RESEARCH DATA MANAGEMENT GUIDELINES FOR INFORMATION SECURITY
VRIJE UNIVERSITEIT AMSTERDAM

VU VRIJE UNIVERSITEIT AMSTERDAM | Information Technology

STATUS Final
VERSION: 1.9.6

AUTHOR Refer to version history table
ASSIGNED BY
DATE 22.11.2019

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
1.0	18-12-2017	N. van Deursen	FSW & UBVU input
1.1	6-12-2018	T. van Loon	Renewed and updated
1.2	19-12-2018	T. van Loon	Updated after review
1.3	15-1-2019	T. van Loon	Updated after review
1.9	21-3-2019	T. van Loon	
1.9.1	26-3-2019	T. van Loon	Updated after review
1.9.2	1-4-2019	T. van Loon	Updated after review
1.9.3	28-5-2019 25-6-2019	T. van Loon P. Mercera	Updated after review, removed classification matrices Changed Solution Architect into research IT advisor
1.9.4	22-7-2019	P. Mercera	Updated after review comments of the VUO voorbereidingsgroep meeting held on 1-7-2019 Comments received from Meijer, Berends and Broerse Research IT advisor changed to Information Security Officer RDM
1.9.5		P. Mercera	Update: a section about the implementation plan is added. This version has been sent to VUO and accepted by the VUO. This version is sent the Vertaalbureau to review the English. Next this version was sent to the MT of Dienst IT
1.9.6	12-11-2019	P. Mercera	Update of the sentence 'When you buy…..' in section 3.2.1. Reviewed version by Vertaalbureau. Concept text deleted and version history actualized Name of the document updated.
1.9.7	2-12-2019	P. Mercera	Remarks from Jeff Trimbos see mail 5-12-2019 'Data classification' updated to 'CIA classification of the data' Title of the document updated Availability is not equal to data loss, but availability is equal to the loss of availability of data Integrity of the research archive after publication is high

TABLE OF CONTENTS

1. INTRODUCTION

The 'Research Data Management Vrije Universiteit Amsterdam – 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. In some cases, grant providers explicitly request a data management plan. In such cases, it is important to develop a tailored data protection plan as part of the data management plan for the specific research project.

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 travelling
- Know 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.

1.1. EVOLUTION OF THIS GUIDELINES DOCUMENT

An evaluation is planned for every nine months to assess the applicability of these guidelines. This evaluation might lead to updates to these guidelines. A vital part of these guidelines are the CIA classification levels of the IT services that support research in general. The CIA classification information indicateis very important and will be added as soon as this is available.

A list of IT services is included at the end of this document. Currently, the CIA classification levels of these IT services are unknown. These classification levels determine how suitable the specific IT service is for handling the research data in terms of confidentiality, integrity and availability. However, financial resources have been asked to start classifying these IT services, with an estimated delivery date of end Q3 2020.
Part of the evaluation every nine months will be to assess the following topics:

- The classification all IT services
- New IT services to be added to the list and their corresponding data classification
- Review comments to be taken into consideration
- New policies, changes in processes and urgent subjects
- The option of adding a frequently asked questions section is also considered for a future version of this document

This document will remain in continual development. However, the recommendation is to start with this document as a catalyst for the further development of the guidelines.

1.2. IMPLEMENTING THESE GUIDELINES

These guidelines will be accompanied by an implementation plan. The CIO is responsible for this implementation plan, which will be drafted in close cooperation with the faculties. The plan includes needs, priorities, potential barriers, facilitating factors, available resources, implementation strategy and cost indication.

In the meantime, the VU Amsterdam Research Support Programme is developing services, tools and support that will make international cooperation, research data management (RDM) and Open Science easier. As such, it contributes to better research data management practices, including security and privacy aspects. In September 2019, DMP Online will be available to all researchers. This is an online tool that enables researchers to make and share data management plans. Pilots

with iRODS-YODA (an RDM tool to manage large research data sets) and Research Drive (to store and share research data) are also currently taking place. In autumn 2019, the requirements for the storage of privacy sensitive data will be identified among researchers, data managers and IT specialists. It is expected that by Q3 2020, a clear and complete overview of applications and their suitability for specific types of data will available to researchers.

1.3. TARGET AUDIENCE

The target audience for this document includes data managers, coordinators of information security and privacy champions. The information security officer will be in charge of updating this document.

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 analysing research data, including that which is confidential or sensitive, so that the data is adequately protected from theft, loss or unauthorized access or use.

If your data is sensitive, you do not want any unauthorized person to access it. In the EU, the collection of non-anonymous data for scientific research is subject to the *General Data Protection Regulation* (GDPR). The GDPR is an EU regulation on data protection. The Dutch translation of the GDPR is the *Algemene Verordening Gegevensbescherming* (AVG). The Dutch implementation guidelines are elaborated in the *Uitvoeringswet Algemene Verordening Gegevensbescherming* (UAVG). This law regulates all relevant aspects of informed consent, data collection, storage, protection, retention and destruction of personal data, as well as the rights of those individuals involved in the research. Contact a privacy champion for assistance on this subject. Certain types of data may also be bound by specific laws,[i] for example:

- Certain medical research data may fall under laws, guidelines or regulations that are designed for medical scientific research. Some examples of these are:
    - Wet Medisch wetenschappelijk Onderzoek met mensen[ii] (WMO)
    - Code of conduct for medical research[iii]
    - Good Clinical Practice Guidelines[iv] (ICH-GCP and the EU regulations for GCP)
- Quality assurance guidelines for human-related medical scientific research. Please refer to the NFU site[v] on this topic
- In the area of criminology, there are also some laws, regulations and guidelines that may be applicable
- When animal testing, animal experimentation, animal research or in vivo testing is part of the research the following are applicable:
    - The EU directive[vi] on the protection of animals used for scientific purposes
    - The Dutch law, *Wet op de dierproeven*[vii]

Within Vrije Universiteit Amsterdam (referred to below as VU Amsterdam), staff in various roles can support you with issues relating to privacy and security when you are preparing your research:

Role	First line of contact for …
Data steward/ Research Data Management Officer	Research data classification, contact with technical 2nd line for data management plan, general support, promoting quality data, teaching about FAIR principles (1st line)
Privacy champion	Privacy-related questions and issues, assistance with privacy-related products

Domain teams (research)	IT assistance on capacity for security-related products such as security plans
Information Security Officer RDM	Technical security-related questions and issues, assistance with data protection plan (2nd line)
IT servicedesk	Security-related incidents, assistance with applications and services provided by VU Amsterdam
Ethics committee[viii]	For advice on ethical issues concerning research involving human participants

3. INFORMATION SECURITY AT DIFFERENT STAGES OF YOUR RESEARCH

3.1. AT THE START: CLASSIFY YOUR DATA

The AVG requires that there is a description of what and how personal data is going to be used. It also requires that appropriate organizational and technical security measures are in place to protect this data. Grant providers and collaborative research with third parties might set these requirements, but it is important to assure proper data protection not limited to these requirements.

There are a few basic questions that must be answered:

- What is the classification level of your data with respect to confidentiality, availability and integrity (CIA)?
- What personal data are we collecting and is this allowed by law?
- What is the impact of data collection on the privacy of an individual? In other words, what risks to the rights of data subjects are encountered in the processing of personal data? The Data Protection Impact Assessment[ix] (DPIA) is the instrument used to assess this risk.
- What is the impact of data collection on VU Amsterdam?

One of the questions to be asked is whether personal data will be collected, such as names, email addresses, IP addresses, phone numbers, geolocation data or photographs of people. Take into account that a combination of several kinds of data may result in personal data as well. If so, the first two questions need to be analysed and administered respectively in a data processing register, and in some cases a DPIA must be executed. A privacy officer can assist you to answer these questions, and determine which documents need to be delivered.

Example 1
A date of birth is not considered to be traceable to an individual person. A combination of a date of birth and a postal code is traceable to one person in nearly all cases. Therefore, the combination of these two items is considered personal data.

Example 2
A combination of age, gender, race and education can lead to the identification of an individual person.

Whether the research has personal data involved or not, it is advisable to carry out a CIA classification in all cases. This classification entails an analysis which provides insights about confidentiality, integrity and availability; in other words, it provides insights into the level of security required. Confidentiality ensures that sensitive information is only disclosed to authorized parties; integrity prevents unauthorized modification of data; and availability guarantees the data can be accessed by authorized parties when requested. The output of this analysis can be used to produce a security design which will be integrated into the data management plan, or into a dedicated data

protection plan in a more complex research environment. Note, the data management plan will only be produced if the grant provider requests it.

A dedicated data protection plan may be needed when providing information for a grant. The following questions offer some direction in gathering this information:

- Is your research classified as confidential by your faculty or grant provider?
- Could your research lead to public outcry, media coverage or fines, for example, as a result of data leakage? Examples include research into environmental, political, health, sexuality or ethical issues.
- Are you using chemicals that, if misused, could harm people?
- Are there people involved who need higher levels of protection? For example, from foreign oppressive regimes, the elderly, children, refugees or LGBTQ individuals.
- Will data be collected from or shared with foreign countries, especially outside the European Economic Area?[x] There are strict rules about sharing data with or storing data in countries outside the European Economic Area. If a country does not adhere to these rules, it is prohibited to share or store personal data in that country. The privacy champion of your faculty can help you to interpret the rules concerning your research.

You should always consider protected storage of your data and reports, and think about who you can share them with. The following table indicates how your data might be classified:

Vrije Universiteit Amsterdam Information Risk Classification Scheme			
	Level of classification	**Implication of classification**	**Example of VU data**
Confidentiality	Confidentiality **Low**	• The data are 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.	• VUnet ID • Information available on VU Amsterdam websites accessible without VUnet ID authentication • Free public sites or libraries
	Confidentiality **Medium**	• The data should only be available 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 VU Amsterdam. • The data contains sensitive information about individually identifiable people.	• Unpublished research data • Engineering, design and operational information regarding VU Amsterdam infrastructure • Project administration • Non-public contracts and policies/manuals
	Confidentiality **High**	• The data should only be available to a specific group. • Protection is required by law/regulation. • VU Amsterdam 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 VU Amsterdam. • Using this data may have a significant impact on an individual's life.	• Staff employment applications, personnel files, benefits, salary, personal contact information • Patient records • Credit card numbers/bank account details • Copy passport, driver's licence • Health information/e-health app • Intellectual property • Crime records, court cases • Data on sexual behaviour/illegal drug use • Passwords • Big data analysis • Profiling
Integrity	Integrity **Low**	• You accept some errors in your data or analysis.	• Research data with a certain degree of faulty entries tolerated • Information in surveys entered by a subject • Manipulation of data by an unauthorized person
	Integrity **Medium**	• You find some errors acceptable and it would have a mildly adverse impact on your research goals, safety, budget, or reputation of your research group, faculty or VU Amsterdam.	• Research data with a very limited toleration of faulty entries, and impact on the research results
	Integrity **High**	• 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 VU Amsterdam. • 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 VU Amsterdam. • After publication of the research findings, any modification in the	• Biomedical research • High-risk chemical experiments • Patient records

		research archive is unacceptable.	
Availability	Availability **Low**	• Loss of the availability of the data is no problem, as the process can be postponed. • The data may be unavailable up to one week due to issues with the application or database.	• Publicly available and easily accessible dataset, software, hardware
	Availability **Medium**	• Recovery of data after the unavailability of the data 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 VU Amsterdam. • The data may be unavailable up to one day.	• Data, software, hardware that is replaceable within a short timeframe
	Availability **High**	• The data may be unavailable for one hour only. • Some projects need to be online 24/7 as being offline will affect the data and the results immediately.	• Patient life-support systems • Real-time big data analytics

3.2. DATA COLLECTION STAGE

After determining which data is needed for your research, you need to take the appropriate security measures. These must fit the level of CIA classification of your data. The security measures will be part of a data management plan, or, in the case of a more complex research project or environment, it is highly recommended that a separate data protection plan is written. A data protection plan contains the minimum set of security requirements, the set of security measures implemented and, if applicable, the security risks that will not be mitigated. A dedicated Information Security Officer for RDM within the IT department will serve as a second line for the Data Steward. The aim is to help and advise in making a data protection plan, if needed. Complexity may occur when, for example, various methods are used to collect the data; the data is stored in multiple databases; or it is a high-risk research project involving collaboration with multiple national/international universities.

The data protection plan will provide input on the way in which the data is collected; for example, whether it is on premises or in the cloud, and the minimum of security measures needed. It will also provide input for negotiations with third parties (if applicable), as it will stipulate the security measures and reporting required. This will result in a data processing agreement with a third party, which is mandatory by law. This agreement includes security measures (Annex 3) that must be taken by the supplier of the service or application.

If a countermeasure is not feasible, a different solution must be found. This may result in another countermeasure, or a formal acceptance by the data owner (Risk Acceptance Form – RAF). If this occurs, it is highly recommended that you consult the dedicated Information Security Officer RDM.

Please take into account that there are cases in which IT capacity can only be claimed through domain teams ('domein teams') and a budget must be allocated for the hours spent by the advisor. For more information about domain teams, visit the intranet site on this topic.[xi]

3.2.1. SURVEY TOOLS

When you select a survey tool, make sure you read the terms and conditions and licence agreement of the tool provider. Contract management can assist you in this process. The terms and conditions should inform you about:

- Where the provider stores your data (Is it stored in Europe or in a country accepted by the EU?).
- Whether the provider uses the data for commercial activities.
- Which measures the provider takes to provide data protection for your respondents.
- On which terms the application or service may be used. Sometimes a free app may only be used by consumers and not by businesses.
- The licence agreement should inform you how a product or service may be used. For example, whether it can be used by organizations (or consumers only), the fee that must be paid and under which circumstances, and how long the application or service may be used.

VU Amsterdam holds a licence for Qualtrics as a standard survey tool.

3.2.2. VOICE RECORDINGS

- Where possible, the name and other directly traceable information of the interviewee must not be recorded in the audio file.
- An encrypted device must be used for recording, for example an Apple iOS device such as an iPod touch, iPhone or iPad with activated device encryption. Where high-quality audio is required, twin microphones and more than one recording device (e.g. for backup) are required. If encryption is not possible, data must be downloaded to an encrypted device as soon as possible and be erased from the original device immediately. It is highly recommended that a wiping app is used to ensure the data has been erased permanently.
- 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. If this is outsourced to a third party (e.g. automated application, specialized service) a processor's agreement is required. Contact your privacy champion for information if this applies to you.
- The identity of the participant must be pseudonymized in the transcript, unless explicit consent has been obtained to maintain this identity.
- Transcripts must be securely stored in a locked cabinet or at an appropriate digital location (see §3.2.5).
- Transcripts or voice recordings held outside the approved university systems must be stored on an encrypted device for temporary storage only. They must be transferred to VU Amsterdam systems and deleted permanently from temporary storage as soon as possible.

3.2.3. SENDING AND RECEIVING DATA FROM THIRD PARTIES

In some cases, researchers may need to share files because they collaborate with parties within or outside VU Amsterdam (e.g. for secondary data collected with consent from other parties). VU Amsterdam offers various services to support this, but not all services are suitable for all types of data. This is why CIA classification is an important instrument in determining a suitable data-sharing tool, as more security controls must be in place for more sensitive data.

The most commonly used application to send or receive files is email. Internal emails sent to and from ***@vu.nl addresses are considered safe.[1] However, when emails are sent to external parties, security cannot be guaranteed without additional security measures. Therefore, you should avoid sending confidential data or files by email without additional security measures such as ZIVVER, an encrypted file and a password sent separately or a certificate. In the matrix below, you can see which measures are considered secure according to VU Amsterdam standards.

Email collaboration			
	Hosted by	Collaboration	
		Within VU	With 3rd party
VU Outlook email	IT	√	X
VU Outlook with encrypted attachment/ZIVVER	IT	√	√
VU Outlook with certificate	SURF	√	√

The information in this table is indicative, and not yet final. In a project, yet to start, the above IT services will be analysed to determine the exact CIA classification level of the IT service. As a result the appropriate compliance documentation and security controls has to be applied to the service.

[1] Email between VU accounts is considered secure, as these messages are routed between internal servers only. However, be careful, as there is a risk that documents will be stored within the email application, and it is easily forgotten that they need to be removed. Therefore, it is preferred that encryption or SURF filesender are used as well.

In addition to this matrix, the following will ensure a more secure use of email:

- Do not send or request that anyone send confidential files or files with sensitive personal data by email. Email is not a safe medium and therefore one must be cautious about using it for data transfer.
- Should you send or receive confidential or personal data by email accidently, transfer the data to a secure medium, as listed in §3.2.5. Delete the email from all folders in the email application (e.g. Inbox, sent items, bin) and inform the other party so they can also delete these items from the application.
- In some cases, sending (confidential) personal data is considered a security incident or data leakage (e.g. a list of interviewees with names, addresses; a list of marks for a test and/or to a wrong receiver). If this occurs, this must be reported to the IT servicedesk because VU Amsterdam is obliged to investigate the incident and in some cases report it to the authorities within 72 hours.
- Use SURF filesender or suggest that the third party delivers the files with SURF filesender (with encryption) as provided by VU Amsterdam. A third party can use SURF filesender if they have a contract with SURF or when receiving a voucher sent by you. The encryption key to the file must not be sent in the same email, but instead in two separate emails or by email in combination with the code sent by text message. See also §3.3.
- Use SURF drive or suggest to the third party that they upload the files to SURF drive as provided by VU Amsterdam.
- Use ZIVVER or suggest to the third party that they use ZIVVER. This add on to email applications supports secure emailing and is provided by VU Amsterdam.
- Access and download the data directly from the supplier's systems using a secure connection. As VU Amsterdam has services to share data, other organizations have similar options as well; for example, an own storage and collaboration facility from which the data may be securely downloaded.
- Portable media (external hard disks, USB sticks, recorders, etc.) should be encrypted when used to store personal or sensitive data and should be stored in a locked cabinet and destroyed when no longer needed.
- Encrypt your data with a tool such as Veracrypt. Contact the Research Data Management specialists at the University Library (rdm@vu.nl) if you have questions about installing Veracrypt.

3.2.4. ENABLE DATA SHARING AND COLLABORATION

VU Amsterdam offers various services to support collaboration between parties, as this is fundamental to many research projects. Collaboration means that other researchers may need to have access to your files. If data must be shared between parties, not all services may be suitable for all types of data. Data classification is used to determine which service must be used. In addition to email, as described in § 3.2.3, there are also other options for sharing data and/or files in a secure manner, both within VU Amsterdam or between VU Amsterdam and third parties.[2] VU Amsterdam provides the following services:

[2] When collaborating with other parties, a joint controller agreement is advisable as this allows the various parties to acknowledge and agree to their responsibilities regarding the data under the GDPR. This, of course, only applies when the GDPR applies. Contact your privacy champion for more information.

Data sharing / Collaboration				
	Hosted by	Collaboration		Access rights controlled by
		Within VU	With 3rd party	
VU-network G:	IT	√	X	you
VU-network projectfolder	IT	√	X	you
Google Apps VU	IT	X	X	you
VU SQL database	IT	√	X	you
SURF drive	SURF	√	√	you
EDU groups	2AT	√	√	you
Secure file server	IT	√	√	you
SciStor	IT	√	X	you
SciCloud (virtualization platform)	IT	Depending on the application being virtualized	Depending on the application being virtualized	you
SURF filesender without encryption	SURF	√	√	
SURF filesender with encryption	SURF	√	√	

The information in this table is indicative, and not yet final. In a project, yet to start, the above IT services will be analysed to determine the exact CIA classification level of the IT service. As a result the appropriate compliance documentation and security controls has to be applied to the service.

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

3.2.5. WHY CAN'T I USE FREE SERVICES FOR FILE SHARING?

Below, we list some general risks associated with putting your data into services such as WeTransfer, Dropbox, Google Drive or OneDrive:

1. Using these services may result in data being stored outside the European Economic Area (EEA). Essentially, personal data may not be transferred outside the EEA by law (GDPR/AVG). Exceptions can be made under specific conditions.
2. Using these services is beyond the control of VU Amsterdam and therefore may result in data breaches, loss of data, conflicting privacy laws in other countries and, as a result, non-compliance to the GDPR/AVG.
3. Foreign governments may, by law, have permission to access, remove and use the data you put in such facilities.
4. There is no guarantee of data confidentiality. The data may or may not be held in the manner you expect.
5. There are no safeguards about the continuing existence of the data and no guarantee that the access rights you set will be maintained.
6. The data may be altered or corrupted without your knowledge, and you won't have any way of getting uncorrupted copies back.
7. There is no guarantee of data availability (i.e. if the files are accidentally deleted, there may be no backup). There is also no guarantee of the service continuing to exist.
8. Most cloud storage providers do not guarantee the removal – permanent or otherwise – of data.

9. Most cloud storage providers do not allow auditing of who has accessed or downloaded your data.
10. During your employment contract with VU Amsterdam, your work is the intellectual property of VU Amsterdam. There is no way for VU Amsterdam's IT department to retrieve files from your personal cloud storage in the case that you should leave VU Amsterdam, fall ill, or lose your password. This could lead to data loss for VU Amsterdam. Therefore, uploading data to such tools is at your own risk.
11. External administrators can access ANY content used within their service, and if their access is compromised, it means all data is automatically at risk of compromise.

3.2.6. STORE YOUR DATA APPROPRIATELY DURING RESEARCH

Not all IT facilities provided by VU Amsterdam are suitable for storing high-risk data. The following table shows what services are advised for various risk types.

Data storage			
	Hosted by	Types of files	
		Personal	Business
Personal device	IT	√	X
VU-network H:	IT	√	√
VU-network G:	IT	X	√
VU-network projectfolder	IT	X	√
Google apps VU	IT		X
VU SQL database	IT		√
SURF drive	SURF	√	√
EDU groups	2AT		√
Portable data storage			√
Secure USB with PIN			√
SciStor	IT		√
SciCloud (virtualization platform)	IT		√

The information in this table is indicative, and not yet final. In a project, yet to start, the above IT services will be analysed to determine the exact CIA classification level of the IT service. As a result the appropriate compliance documentation and security controls has to be applied to the service.

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

3.2.7. PREVENT UNSECURE 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 advice:

- Never provide others with your login credentials. This is considered to be a security incident.
- Be aware of social engineering: no reliable organization will ever call you and ask for your login credentials. Also, respond by informing security when you see unknown people and suspicious behaviour.

- Be aware of SPAM and phishing emails: always check the email address of the sending party and do not click on suspicious links. Inform the IT servicedesk by sending the SPAM email as an attachment.
- Have a strong password or passphrase.
- Do not connect any insecure, personal devices to VU Amsterdam's network.
- Free public Wi-Fi is insecure, as these networks are generally unrestricted and can be abused to gain access to internet traffic and/or devices in the present and the future. When there are no other options, it may only be used with a VPN-client provided by VU Amsterdam and/or a digital platform (e.g. Citrix).
- Use Eduroam where available, see: www.eduroam.org/where/.
- Make sure your virus scanning application is always up-to-date and running on all devices. If a virus scanning application has been switched off, this might be a sign that your device has been breached. Contact the IT servicedesk for assistance.
- Create backups of your files, especially when your data requires high availability. VU Amsterdam automatically creates backups of your network folders (G:, H:) and storage such as SciStor and SURF drive. Make sure your backups are also secure.
- Do not use free cloud solutions (such as Dropbox or WeTransfer) for storage or file sharing for work related to VU Amsterdam. There is no VU Amsterdam support for these services, nor can privacy and security be guaranteed. Among other services, VU Amsterdam supports:
    - For file transfer, SURF filesender and ZIVVER. See §3.2.3 and §3.3.
    - For storage, SciStor, G: and SURF drive. See §3.2.5.
- Do not leave unsecured copies of your data lying around. Consider a clean desk a secure desk. Store paper files with personal data in a locked cabinet.
- Encrypt your device. Most devices have built-in encryption tools for storage, for example. Always check that the encryption is valid. When no valid encryption is available, Veracrypt is considered a good alternative.
- 'Need to know' is a basic privacy principle, which states that you should never send more data than needed for the task to be fulfilled. Parts of the data that are unnecessary for the task to be fulfilled should be removed, anonymized or aggregated.
- Lock your computer when leaving it, even if it is for a short time. You do not know who might have access to your computer during your absence.
- Lock your laptop to the desk to prevent it being stolen.
- If necessary, ensure that physical access to your office or research facilities is granted only to people who are authorized to be there. Lock your door when leaving the room.

For more information: VUNET or cybersaveyourself.nl

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

Some general risks involved in collaborative data sharing were listed in §3.2.4, such as the use of WeTransfer. The same risks apply to cloud solutions for storage such as Dropbox, OneDrive or Google Drive.

3.2.9. ANONYMIZING DATA

Pseudo-anonymizing or anonymizing research data may be necessary for various reasons (e.g. data security, research integrity). In general, such measures make it more difficult to identify an individual, or prevent identification of an individual altogether. There are various forms of data anonymization.

- Masking data: this involves determining what can be seen of the dataset on a database level. Data which cannot be seen, will be 'masked' for the user. The data, however, is still available.

- Pseudo-anonymizing data: in this case, certain data in a subject's profile is interchanged with data from another profile from the same dataset, or fictionalized. This is considered not to be completely anonymized, because there is a stored key.
- Anonymizing data: in this case, the data in a profile in a database has been irreversibly removed or changed to fictional data.
- Aggregate data: involves the merging of data to form groups. These groups must be large enough to prevent traceability to one individual.

In most cases, a combination of security measures must be in place to ensure that you store your data in a sufficiently secure way. For example, you might split a file into two files: one with traceable personal information and one with non-personal or traceable data as input for your research. Both can be linked by an algorithm or key which is kept secure. For example, the key can be kept at a different location, or parts of the key can be held by different team members. Using this method, it is possible to guarantee the substantiation of your research without directly identifiable data. A research data management officer or data steward can support you in determining the appropriate form of anonymization.

3.3. SECURING YOUR DATA AFTER YOUR RESEARCH

Archiving	
	Hosted by
ArchStor	IT
DarkStor	External
DataverseNL	External

The information in this table is indicative, and not yet final. In a project, yet to start, the above IT services will be analysed to determine the exact CIA classification level of the IT service. As a result the appropriate compliance documentation and security controls has to be applied to the service.

Data archiving: contact the Research Data Management specialists at the University Library (rdm@vu.nl) if you have questions about data archiving.

- VU Amsterdam offers three repositories for long-term data archiving, with different properties:
  - DataverseNL: an online platform for the analysis and publication of research data in a semi-open environment.
  - ArchStor: for verification purposes only, not suitable for sensitive (e.g. privacy, copyrighted) data.
  - DarkStor: offline archive for verification purposes only, suitable for sensitive (e.g. privacy, copyrighted) data.
- Repositories outside VU Amsterdam may also be used to archive your data. A registry of repositories can be found on re3data.org. Some are very general, while others serve a specific discipline. Not all repositories score equally well on important requirements for long-term data preservation.
- More information about data archiving and the facilities that VU Amsterdam offers in this respect can be found on VUnet.

- Wiping of data and destruction of devices: erasing data does not result in its permanent removal. In fact, the file has only been delisted in the index. This poses a risk, especially when a device is not used anymore or will be used by someone else. Contact the IT servicedesk for support with permanent wiping of a device or the destruction of a device.
- Delete the access rights of people who no longer need your files and data.

4. KEEPING RESEARCH DATA SECURE OUTSIDE VRIJE UNIVERSITEIT AMSTERDAM

VU Amsterdam research carried out external to VU Amsterdam property can take place in a wide variety of settings, some of which may pose considerable challenges for upholding the promise of confidentiality and keeping data stored securely.

At all costs, avoid the storage of large sets of research data, particularly with personal data, on any device while travelling or working outside VU Amsterdam. Some countries may copy the data on a device even without a warrant.

Also check §3.2.7 to ensure data connections and storage during travel are secure.

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 the choice of paper documents might also be a solution in situations in which the use of a computer is difficult or inappropriate, or simply impossible because of limited access to electricity. In situations such as this, researchers who need to keep their data and consent forms confidential, must consider how to protect their paper documents and notes in the best possible way while travelling. In some cases, simple precautions, such as physical separation of consent forms from research data, may be sufficient. In other cases, researchers may wish to take prepaid, pre-addressed shipping envelopes, so that they can send their documents back to VU Amsterdam or some other secure collection and storage point as quickly as possible.

4.2. INTERNATIONAL TRAVEL AND ENCRYPTION

Almost all laptops issued by VU Amsterdam use encryption technology that protects the privacy of the information that resides on them. 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.

When travelling 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 enters or exits their borders. Some countries ban, or severely regulate, the import, export or use of this technology. Travelling to certain countries with your laptop with encryption software installed on it could lead to your imprisonment, or lead to your laptop or other devices being confiscated. In some cases, it may be better not to bring a device at all. Also, be sure a mobile device does not contain files with confidential data. The following sections provide a summary of the important points to remember. For more information, you can visit the website of NCSC.nl.

4.3. THINGS TO REMEMBER WHILE TRAVELLING

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

- Do not trust public or hotel Wi-Fi: use Eduroam where available, see: www.eduroam.org/where/. Or use a VPN-client (if allowed by law), see https://www.surf.nl/eduvpn-maak-onveilige-verbindingen-veilig.
- Be sure all applications on the device are updated with the latest available patches and (virus) libraries.
- By not logging into VU Amsterdam applications while travelling, you eliminate the risk of your ID and password being captured and used to compromise VU Amsterdam's 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 Amsterdam 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 if a file was forgotten during preparations.
- Please note that using Remote Desktop or equivalent software to access, for example, Citrix, your University desktop or other device from a high-risk country should also be avoided, as these transmissions may also expose valuable information (e.g. countries where encryption is prohibited).
- Avoid using public workstations. The security of public workstations 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, and always make sure you actively close the application or service properly by logging out instead of closing the browser. Also delete search history, cookies, etc. within the browser when leaving a public workstation. This setting is available in most browsers.
- Be aware of your surroundings when logging in or entering data into your devices. There have been many cases where an ID, password or a piece of confidential information has been compromised simply by watching the person input the information. Be discrete when entering your ID and passwords.
- Notify VU Amsterdam if a theft or loss occurs. Travelling 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 areas where the distractions are 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. If a laptop or mobile device is lost or stolen, contact the IT servicedesk.
- Never let others make copies (hard or soft) of files. The risk of abuse is high. Always keep files in sight. For example, in some countries a copy of your passport is requested for your stay. However, make sure you never lose track of your passport. Also, be sure to watermark the documents copied and censor all information which is not needed.

4.4. WHEN YOU RETURN

- Change any passwords you may have used during your travels. When travelling, 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 travelled to trusted versions. When our devices connect to a network, there is an increased likelihood that the device will be compromised and have malicious software installed. This software can then compromise information and other devices on VU Amsterdam's network when the device is reconnected to the University's network. The IT servicedesk can assist with this procedure.

5. WHAT TO DO IN THE EVENT OF A DATA BREACH?

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, VU Amsterdam may be required to notify the Autoriteit Persoonsgegevens within 72 hours of discovering a data breach involving personal data.

Anyone at VU Amsterdam 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.

More information regarding data breaches and other security incidents can be found on VUnet.

LIST OF IT SERVICES

List of IT applications (IT services) that need to be classified on the confidentiality, integrity and availability. These classification levels determine how suitable the specific IT service is for handling the research data in terms of confidentiality, integrity and availability.

1. VU outlook mail
2. VU outlook with encrypted attachment/ZIVVER
3. VU outlook with certificate
4. Google Apps VU
5. VU SQL database
6. SURF drive
7. EDU groups
8. Secure file server
9. SciStor
10. SciCloud
11. SURF filesender without encryption
12. SURF filesender with encryption
13. VU network H:
14. VU network G:
15. VU network projectfolder
16. Portable data storage
17. Secure USB with PIN
18. ArchStor
19. DarkStor

[i] The legal framework for medical scientific research can be found at: https://english.ccmo.nl/investigators/legal-framework-for-medical-scientific-research/laws

[ii] Please refer to this site to check whether your research is subject to the Wet Medisch wetenschappelijk Onderzoek met mensen (WMO): https://english.ccmo.nl/investigators/legal-framework-for-medical-scientific-research/your-research-is-it-subject-to-the-wmo-or-not

[iii] The code of conduct for medical research can be found at: https://www.federa.org/sites/default/files/bijlagen/coreon/code_of_conduct_for_medical_research_1.pdf

[iv] The guidelines for good clinical practice can be found at: https://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6/E6_R1_Guideline.pdf

[v] NFU Nederlandse Federatie van Universitair Medische Centra publishes guidelines to regulate the quality of medical scientific research in which humans are involved. This is a Dutch site: https://www.nfu.nl/img/pdf/NFU-12.6053_Kwaliteitsborging_mensgebonden_onderzoek_2.0.pdf

[vi] The EU directive on the protection of animals used for scientific purposes: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010L0063

[vii] Wet op dierproeven, this is a Dutch site: https://wetten.overheid.nl/BWBR0003081/2019-01-01

[viii] Committee on ethics: https://vunet.login.vu.nl/services/pages/practicalinformation.aspx?cid=tcm%3a165-858762-16

[ix] Data Protection Impact Assessment, DPIA

[x] To determine if a country outside the EU has proper data protection, see chapter V, which focuses on the AVG: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[xi] Intranet site on domain team: https://vunet.login.vu.nl/organization/pages/organization.aspx?cid=tcm%3a165-312557-16