Categorization of storage

Portable media

Flash disks, memory cards, external HDD/SSD, CD, DVD, etc., external memory media that are not a permanent component of any device and that are used to transfer information between various devices or for temporary data storage.

What to watch out for...
Portable media are typically transferred from place to place. They can easily be left without supervision or lost in public spaces where they can be stolen, and then the stored data could be misused or disclosed.

For this type of media, it is also difficult to determine whether unauthorized access to data has occurred (e.g. a colleague copies not only a conference presentation from the flash disk, but also other files stored on the disk).

This method of storage has practically no protective mechanisms against the loss of data (multiple storage, automatic control of stored data, etc.), so if a drive fails, the data on it could be easily lost without warning. Hence, these are not appropriate as the only primary data storage method but for storing a second or additional copy.

Local disks

a) in computers and laptops

Disks permanently installed in desktops or laptops owned by the University (typically internal HDD/SSD, etc.). These are devices accessiblein university spaces, in employee offices, in study rooms, etc. Every device must have a defined administrator (administrative account), and is properly secured (updates, antivirus protection, …). The devices are typically managed by IT professionals from IT departments of faculties and units who ensure and monitor their secure operation.

This form of storage is suitable for data that require fast local access directly on the computer and do not need to be shared with other people or processed on multiple devices. It can also be used when there is limited or no Internet connection (off-line work).

What to watch out for...
In order to prevent unauthorized access to data, special care must be taken to restrict access to the user/administrator account (login passwords, etc.), to correctly set access rights, and to observe physical security principles, especially not leaving acomputer unattended without a “screen lock”(where possible, lock the office in the absence of the computer user), etc.

This method of storage providespractically no protective mechanisms against the loss of data (multiple storage, automatic control of stored data, etc.), so if the device fails, the data on it could be easily lost without warning. Hence, locally stored data that we need to keep for a longer period of time should be protected against loss using backup (e.g., on portable media, on network or cloud storage, etc.).

Special warning for laptops

Special care must be taken with laptops. They may be easily left without supervision or forgotten in public spaces, which increases the risk of being stolen and then the loss/misuse of stored data.

With respect to the loss of data, this risk is even higher for portable computers because they are exposed more to vibrations, dust, shocks, extreme changes in temperature, etc. which increases the chances of malfunction of the local data storage unit.

b) in other mobile devices

Data storage permanently installed in mobile devices, i.e., mobile phones, tablets, etc. (typically an internal non-removable memory in devices, an installed memory card, etc.) used by employees/students.

Because these devices are often used simultaneously for work and personal purposes, and are usually not managed by the relevant IT departments of the faculty or unit, they cannot be recommended for storing work or research data for security reasons.

What to watch out for...
Mobile devices are often used both for work and private matters. Hence, one must be especially careful that work data is not accidentally stored in private cloud storage.

Depending on the nature of the stored data, a screen lock must be used on the device, i.e. a “pattern”, PIN, password, or fingerprint, which prevents unauthorized access to the device.

Special attention should also be paid to installing fraudulent or “infected” applications. Even a seemingly innocent application, such as a computer game installed for personal entertainment, could gain access to work data. For example, an unreasonably large request for access rights can point to a potentially harmful application. Therefore, it is recommended to use only applications from official sources (Google Play, Apple App Store, etc.).

A considerable problem in the safety of mobile devices is the care relating to their security taken by manufacturers. If the manufacturer does not provide timely software fixes for operating system security issues, etc., the end user may not be able to sufficiently secure the device despite all efforts on their part.

In order to prevent data loss in the event of loss/theft/failure of the device, it is advisable to synchronize the maximum amount of data from the device to a cloud or network storage, which is a typical situation with modern mobile devices (see below).

Network and cloud storage operated on the CU infrastructure

Data storage owned by CU accessible to end users via a computer network. These data storage methods are especially appropriate for data that must be shared with other persons or processed on various devices.

Note
The security and accessibility of data in network and cloud storage is not only a question of the selected technical solution but especially the professional management and the settings for data storage and backup processes.

a) NAS (Network Attached Storage)

If properly managed, stored data on repositories connected to LAN must meet the requirements for the security and accessibility of scientific data. However, it is recommended to use mechanisms that protect against physical failure of one or more disks (RAID, etc.). Although NAS can be recommended as the primary data storage method when data management is handled properly, backup must also be taken into consideration.

What to watch out for...
This type of less expensive and intuitively manageable storage often leads to semi-professional management directly by users/data owners. However, in the case of inappropriate configuration without backup mechanisms, this type of data storage can be relatively risky (e.g. when several disks fail without continuous backup, the data is compromised similar to local disks). ***Give preference to professional solutions managed by IT experts.***

b) Professional data storage for faculties and units (disk arrays, SAN, …)

Storing data in the server rooms of faculties and units using professional storage solutions (often redundant disk arrays, SAN) provides increased protection of data against damage or loss. Data is backed up automatically by the storage administrator, and the specific backup policy is usually available in the description of storage parameters. Central server data storage enables better monitoring of data access, thus improving the ability to detect unauthorized access.

What to watch out for...
In order to prevent unauthorized access to data, close attention must be paid to the correct setting of data access rights. The capacity of these storage spaces is often a problem, as they are not designed at the time of purchase as storage providing capacity for extensive scientific data, but only for the normal operations of the faculty/unit.

Network and cloud storage operated by external entities outside the CU infrastructure

Technically, these are advanced data centres with multiple data storage and special storage functions providing superior data protection against damage or loss. Cloud storage also enables better monitoring of data access, thus improving the ability to detect unauthorized access. Given that these repositories are often designed for the frequent commercial provision of services to a wide group of users, it is usually not a problem to agree on above-standard capacities for individual scientific projects.

a) CESNET storage

The academic staff, students, and employees of research institutions in the Czech Republic may use a data repository operated by the CESNET Department of Data Storage for educational and research activities either without the sharing of data (i.e. VO Storage) or as a virtual organization allowing the sharing of data between users as a part of the federation of identities eduID.cz . This category also includes services such as CESNET OwnCloud and CESNET FileSender . Use of these repositories are regulated by the Rules for the Use of CESNET Data Repositories . The repositories are operated by a Czech organization that is co-owned by academic institutions in the Czech Republic, and CU is a member of its executive board. The data repositories are **certified according to the standard for information security management systems ČSN EN ISO/IEC 27001:2014**. The operator of the repository makes every effort to protect the data against loss or unauthorized access. The services can also be recommended for the storage of protected data. It is advisable to enter into an individual service level agreement.

b) Storage provided based on centrally concluded contracts with CU

Currently, University students and staff can use Microsoft 365 cloud services. In particular, these services include personal storage OneDrive and the document library service SharePoint, as well as e-mail service Outlook and a number of other services offered as part of the Microsoft 365 package.The management of data as a part of this cloud service is secured through an agreement concluded between CU and Microsoft. The agreement also includes “standard contractual clauses” issued by the European Commission and **guaranteeing that the processing of data is in accordance with EU law**. The data of users from the EU are stored in data centres in the EU (specifically in the Netherlands and Ireland). The security policy of Microsoft is in accordance with ISO 27001, 27002,and 27018. These Microsoft cloud services also meet the GDPR requirements.In terms of security and given the relatively high capacity of the services provided (for example, the OneDrive for Business service provided as part of the A1 license package is limited to 1TB per user, and in the case of the A3 license, up to 5TB of data per user), as well as the ease of sharing data, this method of storage can be recommended, even for data and documents created within research projects.

Note
Personal storage is primarily used for storing personal data. Only you have access to your **OneDrive** personal storage, and you alone determine whether and to whom to grant access to a document or folder if needed. Here, you have documents stored that you usually do not need to share with colleagues. If you need a one-time addition or consultation, it is possible to share the document, but it is advisable to end the sharing once the activity is complete.

On the other hand, **SharePoint** is a shared team storage (department, project, process, etc.). There is no need to set access to documents for individual users, as access is controlled by membership in the team. Shared data are accessible to all team members throughout the collaboration.

c) Storage provided based on individual contracts with CU

A recommended option is the use of standard commercial services. Attention must always be paid to the proper contractual assurance of the quality of services (definition of SLA parameters) and ensuring that data processing is fully in accordance with EU law (full compliance with GDPR requirements).

What to watch out for...
The use of professional commercial services is often associated with the relatively high price of these services. When negotiating contracts, think about the sustainability of the chosen solution in the long term (e.g. after the end of project financing). Have you really verified the possibility of using CESNET z.s.p.o. services?

Security notice...
This category also includes, for example, cloud data storage provided as a part of the ***Google G Suite for Education*** *service on the basis of individual agreements with selected faculties/units of CU. In particular, this involves the data capacity of Google Drive, but it also includes other data stored in the G Suite for Education cloud, such as e-mail in Google Mail, notes in Google Keep, calendar data in Google Calendar, etc. Despite all efforts, contractual relations have not yet been agreed upon ensuring that the storage and processing of the data complies with EU law. For this reason, the services* ***cannot be recommended for storing confidential and sensitive data without further measures*** *.*

d) Storage without contracts with CU – network and cloud storage for the public

This category includes, in particular, public cloud services (typically arranged free of charge by the end user after online registration) such as Microsoft OneDrive, Google Drive, Dropbox, Úschovna, Uložto, Amazon storage, repositories on GitHub, etc.

The main difference and attribute of this category of cloud storage compared to the cloud services mentioned above is that CU has no (legal) relationship with the operators of these external services and is therefore unable to guarantee the security/confidentiality of stored data or data management policies.

What to watch out for...
Keep in mind that none of these services are really free – in fact, you "pay" by entrusting all of your data to the service provider, often for unlimited use. Therefore, you should be aware of the potentially high risk of misuse of such stored data.