MUNI
ICS

Recommendations for the Usage of MUNI Storages

Revision 1.2.0

1 March 2021

By:

Institute of Computer Science MUNI

Department of Data Security and Management
<BaSD@space.muni.cz>

Document Revisions

Revision 1.0 (5 December 2018)

- Internal edition.

Revision 1.1 (11 December 2018)

- The first public edition.

Revision 1.1.1 (14 December 2018)

- Google G Suite for Education status refinement.
- CC-BY license.

Revision 1.2.0 (1. March 2021)

- Microsoft O365 status refinement.
- Google G Suite for Education status refinement.
- Detailed Grammarly status adding.
- Replacement of the MU abbreviation for MUNI.

License

Obsah

Document Revisions 2
1 Purpose of Document 4
2 Security of Sotred Data 4
2.1 Protection of Data against Disclosure to an Unauthorized Person 4
2.2 Protection od Data against Modification or Loss 4
3 Data Categorization 5
4 Storage Categorization 6
5 Recommendations for Using Data Storages at MUNI 7
5.1 A Summary Overview Diagram 7
5.2 Portable Media 10
5.3 Local Storage 10
5.3.1 In Computers 10
5.3.2 In Mobile Devices 11
5.4 Network and Cloud ICS Storage 12
5.5 IS MUNI Storage 12
5.6 CESNET Storage 13
5.7 External Storage 13
5.7.1 With MUNI Contract 13
5.7.2 Without MUNI Contract 15
6 Data Encryption 15
6.1 Local Computer Storage 16
6.2 Local Mobile Devices Storage 16
6.3 Network/Cloud Storage 16
7 What to Look out for 16
7.1 Security of your Login Data 16
7.2 Private Computers Used for Work Purposes 17

1 Purpose of Document

This document aims to propose a classification of data with which students and employees of MUNI come into contact. At the same time, the paper provides an overview of the most common data repositories available at the university and beyond. Next, it presents the mapping of data categories to individual types of repositories in terms of the suitability of their use. At the same time, it provides basic recommendations for the safe use of storage.

The document is devoted to commonly processed data that employees and students encounter in research, in ensuring the operational and administrative activities of the university, or in teaching. Most students and university employees do not meet any other type of data in their work.

The document deals only marginally with working with highly sensitive data (health care, etc.), or highly valuable data, where there is a risk of serious damage in their destruction or leakage (research data with [potentially] high financial value, data of high strategic importance in terms of national and security interests of the state, etc.). In all these cases, it is necessary to proceed individually and prepare a separate analysis to select a suitable data repository. Data classified by law are entirely outside the scope of this document and must be subject to specific rules.

2 Security of Sotred Data

When working with data, we face two fundamental problems with their security: protection of data against disclosure to an unauthorized person and protection of data against unauthorized modification and loss.

2.1 Protection of Data against Disclosure to an Unauthorized Person

We protect ourselves against "data theft by hackers", copying data by accidentally finding a flash drive, misuse of data by a laptop thief, etc.

The protection is primarily the choice of the appropriate storage for a given type of data, the use of login passwords for access to data on devices, restricting access to files using access rights, data protection by encryption, etc.

2.2 Protection od Data against Modification or Loss

Here we prevent data loss due to accidental deletion/change of the file content by an (unauthorized) user, failure of the data storage in the device, extortionary encryption/deletion of data by a computer virus, etc.

Again, it is essential to choose suitable storage, or storages, which may itself contain mechanisms to protect against data loss. General methods of protection are data backup (storing multiple copies of the same files on different, independent storage) and long-term storage of their historical copies, deleting "to the trash", using advanced storage with integrated data protection (e.g. cloud storage, storage on professional data servers using redundant storage), etc.

3 Data Categorization

DATA CATEGORIZATION	DESCRIPTION	EXAMPLES
GREEN: PUBLIC DATA	• Data is accessible to anyone without any restrictions, e.g., publicly displayed on the Internet. • Their publication does not pose any threat to MUNI or other institutions/persons.	• presentations from public lectures; • publicly available research reports; • open-source software; • public research data; • promotion, public information about services.
BLUE: INTERNAL DATA	• Data is intended only for a generally defined group of persons (e.g., project collaborators, institution employees, etc.). • However, they do not require special regulation or protection (by law, contract, etc.). • Disclosure outside the group will not cause direct damage (financial, moral, legal, etc.).	• internal correspondence; • minutes of meetings; • internal regulations and rules; • internal work plans, notes, etc.; • unfinished/unpublished research reports
ORANGE: DISCRETE DATA	• Data is intended exclusively for the internal needs of a precisely defined group of persons (e.g., an employee and his/her immediate superior, an employee of the HR department and a job applicant, a group of IT system administrators with administrator rights to it). • They require regulation or protection by their nature; typically, the data is protected by law or under a contract/license (for example, personal data of persons, data covered by trade secrets, etc.). • Making available outside a given group of people is likely to cause harm (financial, moral, legal, etc.).	• economic and personal data; • personal data of students/employees/collaborators...; • identification card numbers, identification numbers, etc .; • credit card numbers; • valuable research data (providing, for example, a competitive advantage) or data containing otherwise sensitive information; • extensive collections of internal data; • access data (e.g., passwords or encryption keys) to minor systems and internal data; …

DATA CATEGORIZATION	DESCRIPTION	EXAMPLES
RED: SENSITIVE DATA	• Data is strictly intended only for a precisely defined group of people (e.g., a healthcare professional and his patient, project leaders with a security clearance of a certain level, etc.). • They require special regulation or special protection by their nature; typically, the data is strictly protected by law or by contract/license (for example, precious data covered by trade secrets, sensitive personal data, etc.). • Disclosure outside the given group of authorized persons is likely to cause large-scale damage (financial, moral, legal, etc.) with serious/irreversible consequences. • *In practice, little data will fall into this category; most will fall into the category of discrete data at most.*	• health data, sensitive personal data; • precious research data (providing, e.g., a unique and challenging to repeat competitive advantage) or research data containing highly confidential data; • extensive collections of discrete data; • access data (e.g., passwords or encryption keys) to essential systems and data of the discrete or sensitive category.

4 Storage Categorization

REPOSITORY TYPE	DESCRIPTION
PORTABLE MEDIA	e.g., flash disks, memory cards, external HDD/SSD, CD, DVD, … i.e., external storage media that are not an integral part of any device and are used by users to transfer information between devices or store data offline
LOCAL STORAGE	
IN COMPUTERS	Data storage built into desktop computers/notebooks (typically internal HDD/SSD, etc.) in employees' offices, study rooms, etc.
IN MOBILE DEVICES	Data storage is built into mobile devices, i.e., mobile phones, tablets, etc. (typically internal non-removable memory, memory card installed in the device, etc.) for use by employees/students.
NETWORK AND CLOUD STORAGE ICS	Data repositories operated by ICS and made available to end-users via the data network - the so-called standard and medium network storage. CERIT-SC data repositories for high-volume research data also fall into this category.
STORAGE IS MUNI	Document server, Depository and similar storage capacities integrated in the system IS MUNI.
STORAGE CESNET	Data repositories operated by the CESNET Storage Department. This category also includes services that use these repositories for the physical storage of data, e.g. CESNET OwnCloud, CESNET FileSender etc.
EXTERNAL STORAGE	Data repositories operated by external entities, i.e. entities outside MUNI and CESNET.
WITH MUNI CONTRACT	

REPOSITORY TYPE	DESCRIPTION
MUNI MICROSOFT O365	Cloud data storage provided within the Microsoft Office 365 for Masaryk University. These include OneDrive personal storage, SharePoint document libraries, and O365 Groups. However, this also includes other data stored in the MUNI O365 cloud, such as electronic mail in MUNI O365 Outlook, files shared in the social network MUNI Yammer, etc.
MUNI GOOGLE G SUITE FOR EDUCATION	Cloud data storage provided within the Google G Suite for Education service for Masaryk University. In particular, these are the data capacities of MUNI Google Drive, but this also includes other data stored in the MUNI Workspace for Education cloud, e.g. e-mail in MUNI Google Mail, notes in MUNI Google Keep, calendar dates in MUNI Google Calendar, etc.
WITH MUNI CONTRACT	
PUBLIC GOOGLE/MICROSOFT/DROPBOX/… STORAGES	This category includes mainly public cloud services (typically set up free of charge by private end-users only with electronic registration via the web) such as Google Drive, Microsoft OneDrive, Dropbox, Amazon storage, repositories on GitHub, etc. The main difference and "distinguishing mark" of this cloud storage category compared to the cloud services mentioned above is that MUNI has no (legal) relationship with the operators of these external services and is unable to guarantee anything regarding security/confidentiality or stored data policy.

5 Recommendations for Using Data Storages at MUNI

5.1 A Summary Overview Diagram

REPOSITORY TYPE	USAGE			
	GREEN: PUBLIC DATA	**BLUE: INTERNAL DATA**	**ORANGE: DISCRETE DATA**	**RED: SENSITIVE DATA**
PORTABLE MEDIA (FLASH DISK, EXTERNAL HDD, CD, DVD, …)	**Appropriate**	**Possible the use of encryption is recommended**	**Inappropriate possible when using encryption**	**Inappropriate**
LOCAL STORAGE				
IN COMPUTERS (DESKTOP, NOTEBOOK)	**Appropriate**	**Appropriate**	**Appropriate the use of encryption is recommended**	**Inappropriate possible in well-justified cases, when performing an individual analysis, the use of encryption and the application of other security measures that result from the analysis**

REPOSITORY TYPE	USAGE			
	GREEN: PUBLIC DATA	BLUE: INTERNAL DATA	ORANGE: DISCRETE DATA	RED: SENSITIVE DATA
IN MOBILE DEVICES (MOBIL PHONES, TABLETS, …)	Appropriate	Appropriate screen lock required (pattern, fingerprint reader, PIN, password)	Possible necessary to use encryption, strong screen lock required (fingerprint reader, PIN, password)	Inappropriate possible in well-justified cases, when performing an individual analysis, the use of encryption and the application of other security measures that result from the analysis
NETWORK AND CLOUD STORAGE ICS (SO CALLED STANDARD AND MEDIUM STORAGES, SEE IT CATALOG, CERIT-SC STORAGE)	Appropriate	Appropriate	Appropriate	Appropriate, it is recommended to perform an individual analysis, use encryption and apply other security measures that result from the analysis
STORAGE IS MUNI (E.G. DOCUMENT SERVER, DEPOSITORY ETC.)	Appropriate	Appropriate	Appropriate	Appropriate, it is recommended to perform an individual analysis, use encryption and apply other security measures that result from the analysis
STORAGE CESNET (E.G. CESNET ARCHIVE STORAGE, OWNCLOUD, FILESENDER, …, SEE CESNET STORAGE DEPARTMENT)	Appropriate	Appropriate	Appropriate	Appropriate, it is recommended to perform an individual analysis, use encryption and apply other security measures that result from the analysis
EXTERNAL SOTRAGE				
WITH MUNI CONTRACT				

REPOSITORY TYPE	USAGE			
	GREEN: PUBLIC DATA	BLUE: INTERNAL DATA	ORANGE: DISCRETE DATA	RED: SENSITIVE DATA
MUNI MICROSOFT O365 (MUNI O365 ONEDRIVE, SHAREPOINT, …, SEE MUNI O365)	Appropriate	Appropriate	Appropriate the use of encryption is recommended	Possible exclusively with adequate procedural coverage of the situation on the basis of individual analysis and the application of security measures that result from the analysis
MUNI GOOGLE G SUITE FOR EDUCATION (SEE MUNI GOOGLE APPS)	Appropriate	Appropriate	Inappropriate possible when using encryption	Inappropriate
GRAMMARLY	Appropriate	Appropriate	Inappropriate	Inappropriate
WITHOUT MUNI CONTRACT				
PUBLIC GOOGLE/MICROSOFT/DROPBOX/… STORAGE	Appropriate	Inappropriate	Inappropriate	Inappropriate

5.2 Portable Media

What to Store Here

Public Data, Internal Data.

In the case of internal data, the use of encryption is recommended.

These repositories are suitable for data that needs to be transferred to a computer with limited or no internet connection or internal data network. Alternatively, when it is a "foreign" computer, the user does not want to log in to his accounts for security reasons. They can also be used for (offline) storage of backup copies of data primarily stored elsewhere.

What Not to Store Here

Sensitive Data.

Storing discrete data is not reccommended, although it is possible with encryption.

Why (not) Use it like this

Portable media are often transferred from one place to another. They can easily be left unattended/lost in public places where their theft and subsequent misuse/disclosure of stored data is a risk. With these media, it is also challenging to determine whether there has been unauthorized access to data (for example, a colleague copies from the flash drive not only the conference presentation but also other files stored on the drive).

Whatsmore, for practical and economic reasons, these media contain practically no protection mechanisms against data loss (multiple storages, automatic checks of stored data, etc.), so due to media failure, the data stored on them can be easily lost without warning. Data loss can also quickly occur by simply losing/stealing the device itself. Therefore, these media are not suitable as a single primary data store but only for storing a second or additional copy.

Note: Portable media are very suitable for storing the second or third copy of data as an offline backup. In combination with appropriate physical (storage in a locked cupboard, safe, etc.) / logical (data encryption, etc.) security, they can be used to backup sensitive data after appropriate analysis.

5.3 Local Storage

It is important to remember that the data stored on the device's local storage and data primarily stored in the network/cloud storage is often stored/synchronized (automatically and/or temporarily). So if you work on the device with data from the network/cloud, you need device security has adapted the category of this data, even if the data is otherwise primarily stored outside the device on network storage/in the cloud (e.g., Google Drive, Microsoft OneDrive, OwnCloud, mail, calendars,…).

5.3.1 In Computers

What to Store Here

Public Data, Internal Data, Discrete Data.

In the case of discrete data, the use of encryption is appropriate.

These repositories are suitable for data that requires fast local access directly on the computer and does not need to be shared with other people or processed on multiple devices.

What not to Store Here

Sensitive Data. They can be stored only in exceptionally justified cases after performing an individual analysis of a specific case and implementing appropriate measures, typically including data encryption, special computer security mode (physical and network access restrictions, particular software installation, and configuration mode, etc.).

Why (not) Use it like this

Local storage on computers typically contains no protection mechanisms against data loss (multiple storages, automatic checks of stored data, etc.), so data stored on them can be easily lost without warning due to storage failure. Locally stored data, which we need to preserve for a long time, must therefore be protected from loss by backup (e.g., portable media, network storage, cloud, etc.).

In order to prevent unauthorized access to data, strict care must be taken to restrict access to the user/administrator account (login passwords, etc.), to properly set access rights to data in the storage, and to observe physical security principles, especially not leaving an unattended computer without "locked screen" (if possible, lock the office in case you leave the computer), etc.

Particular attention should be paid to laptops - they are typically carried from one place to another. They can easily be left unattended/lost in public places, with an increased risk of theft and consequent loss/misuse of stored data. In terms of data loss, the risk of laptops is all the higher because laptops are exposed to higher loads (vibration, dust, shock, significant temperature changes,…) during transport and use on the road, which increases the likelihood of internal data storage failure. Nevertheless, in principle, the same rules apply to internal storage for a laptop as to storage on desktop computers.

5.3.2 In Mobile Devices

What to Store Here

Public Data, Internal Data, Discrete Data.

When storing internal data, it is necessary to use a screen lock on the device, i.e., protection of access to the device functions by "pattern", PIN, password, or fingerprint, which prevents anyone who meets the device from working with data in it freely.

In storing discrete data, it is necessary to use a strong screen lock - i.e., it is no longer enough to use a pattern, but it is required to use a strong PIN or password or a fingerprint reader.[1]

Encryption is also required for discrete data. It is typically possible to configure a mobile device to remotely lock/erase it at the request of its authorized user if it is lost/stolen.

What not to Store Here

Sensitive Data. They can be stored only in exceptionally justified cases after performing an individual analysis of a specific case and implementing appropriate measures, typically including data encryption, the use of a particular mobile device model with particular software, configuration, security, and the usage mode. (physical and network access restrictions, particular software installation, and configuration mode, etc.).

Why (not) Use it like this

Mobile devices, such as smartphones, are often used by users as both - devices for work and personal purposes. Therefore, care must be taken to ensure that "work" data is not

[1] A fingerprint is usually less secure than using a strong PIN or password but has a much smaller negative effect on the convenience of using the device.

accidentally stored on private cloud storage. Increased attention must also be paid to the installation of applications - in addition to installation exclusively from official application sources (Google Play, Apple App Store, etc.), which helps prevent the installation of fraudulent or "infected" applications, it is necessary to pay increased attention to application permissions - unnecessarily extensive requirements the access rights of the application may point to a malicious application. Even legitimate applications, such as a computer game installed for personal entertainment, can then access "work" data, which should also be prevented.

A big problem in the safety of mobile devices is the care for their security by their manufacturers. If the manufacturer does not provide timely software fixes for operating system security issues, etc., the end-user may not adequately secure the device despite all efforts. The ecosystem around Google Android suffers the most from this problem, which many different manufacturers use under its brand to varying degrees. In particular, lesser-known brands and cheaper models are often left without proper software support. The recommendations on the Android Enterprise Recommended page can help you choose an Android device with a higher level of security.

To prevent data loss in the case of loss/theft/failure of the device, it is advisable to synchronize the maximum amount of data from the device to the cloud or network storage, which is a typical situation with modern mobile devices.

5.4 Network and Cloud ICS Storage

What to Store Here

Public Data, Internal Data, Discrete Data, Sensitive Data.

In storing sensitive data, it is necessary to perform an individual analysis of a specific case and implement appropriate measures, which may include the use of data encryption and other requirements for how to work with data.

Repositories are especially suitable for data that must be shared with other people or processed on multiple devices.

What not to Store Here

Sensitive Data without carrying out the appropriate analysis and implementing the necessary measures.

Why (not) Use it like this

Data storage in data centers on backed-up servers provides increased data protection against data corruption or loss; data is backed up automatically by the storage administrator. The exact backup policy is available in the description of storage parameters. Central server data storage enables better monitoring of data access, thus detecting unauthorized access.

To prevent unauthorized access to data, care must be taken to set access rights to the data in the storage properly.

5.5 IS MUNI Storage

What to Store Here

Public Data, Internal Data, Discrete Data, Sensitive Data.

The repositories are closely integrated with the functions of IS MUNI, so they are very suitable, especially for data belonging to this system. In storing sensitive data, it is necessary to perform an individual analysis of the specific case and implement appropriate measures, which will typically include the use of data encryption and other requirements on how to work

with the data. IS MUNI is primarily intended to store study and related data, not for storing sensitive user work/research data.

The MUNI IS also includes the Office and a document server, where all documents related to the operation of the university can be stored.

What not to Store Here
Sensitive Data without carrying out the appropriate analysis and implementing the necessary measures.

Why (not) Use it like this
Storing data on backed-up IS MUNI servers provides increased data protection against data corruption or loss. Central server data storage enables better monitoring of data access, thus detecting unauthorized access.

To prevent unauthorized access to data, care must be taken to set access rights to the data in the storage properly.

5.6 CESNET Storage

What to Store Here
Public Data, Internal Data, Discrete Data, Sensitive Data.

In storing sensitive data, it is necessary to perform an individual analysis of a specific case and implement appropriate measures, which may include the use of data encryption and other requirements for how to work with data.

In general, these repositories are particularly suitable for long-term storage/sharing of large amounts of data with the possibility of the geographical distribution of physical storage within the Czech Republic and the creation of multiple geographically distributed copies (backups).

What not to Store Here
Sensitive Data without carrying out the appropriate analysis and implementing the necessary measures.

Why (not) Use it like this
The use of CESNET repositories is governed by the Data Storage CESNET - Terms of Service. The repositories are operated by a Czech organization co-owned by academic institutions in the Czech Republic, and MUNI is a member of its statutory body. CESNET is ISO 27001 certified; the storage operator makes an effort to protect data from loss or disclosure to unauthorized persons. It is possible to individually agree on purchasing a *Service Level Agreement*, which provides higher guarantees for data security and availability.

5.7 External Storage

5.7.1 With MUNI Contract

5.7.1.1 MUNI Microsoft O365

What to Store Here
Public Data, Internal Data, Discrete Data, Sensitive Data.

In the case of discrete data, the use of encryption is appropriate. The storage of sensitive data (special categories of personal data, especially medical data) is possible only with adequate procedural coverage of the situation based on individual analysis and the application of security measures that result from the analysis.

Storage is especially suitable for storing data that needs to be shared with multiple people or backing up/synchronizing data from Windows personal computers to the cloud.

What not to Store Here
Sensitive Data (special categories of personal data, especially medical data) without proper analysis and procedural coverage of the specific case by appropriate measures.

Why (not) Use it like this
Data management within this cloud service is ensured by a contract concluded between Masaryk University and Microsoft. The agreement also includes "standard contractual clauses" issued by the European Commission, guaranteeing that data processing complies with EU law. EU user data is primarily stored in data centers in the EU. Microsoft's security policy complies with ISO 27001, 27002, and 27018. Office 365 also meets GDPR requirements.

Multiple storages in technically advanced data centers and special storage functions (multi-level "trash" deletion, from which data can be recovered in the event of a malware client attack, etc.) provide high data protection against damage or loss. Cloud storage also enables better monitoring of data access, improving the ability to detect unauthorized access.

5.7.1.2 MUNI Google G Suite for Education

What to Store Here
Public Data, Internal Data.

The storage is especially suitable for storing data that needs to be shared and edited in real-time in a web browser with multiple people or for backing up/synchronizing data from personal computers and mobile devices of all platforms.

What not to Store Here
Sensitive Data.

Storing discrete data is not recommended, but it is possible when using encryption.

Why (not) Use it like this
Currently, an agreement including the Data Processing Addendum is concluded between MUNI and Google. When storing data, the storage in the EU is not guaranteed.

Multiple storages in technically advanced data centers provide high protection of data against data corruption or loss.

5.7.1.3 Grammarly

What to Store Here
Public Data, Internal Data.

Due to the principle of operation of the service, it is necessary to make the data available to the service in an open form (without encryption) so that their content analysis can occur.

What not to Store Here
Discrete Data, Sensitive Data.

The data cannot be protected by encryption and is analyzed by a third party.

Why (not) Use it like this
The Grammarly service processes data outside the EU; the data cannot be protected by encryption, as the principle of operation of the service requires access to the data for their content analysis. According to the service documentation, data can also be passed on to human editors. On the other hand, Grammarly declares the contracting of its employees and suppliers following the requirements of GDPR, provides information on how to process and

secure data, and undertakes to use user data only for the needs of the service - using Grammarly for public and internal data is possible.

Users should be aware of the above when providing Grammarly data and strictly control which categories of data they provide to the service. For optimal control, it is advisable to use only the Grammarly web editor (where the service has access only to data explicitly entered by the user in this dedicated text editor), or the input keyboard for Android or iOS (where the service has access only to texts entered by the user using this software keyboard, for other texts it is possible to use another software keyboard that does not send data outside the device), not extensions for a web browser or MS Office, where it may not be clear which data can Grammarly access.

5.7.1.4 Another External Services with MUNI Contract

University, resp. its components have or may have a contract with other external cloud services providers - an example is Grammarly. In such cases, at least a fundamental legal analysis of the conditions for providing the service is needed. Still, it can be expected that at present, most such contractual relationships (especially when concluded with organizations operating in the EU environment) already include data protection guarantees in terms of retained ownership and GDPR requirements. Nevertheless, discrete data storage should always be subject to preliminary analysis, especially concerning compatibility with GDPR requirements. Contracts with non-European organizations should always be subject to legal analysis.

5.7.2 Without MUNI Contract

5.7.2.1 Other Cloud Services

i.e. public (and typically free) Google/Microsoft/Dropbox/GitHub/… storages, services such as Draw.io, Overleaf etc.

What to Store Here
Public Data.

What not to Store Here
Internal Data, Discrete Data, Sensitive Data.

Why (not) Use it like this
MUNI has no relationship or control over these repositories; therefore, it cannot guarantee anything regarding data security and data handling policy. Only a few services are indeed free - as regards free services, you typically "pay" for the service with the data entrusted to you, which you make available to the service provider, often for unlimited use. For work data, you must not allow this in most cases.

Due to the attractiveness and widespread use of these repositories, end of use cannot be expected; however, the potentially high risk of data misuse must be considered. Public cloud and similar services without explicit contractual treatment should not be offered as part of any MUNI services. Where their use is appropriate or necessary, the use for MUNI students and employees should be properly contracted.

6 Data Encryption

Data encryption can be an effective way to protect stored data from being made available to unauthorized persons. However, the risks associated with losing the encryption (decryption) key need to be considered - data encryption tools may require the end-user to take care of backing up encryption keys/passwords in case they are lost, which may be a process requiring advanced technical knowledge. **Without decryption keys/passwords, it will not**

be possible to recover data in any way! At the same time, disclosing decryption keys/passwords (e.g., their backup) to an unauthorized person jeopardizes the effectiveness of encryption as a means of data protection.

Due to the complexity of managing passwords/encryption keys, we recommend using storages that do not require encryption for a given data category. If you need help securing your data, contact the ICS MUNI workers at the e-mail address sprava-dat@ics.muni.cz.

6.1 Local Computer Storage

In the Windows operating system, it is possible to use the integrated functions of NTFS Encrypting File or BitLocker; FileVault on Apple MacOS; in GNU/Linux operating systems using dm-crypt/LUKS/EncFS technologies, etc. Alternatively, it is possible to use trusted external multiplatform tools such as VeraCrypt.

6.2 Local Mobile Devices Storage

The options for encrypting data on the local storage of mobile devices vary depending on the manufacturer and model of the device. In some cases, encryption is turned on by default and cannot be turned off by the user. Data security then depends primarily on the strength of the screen lock used.

In other cases, encryption must be turned on by the user in the device settings. For very old and/or cheaper devices, encryption may not be available at all.

Encrypting data on an external memory card may be complicated/impossible if the device supports its use.

6.3 Network/Cloud Storage

It is possible to use, e.g., EncFS technology, etc., in Unix operating systems or use trusted external multiplatform tools such as VeraCrypt. For encryption of individual files, it is also possible to use technologies specific for a given data format, e.g., integrated encryption of MS Office documents (i.e., password protection of Word/Excel/PowerPoint documents), encryption/password for ZIP archives, etc. However, it is necessary to pay increased attention when choosing a specific technology - e.g., there are historically several standards for encrypted ZIP archives, some of which provide little data protection, and nowadays, such protection can be easily overcome without knowing the password used by the user.

7 What to Look out for

7.1 Security of your Login Data

Even if the data security on network/cloud storage is at the level of physical servers/server software, etc. at a high level, the weakest element may be the end-user or the way of his authentication: If you use a weak password/password shared with other services, etc. for access, and at the same time, the password is the only item of authentication, then revealing the password to an unauthorized person can compromise the security of all data and services to which the user has access. You should never enter access information to work data into other people's computers (in a café, at a friend's, etc.) for which you have no knowledge or guarantee of their security, use your laptops, phones, etc.

To be able to use strong passwords unique for each service, it can be helpful to use a quality password manager, such as KeePass.

7.2 Private Computers Used for Work Purposes

It is essential to realize that home computers, etc., used to access work data should be subject to at least the same security requirements as workstations. Almost no one has a camera system and a gatehouse with constant supervision at home, as it is in the MUNI workplaces. That's why you should pay special attention to physical security during your absence (e.g., when you are at work), quality security locks and entrance door fittings should be necessary minimum, security doors a good improvement.

Don't forget your little ones, who not only may forget to lock the door when they leave the house, but they will often use the home computer with you. Strict separation of user accounts on the computer for work and personal purposes and unavailability of administrator privileges for children on a shared computer should be an essential security minimum, as well as the installation of quality antivirus and antimalware software and firewall. Avoid installing games and suspicious software on the computer you use for work. MUNI workstations contain only selected software in a suitable configuration. The same rules should apply to a home computer used for work purposes - only install trusted software that you have authenticated, think about software configuration (e.g., antivirus programs often automatically send files they think suspicious to their manufacturer - data that should not fall into the hands of a third party may be sent this way from your computer without your knowledge, consider disabling similar features with the software you are using). Your computer's security is determined not only by the security of your behavior but also by the installed software and its configuration.

Remember that you don't have to protect data that you don't have on your home computer. Leave your work data on MUNI network/cloud storage and download only the minimum amount of it to your home computer and only for as long as necessary. Remember the security of your login data entered into your private computer - you are responsible for its protection.