).
6. There is no guarantee of data confidentiality. The data may be held in the manner you expect, but may not.
7. Most cloud storage providers give no way of auditing who has accessed or downloaded your data.
8. Dropbox administrators can access ANY content on the Dropbox site, and if their access is compromised, it means all Dropbox data is automatically at risk of compromise.

3.6. ENABLE DATA SHARING AND COLLABORATION

In some cases, some people may need to gain access because you are in a collaboration.
Be aware that emailing confidential documents without additional security controls is not secure!
De VU provides the following facilities for collaboration:

Approved Data Sharing/Collaboration													
	VU-network G:	VU-network project folder	Google Apps VU	VU SQL database*	SURF drive	EDU groups	Secure file server	Scistor/ Scicloud	VU outlook email	VU outlook with encrypted attachment	VU Outlook with certificate	SURF filesender with encryption	SURF filesender without encryption
Collaboration within the VU (low risk data)	√	√	√	√*	√	√			√	√	√	√	√
Collaboration within the VU (medium risk data)	√	√	X	√*	√	√	√	√	√	√	√	√	√
Collaboration within the VU (high risk data)	√*	√*	X	√*	√*	X	√	√	X	√	√	√	X
Collaboration with third parties (low and medium risk data)	n/a	X	X	√*	√	√	√	√	X	√	√	√	√
Collaboration with third parties (high risk data)	n/a	X	X	√*	√*	X	√	√	X	√	√	√	X
Access rights controlled by:	you	you	you	you	you	you	you	you					
Available from:	IT	IT	IT	IT	SURF	SURF	IT	IT	IT	**	SURF	SURF	SURF

* = requires additional security controls, such as management of user access rights, antivirus & encryption on workstations

**Encryption software at your own discretion

Should you require additional software which is not listed on the IT software pages, contact the IT servicedesk.

3.7. SECURING YOUR DATA AFTER YOUR RESEARCH

- Data archiving: contact the Library for data archiving.
- Destruction of data: contact the IT servicedesk for support with permanent destruction of data from your device.
- Delete the access rights of people that no longer need your files and data.

4. KEEPING RESEARCH DATA SECURE WHEN TRAVELING

A growing number of researchers are conducting their research outside of The Netherlands in a wide variety of settings, some of which may pose considerable challenges for upholding the promise of confidentiality and keeping data stored securely. When traveling in other countries, researchers should be aware of local laws regarding the legal status of confidential research information that could be confiscated by police, customs agents or other government officials. In addition some countries have rules designed to control the movement of encryption technology that enter or exit their borders. This is important for anyone who wants to travel with a laptop computer in order to collect confidential research data.

4.1. PROTECTING PAPER FILES

Researchers working in different settings will often collect field notes, observations, interviews or informed consent using notebooks or other types of paper documents. In some cases this may reflect the researcher's preference but might also result in situations where use of a computer is difficult or inappropriate, or simply not possible because of limited access to electricity. In situations like this, researchers who need to keep their data and consent forms confidential need to consider how best to protect their paper document and notes while travelling. In some cases, simple precautions, such as physical separation of consent forms from data may be sufficient. In other cases, researchers may wish to bring along prepaid, pre-addressed shipping envelopes so that they can send their documents as quickly as possible back to the VU or some other secure collection and storage point.

4.2. INTERNATIONAL TRAVEL AND ENCRYPTION

Nearly all VU-issued laptops use encryption technology that protects the privacy of the information that resides on those laptop machines. Users may not even be aware of this encryption software because it is designed to run unnoticeably in the background much like firewall or virus protection software. Encryption is controlled or restricted in many countries. Some countries ban, or severely regulate, the import, export, or use of this technology. Traveling with your laptop with encryption software installed on it to certain countries could lead to your imprisonment or cause your laptop to be confiscated. In some cases it may be better not to bring a device at all.

4.3. THINGS TO REMEMBER WHILE TRAVELING

When traveling, the University recommends that extra measures be taken to ensure that any breach of security on a traveling device does not result in a broader compromise of the VU's systems and data.

- Don't trust public or hotel Wifi: use Eduroam where available, see: www.eduroam.org/where/
- By not logging into VU applications while you travel, you eliminate the risk of your ID and password being captured and used to compromise VU systems. You also reduce the amount of data that is retrievable if your mobile device is lost, stolen or otherwise compromised. Therefore, keep your direct access to VU systems and information to an absolute minimum, preferably zero.
- Access the data you need for your trip from the external storage service (e.g., Surf Drive). Allow a colleague to add files to your external network drive in case a file was forgotten during preparations.

- *Please note that using Remote Desktop or equivalent software to access your University desktop or other device from a high risk country should also be avoided as these transmissions may also expose valuable information.*
- Avoid using public workstations. The security of public workstations, especially in high risk countries, cannot be trusted. When you use a public workstation, anything that you enter into the system - IDs, passwords, data - may be captured and used, so limit your activity to the devices that you bring.
- Be aware of your surroundings when logging in or inputting data into your devices. There have been many cases where an ID, password or a piece of confidential information had been compromised simply by watching the person input the information. Be discrete when inputting your ID and passwords.
- Notify the VU if a theft or loss occurs. Traveling can be fraught with a variety of distractions - going through airport security, finding your way around town, getting used to cultural norms, etc. Unfortunately, most instances when mobile computing devices are lost or stolen occur in the areas where the distractions are the greatest. Recognizing distracting situations and, when they occur, taking extra care to maintain your focus can prevent you from having to take the steps necessary to disable those devices and obtain replacements. In case a laptop or mobile device is lost or stolen, contact the IT service desk.

4.4. WHEN YOU RETURN

- Change any passwords you may have used during your travels. When traveling, especially in high risk countries, the likelihood that your ID and password will be captured is high. Click here to change your VUnet password.
- Restore the software on the systems with which you traveled to trusted versions. When our devices connect to a network in a high risk country, there is an increased likelihood that the device will be compromised and have malicious software installed. This software then can compromise information and other devices on the VU network when the device is reconnected to the University's network.

5. WHAT TO DO IN THE EVENT OF THEFT, LOSS OR UNAUTHORIZED USE OF CONFIDENTIAL RESEARCH DATA

A data security breach occurs when there is a loss or theft of, or other unauthorized access to, sensitive personally identifiable information that could result in the potential compromise of the confidentiality or integrity of data. By law, the VU is required to notify the Autoriteit Persoonsgegevens of security breaches involving personal information.

Anyone at the VU who knows or suspects that their confidential research data has been lost, stolen or used inappropriately is advised to contact the IT servicedesk for immediate assistance.