How to manage data safely and securely

Table of Content

1. Purpose of the document

The purpose of this document is to propose a classification system for the data with which the students and staff of Charles University (CU) come into contact. In addition, the document provides an overview of the most common data storage methods and provides recommendations relating to their suitability.

The document looks at typically processed data that employees and students come into contact with during research, when handling the operational and administrative activities of the university, or during instruction.

The document only briefly touches on work with highly sensitive data (healthcare documentation, etc.), highly valuable data where there is a risk of financial damage when destroying them or disclosing them (research data with a high financial value, data of a high strategic importance with respect to national and state security interests, etc.). In all of these cases, one must proceed on an individual basis and prepare a separate analysis for selecting an appropriate data storage method.

Data classified under the law are completely outside the scope of this document and are subject to specific rules.

2. Security of stored data

When working with data, we deal with two basic security issues:

- Protecting data against unauthorised disclosure
- Protecting data against unauthorised or unwanted modification and loss.

2.1 Protection of data against unauthorised disclosure

We protect ourselves against “hackers who steal data”, the copying of data by someone who finds a flash drive, misuse of data by someone who steals a laptop, etc.

Protection is first and foremost the choice of an appropriate storage method for the specific type of data, the use of login passwords for access to data, restriction of access to files using access rights, data protection by encryption, etc.

Data encryption

Data encryption can be an effective way to protect stored data against unauthorized access. However, the risks associated with the loss of the encryption key must be taken into consideration – tools for the encryption of data could be requested from the end user so that they may back up the encryption keys/passwords themselves in the event of a loss, which could be a process requiring advanced technical knowledge.

However, without the encryption keys/passwords, the data cannot be in any way restored! In addition, access to the encryption keys/passwords (e.g., their back-ups) by an unauthorized person endangers the effectiveness of encryption as a means of data protection.

Due to the complexity of managing passwords/encryption keys, we recommend using a storage method that does not require encryption for the specific data category.

2.2 Protection of data against modification or loss

We prevent the loss of data due to unintentional or intentional deletion/change of the contents of a file, failure of the data storage in the device, extortionary encryption/deletion of data by a computer virus, etc.

Here again, it is important to choose a storage method or methods that have built-in protection mechanisms against the loss of data.

General methods of protection include backing up data (storing several copies of the same files in various independent storage locations) and long-term storage of their historical copies, deletion to a "trash" folder, use of advanced storage with integrated data protection (e.g., cloud storage, storage on professional data servers using redundant storage), etc.

Data backup

Always verify whether and how your selected storage method handles data backup. Without a defined process of regular backup, there is always a risk of the loss of data, regardless of the selected storage type. This also applies to professional data storage and cloud storage provided you do not explicitly arrange data backup as a part of the extended SLA services.

3. Categorization of data

Data category	***Description***	***Examples***
Public data	Data accessible to anyone with no restrictions, e.g., public web-based data. Disclosure is not a risk to CU or other institutions and people.	• Publicly accessible research reports and data • Open-source software • Promotional materials • Public service information
Internal data	Data intended only for the internal needs of a generally defined group of people (e.g., co-worker of a project, employees of an institution, etc.). However, no special regulation or protection is required (under law, a contract, etc.). Disclosure outside the specific group does not cause direct damage (financial, moral, legal, etc.).	• Internal correspondence • Minutes of meetings • Internal directives and regulations • Unpublished research reports
Confidential data	Data intended exclusively for the internal needs of a precisely defined group of people (e.g., an employee and their direct superior, an HR department employee and a job applicant, a group of IT system managers with administrative rights). By nature, the data require regulation or protection; typically, the data are protected by law or under a contract/licence (e.g., personal data of persons, data covered by trade secrets, etc.). Disclosure outside the specific group of people most probably causes damage (financial, moral, legal, etc.).	• Economic and personal data of a private nature • Personal data of students, employees, co-workers • ID numbers, birth numbers, etc. • Credit card numbers • Valuable research data (providing, e.g., competitive advantages) • Extensive collection of internal data • Access data (e.g., passwords or encryption keys) to minor systems and internal data

Sensitive data	Data intended strictly for the internal needs of a precisely defined group of people (e.g., healthcare worker and their patient, project managers working with data that are subject to trade or similar secrecy, etc.). By nature, the data require special regulation or specific protection; typically, the data are strictly protected by law or under a contract/licence (e.g., very valuable data covered by trade secrets, sensitive personal data, etc.). Disclosure outside the specific group of authorized people most probably causes large-scale damage (financial, moral, legal, etc.) with serious and irreversible consequences. In university practice, only certain data fall into this category.	• Healthcare data, sensitive personal data • Very valuable research data (providing, e.g., unique competitive advantages that cannot be easily replaced) or research data containing highly confidential information • Extensive collection of confidential data • Access data (e.g., passwords or encryption keys) for important systems and data of a confidential or sensitive nature

4. Categorization of storage

4.1 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 they can be used for storing a second or additional copy.

4.2 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 accessible in 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 a computer unattended without a "screen lock" (where possible, lock the office in the absence of the computer user), etc.

This method of storage provides practically 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 a 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.

4.3 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 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, data stored in repositories connected to LAN must meet the requirements for the security and accessibility of research 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 can be 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.*

4.4 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 research 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 may also be recommended for storing confidential information** (e.g., when required to guarantee the security and accessibility of data, e.g., **for sensitive data**). We also recommend arranging 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 1 TB per user, and in the case of the A3 license, up to 5 TB 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 a 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 on that would ensure 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 set up 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 the fact 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.

5. Recommendations for the selection of data storage

	public data	internal data	confidential data	sensitive data
portable media	🟢	🟡	🔴	🔴
local disks (computer / laptop)	🟢	🟡	🟡	🔴
local storage (phone / tablet)	🟢	🟡	🔴	🔴
NAS (Network Attached Storage) operated on the CUNI infrastructure	🟢	🟡	🟡	🔴
professional data repositories of faculties and units (disk arrays, SAN, …) responsibly operated by IT employees on the CUNI infrastructure	🟢	🟢	🟢	🟡
CESNET repositories and services	🟢	🟢	🟢	🟡
network and cloud storage operated outside the CUNI infrastructure based on centrally or individually concluded contracts (with proper GDPR and SLA contractual agreements)	🟢	🟢	🟢	🟡
network and cloud storage for the public	🟢	🔴	🔴	🔴

🟢 Appropriate

🟡 Possible after taking security measures (encryption, access password, access rights)

🔴 Inappropriate

In the case of specific requirements or in special justified cases where the recommended data storage method cannot be used, an individual analysis of the specific case must be carried out and measures put in place to ensure the security of the stored data.

6. Methods of data transfer

When collaborating with colleagues, we handle the sharing and transfer of data files on a daily basis. The options for the transfer of data depend on the scope of the transferred data.

6.1 Sending data as an e-mail attachment

Small-scale data (typically office application files, etc.) of several MBs are often transferred by e-mail (depending on the type of email client, files up to 10 MB can be transferred in one message).

> ***What to watch out for***
>
> *When transferring confidential data, it is always necessary to **encrypt** the files. Emailing sensitive data is not recommended even when using encryption. Emails are now commonly delivered to various mobile devices (phones, tablets, watches, etc.) with different levels of security, so the risk of disclosure is high when transferring unencrypted files.*

6.2 Use of flash disks and USB drives

Today, very cheap flash or USB drives are used to transfer often relatively large amounts of data. When using encryption, there can be no objection to the use of this method, provided that the administration of end PCs allows them to be connected (many companies prohibit the use of USB ports for this purpose in order to protect data from being stolen). However, one must always pay attention to the secure transmission of the encryption key and realize that this method of transmission does not allow for verification of the data recipient.

> ***What to watch out for***
>
> *As mentioned above, when using these portable media, it is essential to ensure the encryption of the stored data for security reasons. One must keep in mind the high risk of easily losing the media, i.e., the loss of stored data or their possible misuse.*

6.3 Use of storage for one-time or time-restricted transfer of data

There are a number of web portals that allow you to conveniently upload even large amounts of data in order to provide them to other people for access or download (the identity of the persons authorized to download is determined by entering an e-mail address). These portals should also be seen as temporary data repositories, and one should keep in mind the above-mentioned aspects of the specific services.

a) CESNET "FileSender" service operated by CESNET z.s.p.o.

This service can be considered trusted and reliable for the reasons stated in paragraph 4.a) of the Section Categorization of storage, and so can be recommended for a one-time transfer of data. The service currently allows the transfer of data up to 1.9 TB per transfer (without HTML5 the limit is 2 GB per file) and now offers the option of encryption when uploading. The user is thus assured that the data stored on the portal is encrypted (the data is not readable even by the storage administrator). The user must then send the encryption password to the recipients (e.g., by e-mail, SMS, etc.).

b) Services of other commercial portals "ulož.to, uschovna.cz, e-disk, etc."

On the other hand, these services are not recommended at all due to the high risk of data misuse.

6.4 Use of the "sharing" data storage functionality

The method of sharing within the appropriately selected data storage is certainly a good solution, as it permanently provides users authorized by you with access to the current shared data. Always be mindful of the sharing rights you provide to other users.

> ***What to watch out for***
>
> *For sensitive or confidential scientific data, the choice of a suitable data storage method is essential, especially from the point of view of guaranteeing the security/confidentiality of stored data or the data management policy (see section 4.3).*

6.5 Sharing within cloud storage

Cloud storage spaces have sophisticated data sharing capabilities for both cloud users and guests, allowing documents to be accessed with a time embargo or requiring user authentication for each access.

> ***What to watch out for***
>
> *It is recommended to share within working groups (Teams). Considering the fact that several environments (so called tenants) are operated within the M365 services at the CU, be careful who you share your data with and whether the user you have selected actually uses an identity in the tenant. Limit sharing via links for guests outside the tenant, as unauthorized users may also gain access to such data.*

7. Basics of cyber-security

DO	DO NOT
Do use a strong password and change it if you think it may have been compromised	Don't give your password to anyone
Do report any loss or suspected loss of data	Don't reuse your University password for any other account
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to the DD&T service desk at abuse@cuni.cz	Don't open suspicious documents or links
Do keep software up to date and use antivirus on all possible devices	Don't undermine the security of University systems
Do be mindful of risks using public Wi-Fi or computers	Don't provide access to University information or systems
Do ensure University data is stored on University systems	Don't copy confidential University information without permission
Do password protect and encrypt your personally owned devices	Don't leave your computers or phones unlocked

7.1 Login data

Although data security on network and cloud storage is at a high level, the weakest link is usually the end user or their method of authentication: If you use a weak password / a password shared with other services, etc. for access, and the password is the only element of authentication, then disclosing the password to an unauthorized person will compromise the security of all data and services to which you have access.

You should never enter access information to work data into other people's computers (in a café, at a friend's house, etc.) for which you have no knowledge or guarantee of their security. Use your own laptops, phones, etc.

To be able to use strong passwords unique to each service, it could be helpful to use a quality password manager.

7.2 Private computers used for work

Home computers or other devices used to access work data should be subject to the same security requirements as work computers. Few people have a camera system or a gatehouse with 24/7 surveillance at home, so pay extra attention to physical security during your absence (e.g., when you are at work).

Don't forget about your children, who may not only forget to lock up when they leave the house, but will often use the home computer together with you – strict separation of user accounts on the computer for work and personal purposes and inaccessibility of administrator privileges for children on a shared computer should be a matter of course. You should also install quality antivirus and antimalware software and firewalls.

Avoid installing games and suspicious software on the computer you use for work. Only install trusted software that you have authenticated. Think about software configuration (for example, antivirus programs often automatically send files they think suspicious to their manufacturer – in such a way, data could be sent from your computer without your knowledge that should not fall into the hands of a third party).

Remember: you do not have to protect any data that are not on your home computer – leave your work data on network and cloud storage, and download only the minimum amount of data to your home computer for as short a period as possible. If possible, always encrypt confidential and sensitive data.

7.3 Obligation to report the loss of work devices

Based on the guidelines by the data protection officer, you are **required to report to the officer any loss or theft of any device or data medium** that may allow access to personal or sensitive data for which CU is responsible. These guidelines apply to any device from which data can be retrieved, for example, by breaking the protection (password) or removing the disk and retrieving the data itself or passwords for accessing the university's systems. Typically, this is a laptop, tablet, computer from the office, or even a mobile phone with access data. The loss should be reported as soon as possible by the employee who discovered it or by their superior to the e-mail address gdpr@cuni.cz.

7.4 Reporting security incidents

The coordination of resolving security incidents in the university networks has been handled since 2015 by a security team for the Charles University computer network **CSIRT-CUNI**. You should send security incident reports according to the instructions by e-mail to abuse@cuni.cz.