Faculty of Science Masaryk University Directive No. 1/2023

Information Security Policy of the Faculty of Science of Masaryk University

(version effective from 1 April 2023)

Pursuant to Section 28 (1) of Act No. 111/1998 Coll., on higher education institutions and amending and supplementing other laws (Higher Education Institutions Act), as amended (hereinafter the "Act"), I hereby issue this Directive:

Article 1

Subject

(1) Information Security Policy of the Faculty of Science of Masaryk University provides for secure and responsible access to various types of data and their use. It also describes the basics of secure communication between employees in order to prevent the loss or theft of data that are stored and processed in accordance with the applicable legislation.

(2) The obligations of information technology users are primarily regulated by Masaryk University Directive No. 10/2017. Directive No. 1/2023 specifies and extends legal regulations and the scope of duties of employees of the Faculty of Science of Masaryk University in the area of information technology.

(3) This Directive of the Faculty of Science of Masaryk University (hereinafter the "Faculty") is issued to ensure effective operation, support and security of the Faculty in the area of ICT *(Information and Communication Technologies),* while respecting academic freedom of the University.

Article 2

Definitions

(1) ISP: Information Security Policy of the Faculty of Science of Masaryk University. The Policy consists of a set of accesses and rules governing secure access to the Employer's data, software and hardware.

(2) ICT: Information and communications technologies

(3) OIKT: Office for Information and Communication Technologies of the Faculty of Science of Masaryk University

(4) ICT administrator: A person appointed by the department head or the head of the workplace responsible for management of hardware and software in the area of information technology.

(5) Data: Information recorded in digital form.

(6) Document: An electronic document governing management processes within the Faculty of Science of Masaryk University or establishing or in any way generally regulating the rights and obligations of employees.

Article 3

Organisation of ICT management

(1) Each workplace (i.e. Departments, Institute of Physics of the Earth, Botanical Garden, Central Library, Dean's Office) is obliged to appoint its own ICT Administrator (hereinafter the "Administrator") and to communicate this fact, including identification of the Administrator, to the Office for Information and Communication Technologies (hereinafter also the "OICT"). If the workplace is unable to appoint the ICT Administrator from among its own staff, the workplace is obliged to arrange with the OICT the provision of these services by the OICT.

(2) Employees may contact the ICT Administrator responsible for the relevant workplace. The contacts are available at https://it.muni.cz/en/sci/contacts.

(3) Employee trainings in the area of ICT are available at the MU Portal at https://portal.muni.cz/o-mne/osobni/profesni-rozvoj/skoleni. The Portal provides the user with instructions and direct contact to employees responsible for the given area.

(4) Employees may also consult the website https://it.muni.cz, a portal dedicated to ICT support at the University.

Article 4

Naming convention

(1) Naming Documents, the process of publishing Documents and ensuring access rights to the employer's Documents, especially the employer's regulations, must be consulted with the OICT, which has developed a uniform methodical procedure for the given processes. It is recommended to contact the OICT at it@sci.muni.cz

Article 5

Data

(1) Data means any and all information recorded in digital form that an employee receives, processes or creates within the performance of his/her work. Each employee should ensure appropriate storage and securing of data in a manner

preventing their loss, damage or misuse. For working with documents and data, it is recommended to use Microsoft 365 applications for which the employer provides user support.

(2) The appropriate way of working with data is determined by their classification. A certain overview of data is provided by the Masaryk University Directives: Masaryk University Directive No. 6/2013, as amended, and Masaryk University Directive No. 1/2018 Personal Data Processing and Protection. For the purposes of this Directive, data are classified as follows:

Public data: Data are 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.

Internal data: Data are intended only for internal needs of a generally defined group of persons, do not require special regulation or protection (by law, contract, etc.) and their disclosure outside the group will not cause direct damage (financial, moral, legal, etc.).

Discrete data: Data are 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); these data require regulation or protection by their nature; typically, the data is protected by law or under a contract/license (for example, personal data, data covered by trade secrets, etc.), where disclosure of such data outside the given group would most likely cause damage (financial, moral, legal, etc.).

Sensitive data: Data are strictly intended only for the internal needs of 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.); these data require special regulation or special protection by their nature; typically, the data is strictly protected by law or under a contract/license (for example, precious data covered by trade secrets, sensitive personal data, etc.), where disclosure of such data outside the given group of authorized persons is likely to cause large-scale damage (financial, moral, legal, etc.) with serious/irreversible consequences.

(3) If the employee is not sure what type of data he/she is working with, the immediate supervisor or head of the workplace will decide on the type of data. Employees may also use a contact form available at https://it.muni.cz/en/forms/consult-or-request-storage-solutions.

Article 6

Available data storage

(1) The employer allows the use of various solutions for storing data. Different storages guarantee different levels of data security. Before storing the data, employees should evaluate which storage is appropriate for which types of data. In case of any doubts regarding an appropriate storage, employees may consult the matter at https://it.muni.cz/en/forms/consult-or-request-storage-solutions.

(2) The employer allows storing data on these storages:

Portable media: External storage media that are not an integral part of any device and are used by users to transfer information between devices or to store data offline.

Local storage: Data storage built into desktop computers/laptops (typically internal HDD/SSD, etc.) in employees' offices, study rooms, etc. or data storage built into mobile devices, i.e., mobile phones, tablets, etc.

ICS Network and Cloud Storage: Data repositories operated by ICS and made available to end-users via the data network – the standard and medium network storage. CERIT-SC data repositories for high-volume research data also fall into this category.

IS MUNI Storage: Document server, Depository and similar storage capacities integrated in the IS MUNI system.

CESNET Storage: Data storage operated by the CESNET Storage Department. This category also includes services that use these storages for the physical storage of data, e.g. CESNET OwnCloud, CESNET FileSender etc.

External storage with MUNI contract: Cloud data storage provided within the Microsoft Office 365 service for Masaryk University and cloud data storages provided within the Google Workspace for Education service for Masaryk University.

External storage without MUNI contract: This category includes storages, where 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.

Storage available at the individual departments: Data may also be stored on departmental servers that meet the requirements.

(3) Annex 1 to this Directive provides a summary chart showing what types of data are appropriate to store at different storages.

(4) Employees will find further and more detailed information on data classification and storage at https://it.muni.cz/en/overviews/recommendations-for-the-usage-of-storages.

Article 7

Data management and backup

(1) For working with data, the employer provides employees especially with the following services: Supercomputing and storage infrastructure, Security tools to ensure secure work with data, Tools for effective collaboration, Consultation, support and training. Employees will find further information on these services at https://it.muni.cz/en/skupiny/vedec.

(2) Open Science principles are an integral part of the research process and service infrastructure of the Faculty of Science of Masaryk University.

(3) 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, using advanced storage with integrated data protection (e.g. cloud storage, storage on professional data servers using redundant storage),

etc. Article 6 specifies the guidelines for choosing a suitable storage (storages), which may contain data loss prevention mechanisms, based on data classification set out in Article 5.

Article 8

Email

(1) The employer's preferred and supported email is provided through Microsoft 365 applications or IS MUNI.

(2) Within the performance of their work for the employer, all employees are obliged to communicate through email accounts provided by the employer. Employees may not use email accounts provided by the employer for private purposes.

(3) If an employee installs his/her own mail server, the server must be located in the university network. The mail server must comply with all the existing security regulations of the National Cyber and Information Security Agency at https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/ and the requirements of the European Data Protection Regulation.

(4) It is not recommended to forward email communication to email addresses not provided by Masaryk University.

Article 9

Final provisions

(1) Compliance with this Directive shall be checked by the Faculty Bursar.

(2) Any exemptions from the procedure under this Directive are granted by the Faculty Bursar.

(3) The Office for Information and Communication Technologies is authorised to interpret this Directive.

(4) This Directive enters into effect on 1 April 2023.

In Brno, on 28 March 2023

Digitally signed by
doc. Mgr. Tomáš Kašparovský, Ph.D.
05.04.2023

prof. Mgr. Tomáš Kašparovský, Ph.D.

Annex 1 – Summary chart of storage types

STORAGE TYPE	USE			
	GREEN: PUBLIC DATA	BLUE: INTERNAL DATA	ORANGE: DISCRETE DATA	RED: SENSITIVE DATA
PORTABLE MEDIA (FLASH DISKS, 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; it is necessary to perform an individual analysis, use encryption and apply other security measures following from the analysis
IN MOBILE DEVICES (MOBILE PHONES, TABLETS, …)	Appropriate	Appropriate screen lock required (pattern, fingerprint reader, PIN, password)	Possible it is necessary to use encryption strong screen lock required (fingerprint reader, PIN, password)	Inappropriate possible in well-justified cases; it is necessary to perform an individual analysis, use encryption and apply other security measures following from the analysis
ICS NETWORK AND CLOUD STORAGE (“STANDARD” AND “MEDIUM” NETWORK STORAGE, SEE THE IT CATALOG, CERIT-SC STORAGE)	Appropriate	Appropriate	Appropriate	Appropriate; it is recommended to perform an individual analysis, use encryption and apply other security measures following from the analysis

STORAGE TYPE	USE			
	GREEN: PUBLIC DATA	BLUE: INTERNAL DATA	ORANGE: DISCRETE DATA	RED: SENSITIVE DATA
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 following from the analysis
CESNET STORAGE (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 following from the analysis
EXTERNAL STORAGE				
WITH MUNI CONTRACT				
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 following 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