UNIVERSITY OF AMSTERDAM | Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

UvA Research Drive and HvA Research Drive Terms of Use

The applicant declares to agree with these terms when applying for a project environment in Research Drive.

Definitions

1. **Data owner:** The Data Owner determines the access rights of groups or individuals to the data stored in Research Drive. The person who fulfils this role in Research Drive is ultimately responsible for the use of Research Drive in a research project. This role is fulfilled by the same person during the project or it can be transferred if necessary.
2. **Group Administrator:** This role is performed by a person who is authorised by the Data Owner to add or remove persons in a group in Research Drive. When the data owner creates a group in Research Drive, the data owner is automatically the group administrator and can then authorise other people to manage the group.
3. **External user:** This is a user who uses Research Drive without a university account (for example with an @gmail or @outlook e-mail address).
4. **Two-factor verification:** Login to Research Drive with UvA-net ID or HvA-ID, password and using an external device such as a mobile phone. Additional user verification is done by mobile phone.
5. **SURFSecureID:** This is a code that an employee or student of the faculty has requested for using two-factor verification.
6. **Encryption:** Data encryption using specific software. This makes the encrypted data inaccessible and therefore unusable for unauthorised persons.

Access Control

1. Within a project, a Data Owner is appointed, who is a member of the research project and is jointly responsible for granting persons access to folders in Research Drive. The Data Owner is granted access by ICTS and is authorised to fully control the project environment in Research Drive. Research Drive includes the option to change data owners. It is not currently possible to have two data owners on one project environment.

2. Circumstances that result in changes in user access to the project environment, e.g. a user leaving employment, must be reported to the data owner well in advance. The data owner then adapts the roles and rights within the project environment to the new circumstances.

3. There must always be an active data owner in Research Drive. If the data owner is no longer actively participating in the research project, or only temporarily, a replacement must be assigned and registered from within the research project.

4. A user with a university account needs a SURFSecureID before two-factor verification can be used in Research Drive. If a user does not yet have a SURFSecureID, it can be requested.

5. The Data Owner in Research Drive is responsible for the use of two-factor verification by External Users. The data owner must verify the identity of an external user before the invitation procedure.

6. External Users are responsible for activating two-factor verification when using Research Drive for the first time. The data owner monitors this so that this additional security measure is guaranteed for the duration of the research. ICTS monitors the activation of two-factor verification by external parties and will inform the data owner if this has not been done.

7. The use of all Research Drive accounts and two-factor verification codes is subject to the institution's ICT rules of conduct. These rules of conduct can be consulted at UvA rules of conduct and HvA rules of conduct.

8. Research Drive accounts and codes for two-factor verification are strictly personal and must not be disclosed to others, including close colleagues and supervisors.

9. Loss and theft of access data must be reported immediately at cert@uva.nl.

10. After the end date of the requested project environment, Research Drive will remain active for another 90 days. After this period of 90 days ICTS will revoke access to Research Drive for all users. The data owner must inform ICTS accordingly if the end date changes before the expiry of these 90 days.

Data protection

1. Research Drive uses ‘server-side' encryption. This means that all research data is automatically encrypted and stored in the Cloud.

2. Research Drive data is stored locally when downloading data from Research Drive and when using the Research Drive software on a device. Due to security risks, the faculty requires all users of Research Drive to use encryption software to encrypt the locally stored research data. Bitlocker encryption software is recommended for Windows and FileVault for Apple.

3. If additional encryption measures are taken for a research project, the responsibility for key management during and after the project rests with the data owner.

4. SURF makes a daily backup of all the data on Research Drive. This backup can be used in case of an emergency. Any changes made in the last (maximum) 24 hours will then be lost. This backup cannot be used to restore data from individual research projects.

5. Research Drive can store user deleted data (i.e. data in the recycle bin) 365 days after deletion for individual research projects. The deleted data is not part of the storage capacity allocated to the research project. The purpose of this recycle bin is to temporarily store data that is no longer used during and after the research project. The data owner must ensure that the recycle bin is only used for this purpose.

6. If a research project requires additional backup facilities, the responsibility for this rests with the data owner. ICTS can act in an advisory capacity.

Data processing

1. The data owner and Research Drive users must be aware that the faculty has concluded general terms and conditions (Appendix 1) and a processing agreement (Appendix 2) with the Research Drive supplier (SURF) for the purpose of the research projects.

2. The Data Owner must make every effort to comply with the terms and conditions (referred to in Article 1, Data Processing) and must be aware that, in extreme cases, failure to comply with the obligations and terms and conditions contained in these agreements may have legal consequences for the faculty.

3. Both the faculty and the supplier of Research Drive (SURF) have taken organisational and technical security measures that the Data Owner must discuss with all users of Research Drive in the research project (see the Processor Agreement Appendix 2). The data owner is responsible for assessing whether the measures taken are adequate and, if necessary, for taking additional safety measures related to:
   a. IB&P (Information security & privacy);
   b. DPIA (Data Protection Impact Assessment);
   c. Processor Agreements with external partners/consortia with which the research project cooperates.

Support and administration

1. The Research Drive service intended for the storage of research data. The content of this service is described in the ICTS Service Catalogue.

2. The persons who have been assigned the roles of Data Owner and Group Administrator in Research Drive must act as an enquiry desk for Research Drive users during the project.

3. If data owners or group administrators are unable to answer support questions, the ICTS Service Desk can be contacted. Only ICTS may directly approach the supplier of Research Drive.

4. Information on accessing and using Research Drive is available through the Research Support Portal (rsp.uva.nl) and the alphabetical list. A starter pack is sent to data owners when requesting a project environment.

5. A Topdesk form can be used to apply for Research Drive. The procedure for this can be found on the alphabetical list.

6. Help with using Research Drive, e.g. manuals, is available through the alphabetical list.

7. Research Drive is specifically intended for the storage of research data during a research project. After this period, the data owner is responsible for archiving and/or publishing the research data.

8. ICTS assumes that the data owner:

   a. conforms to the Research Data Management policy within the faculty, whereby the data steward can be approached for advice and support;

b. will obtain guidance from the privacy officer, data steward and/or ethics committee of the institution or faculty with regard to ethical matters;
c. will obtain advice on measures to be taken with regard to data security from the faculty data protection officer and/or the faculty Security Officer.

9. ICTS reserves the right to amend the terms of use. Data owners will be informed well in advance.

Appendix 1: General terms and conditions for Research Drive agreed with SURF
Appendix 2: UvA Research Drive and HvA Research Drive processor agreement agreed with SURF