Research Data Management Policy
Faculty of Law

Version: 1.0
Date: 9 July 2019
Introduction

*Research data* are defined as recorded information that is necessary to support scientific research. This may involve, for example, text, images, sound, databases, statistical data, geographic data, etc. *Data management* involves organizing, documenting, protecting and distributing any data. Responsible data management is part of good research. Vrije Universiteit Amsterdam (VU) has adopted a Research Data Management Policy which summarizes the general university-wide principles for the careful handling of research data. Each faculty of VU is requested to formulate faculty specific supplemental policies that comply with central policy. The following document describes the Research Data Management Policy of the VU Faculty of Law (hereinafter: the “**Policy**”) and aims to clarify what are the responsibilities of researchers regarding their research data. Please note that an advice of the faculty’s Ethics Committee for Legal and Criminological Research (CERCO) is often mandatory before you start collecting your data.

Definitions

**Confidential Data:** Data that are sensitive and need to be protected from unauthorized access. We use the traffic light categories Red, Orange and Green for the different categories of confidentiality. The term Confidential Data as used herein refers to Red and Orange Data, not to Green data.

| Red Data: High risk data – the loss of confidentiality could have a significant adverse impact on your research goals, safety, budget or reputation of your research group, faculty or VU. This category includes special categories of Personal Data such as data revealing racial or ethnic origins, political opinions, religious beliefs, data concerning health, crime records. It also includes passwords and encryption keys. | Orange Data: Moderate risk data – the loss of confidentiality could have a mildly adverse impact on your research goals, safety, budget or reputation of your research group, faculty or VU. This category includes pseudonymized Personal Data, i.e. data without the obvious personal details, but people can still be traced should you combine information. | Green Data: Low risk data – the loss of confidentiality will have no adverse impact on your research goals, safety, budget or reputation. Green Data are not considered Confidential Data. |

**Dutch Implementation Act:** Dutch General Data Protection Regulation Implementation Act (UAVG) of 16 May 2018 and in force as of 25 May 2018, containing rules on the implementation of the GDPR.

**EEA:** The European Economic Area, consisting of European Union member states, Iceland, Liechtenstein and Norway.

**Effective Date:** 9 July 2019


**Personal Data:** Any information relating to an identified or identifiable natural person. A natural person can be identified directly based on identifiers such as the natural person’s name, date of birth, address,
photographs and/or voice recordings. Identification can also be indirect. This means that data which do not lead to direct identification of a person but by which, using reasonable means, a person can still be identified must also be considered personal data. Example: a research participant number and key list, or the combination of a postcode and house number.

Aim of this Policy
1. The aim of this Policy is to help researchers of the Faculty of Law ensure:
   i. they comply with legal and ethical requirements regarding their research data, including the Netherlands Code of Conduct for Research Integrity;¹
   ii. they comply with the provisions of the GDPR and the Dutch Implementation Act regarding personal data;²
   iii. their research data are reliable, traceable and securely stored throughout the data life cycle;
   iv. they meet the requirements of research funders and scientific journals concerning quality and traceability of data.

Applicability, responsibility
2. This Policy applies to all researchers employed by or affiliated with the Faculty of Law, including all (internal and external) PhD candidates. Supervisors of BA and MA students are formally responsible for their students’ data handling.

3. This Policy applies to all scientific research initiated after the Effective Date and aimed at resulting in a (e-)publication, for example in a scientific or professional journal, as a book, a book chapter, on a website or research platform.

4. The provisions contained herein will be relevant mostly to research that includes Confidential Data. If you are engaged in empirical legal research (in the broadest sense, including both quantitative and qualitative research), the provisions certainly apply. Even if you only work with Green Data, for example in the context of legal doctrinal research, some provisions may still be relevant.

5. Each individual researcher is responsible for complying with this Policy and general VU data management guidelines. If this Policy lacks specific guidelines for certain cases, researchers are expected to act in the spirit of it.

¹ See http://www.vsnu.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf
6. A proviso holds for research that builds on previous research for which the data gathering process was initiated before the Effective Date. Researchers should comply with this Policy as far as is reasonably possible. Notwithstanding the foregoing, researchers should always comply with legal constraints (e.g. for privacy sensitive data).

**Faculty principles**

7. The following faculty principles for data management can be distinguished: **safety, accountability** and **compliance**. The remainder of this Policy further elaborates on these principles in more detail.

   i. **Safety** is realized by ensuring data is stored securely (preventing non-authorized access) and with some level of redundancy (no data is permanently lost for instance in case of a single hardware malfunction, accidental deletion, loss of a storage device, a fire or flooding).

   ii. **Accountability** is achieved through safe and secure data storage. It means that a researcher if necessary is able to reproduce results from publication using the original data sources. It is also about storing data in a well-organized manner with sufficient meta-data available to be able to quickly re-use the data or replicate the experiment, simulation or analysis.

   iii. **Compliance** with legal and ethical norms regarding research data requires for example that the processing of personal data is only possible under strict conditions as defined in the GDPR and Dutch Implementation Act.

   This policy encourages **reusability** and even **shareability** of research data according to the principle: *As open as possible, as closed as necessary.*

8. Notwithstanding that most funding organizations require ex-ante a written **data management plan** for grant approval, this Policy encourages ex-ante written data management plans for all of its research. Planning data management will save time, money and effort.

9. Researchers who are engaged in a complex research project involving large datasets should consider earmarking money in the research budget for information security.

**Ethical review**

10. The faculty’s Ethics Committee for Legal and Criminological Research (CERCO) safeguards the ethical standards of all research involving human participants that is conducted at the Faculty of Law. Before any research involving experiments and/or interviews with human respondents commences, approval of CERCO must be obtained. Researchers should document their correspondence with CERCO. Researchers must make sure to obtain and archive the active consent of their respondents. Respondents have the opportunity and means to withdraw their active consent at any moment and leave the experiment from that moment onwards. Withdrawals should be noted in the data documentation.

---

3 See also the H20 Online Manual on Open Access and Data Management: [http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm](http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm)
Collecting and documenting data

11. Both data and the data gathering process should be well documented, such that both are (in principle) verifiable. The documentation should preferably be part of the published research itself, for example a Materials and Methods section of the publication, or (online supplemental) appendices of the published work. If not, the researcher should provide detailed supplemental README files and archive these securely along with the data. The documentation on the data gathering process should be sufficiently detailed and include at least:

   i. details on the process of gathering the raw data (including survey data, interviews, video material, experiment scripts, details/code on how web sites were scraped, etc., if applicable);
   ii. detailed metadata, including descriptions of the variables (possibly also with database tickers/acronyms in case databases of third parties have been used, and including details on the interpretation of the variable input (e.g., does 1 indicate male or female as a gender dummy));
   iii. details on filters and data manipulations used to get from the raw data to the data used for the empirical analysis, for example details on how recorded interviews were transcribed and coded, how data were pseudonymized and in what way the survey responses have been cleaned;
   iv. ethical clearance (if needed; see point 10 above and the Faculty of Law’s Code of Ethics⁴);
   v. details on how privacy issues are dealt with (if Personal Data are involved);
   vi. details on how access to the data is arranged and ensured (at least for internal purposes) for the minimum period of 10 years.
   vii. An empty informed consent form if applicable.

Storing and archiving data

12. For ongoing research, data should be stored securely and professionally. The principal researcher writes a data management plan before starting up a research project. The principal researcher should take care of the continuity of the research by keeping the data, documentation and access rights up to date throughout the project. Researchers have to make back-ups of the data regularly. Storage solutions offered by VU (Group drive, home folder, project folder, SciStor, Surfdrive) are backed-up daily but if you use your own device (f.e. laptop, USB), back-ups have to be made manually. If you need assistance, contact the IT Servicedesk.

13. Upon publication, researchers archive their raw and processed research data, unless compliance issues arise (e.g., license issues), or storability becomes an issue (for some large data sets; see later in this document). Archiving means: to store data on a secure system, together with the data documentation (see point 11 above). To comply with VU policies, research data that are not relevant for further research need to be archived securely for a period of 10 years. Data that cannot

---

⁴ See https://vUNET.login.vu.nl/_layouts/SharePoint.Tridion.WebParts/download.aspx?cid=tcm%3a164-300366-16
(Dutch version only)
be archived, e.g., due to legal constraints, should still (in principle) be verifiable by archiving the data documentation (point 11 above).

14. Secure storage and archiving is meant to imply there are measures preventing data loss (using back-up facilities and proper hardware maintenance) and data leakage. Recommended (fee-based) solutions for storing (and sharing) ongoing research data are listed in Annex 1. Researchers affiliated with NSCR who process Personal Data are recommended to use NSCR Secure Analytics Lab (SAL), an offline storage facility.

15. Portable media such as USB sticks, external hard drives and recorders should not be used for long-term storage. The use of these devices is permitted for short-term purposes only (f.e. transport of data) and provided the device is encrypted. Portable media should always be stored in a locked cabinet. Confidential Data should be removed from these devices when no longer needed.

16. When research has been completed, you should archive the final version of your research data and documentation. Only authorized individuals can request access to the data, i.e. the original researcher or a research coordinator. Recommended (fee-based) solutions for archiving research data are listed in Annex 2.

We advise against using archiving solutions where the individual researchers pays a fee for the storage facility to continue its services: in this case the storage depends on the availability of the individual researcher for the period of 10 years. A researcher could only use this facility when the financial commitment is transferred to the researchers department.

17. Research data are stored as much as possible in a digital format, not on paper. File formats and other standards should be suitable for long-term preservation and accessibility, the so-called Preferred Formats: .pdf, .txt, .csv, etcetera. Also for picture or movie material the most long-term resistant format should be used. The documentation accompanying the data contains information on the file formats and software versions used. For a list of open standards, please see the Forum Standaardisatie website.5

18. Data owned by the researcher should be licensed to VU for the minimum duration of 10 years for at least purposes of research verification.

19. Department heads are responsible for making arrangements with researchers about managing their research data and documentation in the event of termination of their employment at VU.

Data sharing

20. Confidential Data may only be shared with others in a safe manner and on a ‘need to know’ basis. Recommended solutions for sharing research data are listed in Annex 1.

---

5 [https://www.forumstandaardisatie.nl/open-standaarden](https://www.forumstandaardisatie.nl/open-standaarden)
21. In addition, Confidential Data may be transferred by using **SURF Filesender** (https://www.surffilesender.nl/, for encrypted files < 2GB), **Zivver** (an e-mail encryption tool, available within VU per May/June 2019), via SFTP (Secure File Transfer Protocol) or by using a secured USB-stick or other storage device. Confidential files that are transferred outside of VU should always be encrypted.

22. Confidential Data may be shared via regular e-mail **within** the VU network but not outside of VU without additional security measures (such as encryption with Zivver).

**Personal Data**

23. Research involving the processing (e.g. collection, storage, analysis, sharing) of **Personal Data** is subject to the GDPR and the Dutch Implementation Act. Researchers shall at all times comply with the GDPR and the Dutch Implementation Act. Researchers who collect and process Personal Data in their research must notify the faculty’s Privacy Champion. If the research involves working with respondents, it may be necessary to draw up an informed consent.

24. In accordance with the GDPR, researchers should always adhere to the principle of data minimization, according to which they should limit the collection of Personal Data to that which is directly relevant and necessary to accomplish its purpose.

25. Researchers who collect and process Personal Data for their research must record this in a data processing register, which sets out *inter alia* (i) the categories of Personal Data being processed, (ii) the purposes of and legal grounds for processing Personal Data, (iii) data recipients, and (iv) the technical and security measures taken in order to guarantee an appropriate level of protection of the Personal Data being processed. VU uses Privacy Perfect for this purpose. If in need of assistance, contact the faculty’s Privacy Champion.

26. Besides ‘regular’ Personal Data, the GDPR also discerns **special categories** of Personal Data. The processing of special categories of Personal Data is prohibited, except in the cases specified in the GDPR and Dutch Implementation Act. Special categories of Personal Data concern for example race or ethnic origin, political opinions, religious beliefs, data concerning health or data concerning criminal convictions and offences. Finally, it is prohibited to store data containing BurgerServiceNummers (BSN).

---


7 Scientific research of **Personal Data** often involves the processing of Personal Data. Any information concerning an identified or identifiable natural person is considered Personal Data. A natural personal can be identified directly based on identifiers such as the natural person’s name, date of birth and/or address. Identification can also be indirect. This means that data which do not lead to direct identification of a person but by which, using reasonable means, a person can still be identified must also be considered Personal Data. In other words, pseudonymized data are also Personal Data.
27. When data processing activities are likely to result in a heightened risk to privacy, the researcher will perform a Privacy Impact Assessment to assess the institutional risk of the data and the required security level for storage. If in need of assistance, contact the faculty’s Privacy Champion.

28. Personal Data must at all times be stored on a secured network and in accordance with legal guidelines. Computers should always be locked if the researcher is absent. The researcher is familiar with the VUnet page on handling research data that includes Personal Data. When processing special categories of Personal Data, additional security measures are needed for storage. The researcher and his/her research group are responsible for data that can put society or our faculty at risk. Privacy-sensitive data should never be stored on unprotected data carriers (including unencrypted harddrives in password protected computers) or on synchronized cloud services (Dropbox, Google drive), particularly if these mirror to local non-encrypted hard-drives. After the research, the data can be archived on a safe, off-line server such as DarkStor to comply both with safety requirements and the minimum archiving period.

29. Researchers should, whenever possible, pseudonymize Personal Data before sharing or storing data. Keys relating the pseudonymized data to the Personal Data should be kept safely and separately and be accessible by at least three persons affiliated to VU at all times, especially after the departure of the original researcher. It is advised that next to the researcher, at least the principal researcher and two departmental secretaries (of related departments) have access to the keys, and that these keys are stored on at least two restricted locations, either physically or electronically. The locations for key storage are either physically (safe) or electronically (H: drive or other secure medium) sufficiently well secured. The database ID number of individuals cannot contain any potentially meaningful identifier (such as initials, date of birth, postal code).

30. Encryption is a preferred further security measure. Additional safety measures should meet the general requirement stipulated above, that data access should not be lost in case of the loss of a data carrier, the departure of an individual researcher, or the loss of one of the keys. In particular this means that encryption keys are available to at least two persons affiliated to VU at all times, including after the departure of the original researcher, and that data and keys are stored in at least two locations, both with strongly restricted and regulated access. Recommended encryption tools include Zivver (to encrypt e-mails), SURFfilesender (to send large files encrypted), Veracrypto (to encrypt hard drives, folders or entire storage devices), and Bitlocker (to encrypt part of a hard disk, for computers running on Windows). If in need of assistance, contact the IT Servicedesk.

31. After the research has been completed and/or the data archiving period has elapsed, all data carriers with Personal Data should be deleted in accordance with legal requirements.

32. If a researcher wants to share Personal Data owned by VU with third parties (including co-authors not affiliated with VU), the researcher should make sure to enter into a so-called data processing agreement. This is a legal obligation that is intended to ensure that Personal Data is processed in accordance with the GDPR. The VU legal office has drafted a model “data processing agreement”

for this purpose. The researcher should consult with the faculty’s Privacy Champion to be fully briefed on the requirements to share Personal Data outside VU.

33. Personal Data may be stored for more than 10 years if they will be processed solely for scientific purposes and provided that appropriate technical and organizational measures have been implemented, in accordance with article 5(1)(f) and article 89(1) of the GDPR.

34. If a VU researcher processes Personal Data owned by third parties, the researcher is responsible for safe storage as described above. The researcher should make sure that his/her role as data processor (“verwerker”) is well documented in the “data processing agreement” that is typically issued by the owner of the data. Again, the faculty’s Privacy Champion should be contacted in case of any doubt.

International transfer of Personal Data

35. Personal Data can only be transferred to countries outside the EEA (“an international transfer”) if specific legal requirements are met. An international transfer is for example constituted when Personal Data are stored on a server that is located in a country outside the EEA or when someone located in a country outside the EEA receives or has access to the Personal Data. The researcher should consult with the faculty’s Privacy Champion to be fully briefed on the requirements for international transfers of Personal Data.

36. Researchers should remove any Personal Data from their mobile devices (data carriers) when travelling outside of the EEA. Researchers should also refrain from accessing Personal Data stored on systems offered or recommended by VU from a location outside of the EEA. Contact the IT Servicedesk for advice on appropriate security measures when travelling.

37. For the processing of Personal Data collected in non-EEA countries, additional/other rules may apply. The researcher is responsible for compliance with such rules and to keep contact with the faculty’s Privacy Champion.

Scripts, codes, particular data types

38. Researchers archive their codes and scripts used to produce their research. This includes C- codes, Matlab, SPSS, SAS, STATA, Eviews scripts, etc., including a README file on the version of the language or package in which the codes were run. Finally, researchers should add a list of all files with a short description (register or table of content).

39. Secondary data are data that are collected by for instance a third party for their own research, data that are collected by companies internally, or data collected by institutions that specialize in data collection (such as CBS, Data Archiving and Networked Services (DANS), Dutch National Cyber Security Center (NCSC), Dutch National Police, Netherlands Council for the Judiciary etc.). If the data provider allows for archiving the secondary data, this is preferred. However, secondary data need not be archived if the data are (in principle) recoverable (possibly after paying a fee or establishing the appropriate contacts). The data documentation should still be archived, including the process
of gathering and constructing the raw and cleaned data. Researchers should refer to the source of the (secondary) data and DOI, and add sufficient information on how the data were obtained and accessed. Finally, details (and possibly scripts) to get from the raw (possibly proprietary or commercial) data to the data used for the empirical analysis, similar as in the standard case, are important for understanding the process. This includes the mentioning of company contacts if the data were obtained through private contacts or if agreements with the organization disallow the local archiving of the data at VU.

40. **Large datasets.** Some data sets are too large for (standard) storage. Here researchers will use the best practices in their field, and share these explicitly with either the faculty’s data manager or VU UB Research Data Support (researchdataservices.ub@vu.nl) such that the faculty can develop a more concrete policy in this area. In all cases, including big data studies, the data gathering and construction process should be documented and archived and contain sufficient details such that the published research can (in principle) be verified.

**Final provisions**

41. Non-compliance with this Policy may result in potentially significant reputational and legal risk to the individual researcher and to VU. Serious and/or persistent violations of the provisions in this document, constituting research misconduct, may result in disciplinary action.

42. Any exceptions to this Policy shall be decided upon by the faculty board upon advice of the faculty’s research board (onderzoeksbestuur), the faculty’s data manager and Privacy Champion.

**Practical guidance & support**

43. Please check the Research Cycle in **Annex 3** for a step-by-step approach to research data management.

44. Please check the website of the University Library for research data management best practices and guidelines. More information on handling research data which include personal data can be found on VUNet. For advice on storage of research data, researchers may consult Marieke Polhout, data manager of the Faculty of Law: m.j.polhout@vu.nl. For questions on research involving Personal Data, please contact the faculty’s Privacy Champion, Joost Meijer: j.m.meijer@vu.nl. Finally, VU UB Research Data Support (researchdataservices.ub@vu.nl) offers help to all VU researchers.
### Annex 1: Recommended Solutions for Storing and Sharing Data During Research

<table>
<thead>
<tr>
<th>Category of Confidentiality</th>
<th>Personal Device</th>
<th>VU Home folder (H:) (3 GB)</th>
<th>VU Group drive (G:) (units of 1 GB)</th>
<th>VU network project folder (3GB)</th>
<th>Google Apps VU (unlimited)</th>
<th>VU SQL database (units of 1 GB)</th>
<th>SURF drive (&lt;250 GB)</th>
<th>EDU groups (250 MB &lt; 5 GB)</th>
<th>Portable data storage</th>
<th>SciStor (units of 100 GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green data</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√*</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Orange data</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
</tr>
<tr>
<td>Red data</td>
<td>X</td>
<td>X</td>
<td>√*</td>
<td>√*</td>
<td>X</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
<td>√*</td>
</tr>
</tbody>
</table>

* Provided additional security measures are in place, such as management of user access rights, antivirus & encryption

| Sharing y/n | X | X | √ | √ | √ | X | √ | √ | X | √ |

### Annex 2: Recommended Solutions for Archiving Data After Research

<table>
<thead>
<tr>
<th>Category of Confidentiality</th>
<th>ArchStor</th>
<th>DarkStor</th>
<th>DataverseNL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green data</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Orange data</td>
<td>X</td>
<td>√</td>
<td>X</td>
</tr>
<tr>
<td>Red data</td>
<td>X</td>
<td>√</td>
<td>X</td>
</tr>
</tbody>
</table>
Annex 3: Research Cycle

1. Start-up research: write a data management plan in which you state which data you will (re-) use. Will you process Personal Data? Yes, go to 2. No, go to 4.

2. Consult the Privacy Champion and, if necessary, draw up a PIA together. Will you work with respondents and need an informed consent? Yes: go to 3. No, go to 4.

3. Draw up an informed consent with regards to the GDPR.

4. Ethical review necessary? Consult CERCO and mention your data management plan. Go to 5.

5. During research, archive all documentation: data management plan, CERCO request and advice, permissions from third parties, general conditions from any service you will use etc. Archive your data and describe what media you are using, which files you are producing (file list) and what variables you have. Use versioning. Go to 6.

6. Store your data according to VU RCH policy. If you are using other devices, please state why, according to the ‘apply or explain’ principle. Go to 7.

7. After research, make sure your data and documentation is complete and can be understood independently. Archive your data and documentation in a trustworthy archive as open as possible, closed when necessary.

Annex 4: Description of Storage/Sharing/Archiving Solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArchStor</td>
<td>Archiving solution. A research data archive with a 10-year retention period. Data stored in ArchStor can only be accessed for verification purposes. Green Data only.</td>
</tr>
<tr>
<td>DarkStor</td>
<td>Archiving Solution. An offline archive for storing Confidential Data. DarkStor is only suitable for data which require specific additional security. Once archived, access to the data can only be requested by authorized individuals, i.e. the original researcher or a research coordinator.</td>
</tr>
<tr>
<td>DataverseNL</td>
<td>Archiving solution. An online platform for the analysis and publication of research data in a semi-open environment. DataverseNL allows users to link publications directly to datasets, and to share it through online archives such as DANS. Green Data only.</td>
</tr>
<tr>
<td>EDU groups</td>
<td>Sharing and collaboration solution. Tool for higher education in the Netherlands. EDU groups is based on MS SharePoint 2016. Users work together via a team site. With team sites, you can, among other things, share documents, plan meetings, document projects and distribute tasks. You have a total storage space of 5 GB. Accessible via <a href="https://www.edugroepen.nl">https://www.edugroepen.nl</a> – sign in with your VU e-mail account.</td>
</tr>
<tr>
<td>Google Apps VU</td>
<td>Storing solution. May also be used to share data within VU but not with third parties. VU has an institutional agreement with Google on Google Drive/Docs. Accessible via <a href="http://accounts.google.com">http://accounts.google.com</a> – sign in with VU e-mail account &gt; select VU. Green Data only.</td>
</tr>
<tr>
<td>Group drive (G://)</td>
<td>Storing and sharing solution. The Group drive can be used to share research data with a group, either within the law faculty or with researchers in other VU faculties. Default storage capacity is 1 GB per employee, but this can be increased.</td>
</tr>
<tr>
<td>Home folder (H://)</td>
<td>Storing solution. Default storage capacity is 3 GB. It is possible to have this capacity increased, in which case the costs will be billed to the faculty.</td>
</tr>
<tr>
<td><strong>Project folder</strong></td>
<td>Storing and sharing solution. Employees and guests who work together within VU in a project or collaboration can store data in a project folder. The costs for a project folder will be billed to the applicant/manager (for example, the faculty or department that is the initiator of a project). There is 3 GB of storage capacity available per person; this can be increased. A project folder can be requested via VUNet.</td>
</tr>
<tr>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td><strong>SciStor</strong></td>
<td>Storing and sharing solution. Scistor is a VU data storage facility for research. It is a paid service which can also be used for storing Confidential Data. Not suitable for archiving. The minimum use is 100 GB for at least three months. Increasing or decreasing capacity can be done in units of 100 GB. SciStor can be requested via VUNet.</td>
</tr>
<tr>
<td><strong>SurfDrive</strong></td>
<td>SURFdrive is a personalized cloud storage service for Dutch higher education and research with which employees and researchers can easily store, synchronize and share files and data. You can log in using your VUnetID and password at <a href="https://surfdrive.surf.nl">https://surfdrive.surf.nl</a>. Every employee is granted 250 GB storage space.</td>
</tr>
<tr>
<td><strong>VU SQL Database</strong></td>
<td>Mostly for storing statistical data. The storage capacity is 1 GB by default. It is possible to request extra capacity. A VU SQL Database can be requested via VUNet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Version number</strong></th>
<th><strong>Date</strong></th>
<th><strong>Author</strong></th>
<th><strong>Remarks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.10</td>
<td>18 June 2019</td>
<td>Joost Meijer, Marieke Polhout</td>
<td>Final draft submitted to the faculty board</td>
</tr>
<tr>
<td>0.11</td>
<td>27 June 2019</td>
<td>Joost Meijer</td>
<td>Inserted a compliance clause at the request of the faculty board</td>
</tr>
<tr>
<td>1.0</td>
<td>9 July 2019</td>
<td>Joost Meijer</td>
<td>Policy approved by the faculty board</td>
</tr>
</tbody>
</table>