Explanation on the safe use of Research Drive

Introduction

Research Drive is a data storage service in the Cloud for research data. You want to be able to store and manage this research data securely.

The type of security depends on a number of factors:

- whether you are an internal researcher (with a university account) or an external party,
- whether you are working in the web version of Research Drive, or locally on your device,
- whether you have a managed UvA workstation (Windows PC or laptop) or work with a Mac.
- whether you will be storing confidential data as part of your research.

Access with two-factor authentication for internal and external researchers

Internal researchers

You can use your UvAnet ID and your university account (username and password) to log on to services that UvA makes available to you. This gives you secure access to those services, including Research Drive. The SURFconext authentication service is used for this initial verification.
This is followed by a second verification step with SURFsecureID. Two-factor authentication means that you not only have to enter a username and password, but also possess a device (mobile phone) on which you receive a code that you can enter. This code can be sent in a text message or generated by an authenticator app like tiqr.Two-factor authentication is required for services that process confidential data.

External researchers

A researcher who is a member of the research group must successfully undergo a *vetting* procedure. This is a background check to verify the identity of the person concerned based on his/her proof of identity. The data owner is responsible for registering external parties and configuring two-factor authentication. Refer to *External guest accounts manual for Research Drive*.

Working in the web version of Research Drive or locally on your device

Web version of Research Drive

You work directly on Research Drive and the data held on Research Drive is encrypted by default. You do however need to protect your laptop or PC with Bitlocker or FileVault (see below), and you should encrypt your files if they contain confidential data.

Working locally in Research Drive

You need to install the ownCloud software to be able to work in Research Drive locally on your PC or laptop. See manuals under the alphabetical list for more information. The data you save in the local folder on your PC or laptop is then synchronised on Research Drive. However, this locally stored data is not protected. You need to set up encryption yourself in order to secure the data. See below.

Encrypting the hard disk on your laptop or PC

To secure research data that is stored on your local workstation, you must prevent it from being accessible. This is called disk-encryption. If an unauthorised person gains access to your data on your laptop, he/she will not be able to read your data because he/she does not have the encryption key. So you can use full disk encryption to make data on a laptop, PC, external hard disk, USB flash drive or other mobile storage media unreadable.If you lose these items or if they are stolen, nobody can read the encrypted data.

Bitlocker

If you are a researcher with a managed UvA or HvA workstation (Windows laptop or PC), Bitlocker is used as the default security solution to manage access to the data on this workstation. Bitlocker encrypts the entire hard drive in your workstation. BitLocker is only available on computers running Windows Vista or 7 Ultimate, Windows Vista or 7 Enterprise, Windows 8.1 Pro, Windows 8.1 Enterprise, or Windows 10 Pro. External researchers with a PC or laptop must install Bitlocker themselves. Information about this is available on the Microsoft website.

FileVault

Users of Research Drive who work with a Mac can use FileVault instead. Because FileVault is disabled by default, it has to be enabled separately on the Mac. By encrypting your data with FileVault, you greatly increase the overall security of your Mac. See the Apple website for more information.

Linux

Linux users often have a choice of multiple open source disk encryption software solutions, depending on the Linux version. More information is provided in this overview.

Confidential research data

A laptop with an encrypted drive, once booted up, is equally vulnerable to Trojans and other malware as any other system. Full-disk encryption is an important foundation for a secure system, but it must be supplemented by other elements.

Whenever you collect and store confidential data as part of your research, it must be encrypted. To assess the need for file encryption, you need to consider whether there is an increased risk that the data you want to keep confidential could be read by unauthorised persons and what impact this could have.
If the researcher has questions about this, he or she can contact the data steward or the (faculty) Data Protection Officer.

Different measures:
ICTS ResearchIT can advise the researcher on the measures that can be taken to protect the confidential data:

- File encryption: the encryption of data through a specific encryption software package. The user can use a password to decrypt the file. The purpose of encryption is to protect data from outsiders.
- VeraCrypt as file encryption software and KeePass as password manager are available in the workstations managed by ICTS. Manuals for configuring both packages are also available on the HvA/UvA alphabetical lists.
    - For HvA: How do I encrypt highly confidential research data?
    - For UvA: How do I encrypt highly confidential research data?

- Password manager: a digital 'safe' where you can store all your passwords and encryption key. You then only need to remember the password for your password manager. You can also use the password manager to share passwords with fellow researchers.

- Anonymisation: The processing of personal data in such a way that this data can no longer be traced back to a natural person in any way. If you anonymise/pseudonymise your data, you no longer need to perform file encryption.
    - anonymise: https://anonimiseren-bnas.nl/
- Pseudonymisation: the processing of personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, which are kept separately from the original set of personal data. https://tm7.eu/nl/anonimiseren-of-pseudonimiseren-van-persoonsgegevens-ten-behoeven-van-de-avg