Budapest Metropolitan University Information Technology Security Regulations

With the aim of providing a single framework for the procedures and regulations that ensure the security of the information technology systems and applications of Budapest Metropolitan University (hereafter referred to as METU), METU defines its Information Technology Security Regulations (hereafter referred to as Regulations) as follows.

The objective of the Regulations is to ensure the confidentiality, integrity and availability of the information technology systems/applications used and operated by METU and the data managed by the above systems and applications. In line with this, the Regulations aim to determine the organizational, personal, physical, information technology and administrative security requirements concerning activities related to information technology systems/applications and to lay down responsibilities related to compliance with the above specified requirements.

I. Scope of Regulations

The personal scope of the Regulations applies to each student, academic and staff employees (hereafter referred to as employees) of the University as well as to all persons and organizations in a legal relationship with the University (e.g. based on a service or supply contract) who use its information technology systems.

The territorial scope of the Regulations applies to each property, training venue and premises of the University including all off-site events.

The University pays special attention to familiarize the persons concerned with the Regulations (their ad hoc extract) to the extent necessary and to ensure their adherence to their provisions.

The material scope of the Regulations applies to the information technology systems, applications and their modules (hereafter together referred to as system) of METU, to IT, office, multimedia and data storage devices that can be connected to the IT systems, to the data and documents stored, managed and processed by the IT systems and all information technology and safety activities related to the above.

II. Definitions

Definitions applied in the Regulations relating to the interpretation of the Regulations and to the field of information technology security:

1) **Data**: a fact, an assumption in an electronic format (a single piece of information).

2) **Data set**: all the data managed within a single register.

3) **Data transfer**: the transmission of electronic data between information technology systems accomplished through online or offline electronic means.

4) **Database**: an organized collection of correlating data (data sets) which provides for the effective accessibility of correlating data based on their references to each other.

5) **Data processing**: the performance of technical tasks related to data processing operations regardless of the specific methods and tools applied to perform the operations or the location of application provided that these technical tasks are carried out on data.

6) **Data carrier**: A device that can be connected to or built into an electronic data processing system that helps to store and distribute electronic data, e.g. CD, DAT, DVD, hard drives, USB flash drives.

7) **Data management**: any data-related operation or the collection of operations regardless of the type of procedure applied, including in particular the collection, entry, record, organization, storage, alteration, use, retrieval, transmission, publication, alignment or combination, blocking, erasure, destruction of data as well as the prevention of further use of data, the taking of photographs, audio and video recordings, the record of physical characteristics (e.g. fingerprints, palm prints, DNA sample, iris images).

8) **Administrative security requirements**: requirements related to the existence and application of manuals and procedures that ensure the registration and traceability of data and workflows in the course of the use, operation and development of information technology systems including the monitoring of the performance of related tasks (e.g. maintenance and monitoring of registers, logs, registration procedures).

9) **Archiving**: a special saving process in the course of which data and data sets are deleted from the IT system and moved to a separate independent storage device. It aims at the long-term, safe and retrievable storage of data that are no longer needed in everyday activities but shall be retained.

10) **Authentication (Identification)**: an IT procedure whereby a user verifies his/her identity in the IT system to gain authorization. It might be based on knowledge factors (e.g. including a password), possession factors (e.g. including a token) or inherence factors (e.g. including anything related to biometrics) or might be based on various combinations of the above.

11) **Authorization (Permission)**: an IT process based on identification whereby a clearly identified person (device) is given procedural permission, right of access or other privileges to be able to perform his/her tasks.

12) **Internal network (Intranet)**: a protected network owned by METU to ensure the accessibility of the following:

- functional systems,
- educational systems,
- internal communications systems,
- internal intranet portal,
- further applications, databases necessary for work-related activities,

- electronic storage provided for individual and collective use.

13) **Confidentiality**: a characteristic of information systems that ensures that only authorized users can access, use and decide on the use of any piece of data or information stored in an IT system in accordance with their assigned data access level.

14) **Security event**: an unwanted or unexpected individual event or series of events leading to an unfavorable change or a previously unknown situation within the electronic information system which results in the loss of or damage to the confidentiality, integrity, credibility, functionality or accessibility of the data contained in the electronic information system. A security event might be due to the following:

- an internal problem resulting from the improper use or operation of the information technology system, failure to use or operate the information technology system in compliance with the professional standards, unauthorized access to data, violation of the physical protection system of the IT system, injection of a malicious code into the information technology system,
- a problem related to Business Process Continuity; an event or action bringing about the interruption of the continuity of operations or a disaster,
- an external problem resulting from the malfunctioning of the system related to its bona fide use by a third party, external attack.

15) **Security risk**: a threat against the information system that endangers or may endanger the proper operation of the system and/or the confidentiality, accessibility, integrity of the data managed by the system.

16) **Security compliance**: a characteristic of the information technology system referring to the extent of its conformity to IT security requirements.

17) **User**: a person using the information technology system for performing his/her duties.

18) **Physical (environmental) security requirements**: requirements (object protection, fire protection) relating to the physical environment (buildings, rooms, stores) where the use, operation or development of the information technology system take place.

19) **Functional system (application)**: an information technology system (application) that supports the operation of METU as an organization.

20) **Functional compliance**: a characteristic of the information technology system referring to the extent of its conformity to the functional requirements.

21) **Network:** the connection of computers and their peripheral devices in accordance with specific rules enabling an exchange of data and information. Its basic elements include the following: server (service provider), active and passive network elements (routers, bridges, etc.) that provide for the operation of the network and workstations. Networks may be categorized into three main types according to their area and the technology applied: local area network (LAN), metropolitan area network covering cities and countries (MAN) and wide area network (WAN) that is worldwide.

22) **Hardware**: the physical components of an information technology system (in particular those of a computer); a collective term referring to the technical-technological devices that are necessary for operation.

23) **Information security**: a dynamically changing state where – regardless of its format - information is protected, i.e. its confidentiality, accessibility and integrity are guaranteed.

24) **Information protection**: the development and implementation of organizational, personal, physical, IT and administrative provisions in the interest of information security.

25) **Information technology application**: a program running on a computer or other information technology device that aims to perform certain activities, it is centrally distributed, it may be operated centrally or locally, its access management, functional and security logging are ensured and it may consist of one or more modules (programs).

24) **Information technology security**: a state of the information technology system when the system operates properly and the confidentiality, accessibility and integrity of the data managed by the system is ensured.

25) **Information technology security requirements**: requirements related to the use, operation and development of the information technology system.

26) **Information technology environment**: a collection of information technology solutions (hardware and related basic software) that ensure the logical operating conditions of information technology systems (applications) and determine its basic database connections.

27) **Information system module**: the smallest distinct unit with an independent function within the information systems of METU.

28) **Information system**: a group of computers and their peripherals (network), the software running on computers and the data managed on computers the aim of which is to perform specific tasks, series of tasks and activities.

29) **Helper application**: a small application that enhances support activities related to the information system/application but does not perform data management or data processing activities.

30) **IT service**: a function or collection of functions available for users within the IT system of METU that cannot be classified as a module.

31) **Privilege**: authorization to perform specific operations on data (groups of data) within the information system including for example the rights to read, write, alter and delete data.

32) **Critical information system/application**: an information system or application that can only be dispensable up to four hours without causing damage to METU.

33) **Communications system (application)**: an information system that provides the communication channels (mailing, messaging and VOIP) of METU.

34) **Backup**: copying of data, data sets and applications stored and used within the information system. The process of backing up aims to ensure the restoration of data in case of damage to the primary storage space.

35) **Mobile device**: a portable electronic device with communications services that performs specific IT and communication tasks and does not qualify as a desktop computer. Such devices include laptops, notebooks, tablets, mobile phones, smart phones and external modems.

36) **Workstation**: a desktop or portable computer (laptop, notebook, etc.) provided for a user.

37) **Educational system**: an information system (application) that supports the operations of METU as an educational institution enhancing the process of education including the provision of information and learning materials for students.

38) **Log**: a data set automatically managed by the information system to ensure the tracking of and accountability for changes by recording events, user activities and the time and date when they occur in the system.

39) **Logging**: the automatic recording of events, user activities and their time and date when they occur in the information system to ensure the tracking of and accountability for changes.

40) **Program**: a series of instructions written in a programming language that may consist of a single program module or groups of program modules.

41) **Availability**: providing for the accessibility of information systems and the usability of data stored therein for a user with the appropriate privilege.

42) **System administrator**: a person who is responsible for the supervision and management of operating systems and database management systems. System administrators have the highest-level privileges provided by the systems and they are in charge of system-level privileges.

43) **Personal security requirements**: professional and security expectations of persons maintaining or using the information system that aim to eliminate or minimize security risks resulting from voluntary behavior and activities or negligence.

44) **Organizational security requirements**: professional and security expectations specified for the organization that maintains or develops the information system with the aim of clarifying and setting out rules related to workflows, jobs and responsibilities in official regulations.

45) **Software**: the logical elements of a PC and an information system; the collective term referring to the operating systems (system services) and application programs (applications).

46) **Full documentation**: documentation specified in the Regulations (e.g. developer documentation, user and maintainer guide/handbook, test documentation).

46) **Testing system**: an information system (environment) that aims to support the testing and teaching of software that is being developed or introduced.

III. Classification of Information Systems

The classification of information systems includes the basis and classification of planning and performing activities and the development of regulations related to individual information systems and data carriers.

Based on their purpose, information systems may be classified as follows:

a) functional information system,

b) education information system,

b) communications information system.

Based on ownership, information systems may be classified as follows:

a) private information system,

b) information system owned by a third party.

Based on its supervision, information systems may be classified as follows:

a) an information system supervised by METU,

b) an information system supervised by a third party.

IV. Organizational IT Security Requirements

With regard to the supervision and maintenance of information systems, databases and devices, the risks resulting from malicious activities or errors due to failures in joint operation shall be eliminated or minimized to an acceptable level by the University.

V. Personal IT Security Requirements

Each employee of METU shall declare in writing that he/she is aware of and accept the Regulations. In addition, it must be ensured that students become aware of the Regulations.

Only persons who have made the above declaration may be granted access to the information systems and the data stored therein.

The above declaration shall be completed by each employee at the start of his/her employment. Persons in employment at the University at the date of the introduction of the Regulations shall sign it within two months following its publication.

The declarations shall be attached to the personal records and kept by the HR Office.

VI. Physical Security Requirements

IT devices shall be installed and stored in a way that ensures that only those with the appropriate privilege have access to them.

No IT, office or multimedia device or data carrier shall be taken away from the premises of METU without the permission of the direct supervisor or teacher and a completed property receipt template.

VII. Information Technology Security Requirements

The planning and implementation of development, maintenance and security activities related to individual information systems and data carriers and the preparation of development, maintenance and security documents and provisions shall be carried out in a way that they guarantee the necessary and sufficient level of information security in accordance with the rules on security classes. In line with the above principles, a risk-proportionate, differentiated and multilevel information security protection system shall be established and operated.

When preparing the planning documentation for the purchase and development of IT infrastructure which precedes the actual physical implementation, the future accessibility of various functions shall be evaluated for the client from a professional and information security point of view. During this stage it has to be ensured that the principle of minimum functionality is enforced throughout the full life cycle of the system.

Only authentic, centrally purchased, licensed and registered software shall be installed in the information systems of METU. The number of software installations cannot exceed the amount of licenses purchased. The central register of licenses is managed by the Directorate of Information Technology.

The information systems of METU shall be expanded only by those system components that METU has tested and accredited from an IT/technology point of view and approved in terms of security considerations. The same shall apply to the installation of new system components.

Only those IT, office and networking devices can be connected to the information systems of METU that the Directorate of Information Technology has tested and accredited from an IT/technology point of view and approved in terms of security considerations. No testing and approval are needed in case of USB flash drives (pen drives).

The use of devices and technologies capable of communication outside the network of METU – e.g. Wi-Fi, Bluetooth, external modems, access to the internet using radio waves, etc. – by connecting them to the network of METU is forbidden except for certain cases and devices approved and provided by the Directorate of Information Technology.

Operations performed in the information systems shall be logged in a way that ensures the identification of the user. Databases, software may be uploaded in the system only after a virus protection scan has been performed in accordance with the provisions of the Regulations.

VIII. Administrative Security Requirements

The full life cycle of information systems shall be documented by the Directorate of Information Technology of the University. In case of external partner involvement, the necessary documents shall be taken over and registered including the stages of planning, development, further development, testing, checking, operation, maintenance and termination.

The documentation of an information system is considered to be full in case it contains all essential data related to its conformity with functional and security requirements.

The hardware and software elements, IT, office, multimedia, educational and communications devices as well as data carriers owned and used by METU shall be registered in a way that ensures their individual identification.

IX. Rights and Responsibilities of Users

The user is entitled to use the IT, office, multimedia, educational and communications devices that are necessary to perform his/her work and learn how to use them with the help of documentation or at specific courses.

The user may only use the IT, office, multimedia, educational and communications devices provided to him/her for their intended purposes in accordance with the user's clearing level and to perform work-related activities or activities that are related to the tasks and objectives of METU.

The logged-in user is responsible for the protection of the workstation against unauthorized access and for each transaction carried out on the workstation including all the stages from log-in to log-out. This responsibility exists even if the transaction has been performed by a third person in case the above transaction occurred as a result of the user's non-compliance with the Regulations.

To prevent unauthorized access, the user shall lock the workstation and protect it by using a screen saver password. In case the above is not possible, the user has to log out or turn off the workstation in case he/she leaves it unattended. If possible, automatic screen locking shall be enforced.

Unless otherwise stated, the user has to turn off the workstation at the end of the work day or when finishing his/her work.

In case a workstation is used by several employees, the user may only leave it when he/she has logged out of each running program and the identified connection.

The user shall retain all the portable IT, office, multimedia, educational and mobile devices as well as data carriers provided to him/her and prevent unauthorized access to them by exercising personal supervision or by locking the device or the data carrier.

Senior staff members of the University are entitled to and shall define the array of IT, office, multimedia, and communications devices that the employees under their supervision need to perform their work including the specific information systems to be used together with the privileges necessary to access those systems.

Senior staff members shall ensure that the employees under their supervision have an up-to-date knowledge of the IT security requirements.

In case of detection of any breach of security requirements, senior staff members shall

1. immediately take the necessary measures to restore security and
2. initiate, if appropriate, the suspension of the use of the system if the breach of security requirements is limited to an identifiable system,
3. investigate the circumstances of the security event in particular with a view to determining personal liability,
4. initiate a liability procedure once personal liability has been established.

Employees whose responsibilities include maintenance and development may only use their extra privileges granted to them in addition to their user privileges as intended and in accordance with the Regulations.

X. Provisions Pertaining to External Persons in a Legal Relationship with the University under the Civil Law

Access to the information systems and devices of METU shall be granted to these persons exclusively on the basis of a valid and effective contract, in a documented manner and by clearly defining their privileges.

XI. Identification of Users, Granting Authorization to Use Systems, Password Policy

The user may only use the information system following his/her clear identification and in accordance with the privileges defined for and provided to him/her.

In the course of the use of the information system, the individual identification of the user shall be continuously ensured.

Each user shall be assigned an exclusive, individual ID with an individual password for his/her personal use.

The ID of the user shall contain his/her family name and the first letter of his/her first name. Special, pre-recorded IDs of the operating system, special and test user names used by employees performing special IT tasks as well as technical users for database connections are defined as an exception to the above rule.

User passwords shall meet the following minimum criteria automatically monitored and required by the system. A user password shall

a) be at least eight-character long,
b) contain a combination of numerals, upper-case and lower-case letters,
c) not contain a series of characters that is repeated or can be easily guessed,
d) not contain any personal references,
e) be valid for a maximum of 90 days.

Passwords shall be changed:

a) after the first log-in following the record of the user ID in the information system,
b) after they have been reset or overwritten by an employee working for the organizational unit in charge of IT maintenance,
c) in case an unauthorized person might have become aware of the password or the password might have become public knowledge in any way,
d) when they expire.

Users shall keep their passwords confidential and prevent unauthorized persons from compromising them. It is forbidden to record passwords in a manner that enables other persons to become aware of them and to communicate passwords to any other persons in any way.

XII. Use of Network and Internet

In the course of the use of a METU workstation that is connected to the internal network, virus protection rules shall be continuously enforced. Virus protection is provided centrally and it is strictly forbidden to bypass it or turn it off.

Only data sets and programs that are necessary for work may be uploaded or installed on any METU workstation that is connected to the internal network. Data sets or information cannot be installed or copied on these devices nor can they be made public on the internal network in case

a) they infringe any legal provisions, in particular those related to copyright, data protection or the protection of personal rights,
b) they endanger or may endanger the intended operation, and security of the internal network, in particular when they use its resources in an unreasonable or deliberately excessive or wasteful manner.

The University restricts access to the internet for private purposes. It is the direct supervisor of the employee who is entitled to restrict the employee’s access to the internet for private purposes and

to determine the extent of the above restriction. Where appropriate, considering the tasks of the employee, his/her direct supervisor may grant exemption from this restriction.

Workstations that are not provided by METU cannot be connected to the internal network unless previously permitted by the Director of Information Technology or his/her supervisors. Even in this case, similarly to the use of internal computers, rules pertaining to virus protection shall be enforced with a strict prohibition on turning off the virus protection software or the use of the workstation without virus protection. During this period, data sets or information that endanger or may endanger the intended operation and security of the internal network cannot be used. The same applies to data sets and information that use the resources of the internal network in an unreasonable or deliberately excessive or wasteful manner

Devices connected to the internet (Wi-Fi) network belong to the personal responsibility of their user. Thus, in case the device connected to the Wi-Fi network is proven to have caused the defective operation of any device of the internal network or lead to loss of data or any other damage, the user shall be made liable for incurred damages and action for damages against the user may be initiated.

XIII. Use of the Electronic Mailing System

When tasks specified by METU are performed through electronic mail services, the official mailing address provided by METU shall be used.

Personal responsibility for using a private electronic mailing address for work purposes lies with the user who shall be responsible for the information contained in the mail and shall be liable for damages in case of abuse, voluntary or involuntary damage.

The messages forwarded in the internal mailing system shall be primarily related to official and community activities and purposes, the storage of chain emails and other large private email messages in the central mailing system has to be avoided.

The attachments and links in unknown or unsolicited emails shall not be opened without due care and it is forbidden to give any information such as user names or passwords in these emails. (THE DIRECTORATE OF INFORMATION TECHNOLOGY NEVER SENDS REQUESTS FOR PASSWORDS AND CONFINDENTIAL INFORMATION IN AN EMAIL!)

The electronic email address provided by METU cannot be added to external mailing lists or services that are not related to work activities nor can they be given as default address.

Employees' accounts used in the mailing system of METU will be archived when they leave the University but by accepting the attached Appendix 1, employees approve that the messages in their accounts may be used for official purposes by METU.

Students' accounts will be deleted without being archived once their student status at the University terminates.

XIV. General Requirements of Maintenance Security

The Director of Information Technology is responsible for the accessibility and proper operation of IT systems.

In the course of providing remote assistance (remote support), client-side programs that in any way ensure remote access to the information on the user's screen and the remote control of the user's input devices may only be launched by the user, they cannot be installed as a program that starts automatically. METU applications that support education constitute an exception to the above rule. Before the introduction and application of remote assistance, the user shall be informed about the content of the service and the operations performed during the provision of the service.

METU has the right to centrally regulate the setup of the screen savers, wallpapers, screen lock as well as the installation of approved programs and the deletion of unapproved, forbidden programs.

It is strictly forbidden to install or run programs on any METU device that is not approved by the Directorate of Information Technology.

The accessibility of data managed and stored in the information systems shall be ensured through regular backup or emergency backup when needed.

Data sets managed in the information systems that are not necessary in the performance of daily work activities of employees but whose retention is justified shall be archived.

XV. Virus Protection

Virus protection procedures, rules pertaining to virus protection including a response plan shall be established in a way that

a) ensures the possibility to provide for continuous virus protection monitoring,
b) supports the recognition of real alerts,
c) it is suitable to recognize events incurred by severe negligence and intentional actions,
d) ensures the evaluation of the general virus security situation,
e) enables the timely identification of new threats.

Tasks related to maintenance and maintenance supervision with regard to virus protection are carried out by the Directorate of Information Technology.

Goals of virus protection:

a) definition of a protection system that is sufficient and is based on professional standards and the principle of proportionality,
b) regulated and efficient prevention of effects of malicious software,
c) provision of a procedure to avert attacks launched and to mitigate damages.

With regard to workstations and servers, the internal network of METU is protected against viruses, only data that have been scanned for viruses can be forwarded to the networks.

With a view to the protection of the internal network:

a) the virus protection system is constantly monitored,
b) the virus protection system has a central server and a management surface,
c) the central management is capable of monitoring safety and security, thus it can send failure warning signals, alert signals and information to be evaluated,
d) the virus protection system is capable of updating itself several times a day,
e) virus incidents are taken care of,
f) the virus infection situation is regularly assessed.

The tasks related to virus protection at METU are performed by the staff members of the Directorate of Information Technology who:

a) are responsible for virus protection management,
b) know the virus protection systems of METU, track the developments in the field of applied solutions and professional requirements and are aware of the potential threats targeting METU,
c) continually track and analyze the virus protection situation of METU,
d) document virus incidents and are responsible for the preparation of an annual report on the virus protection situation of METU,
e) participate in the management of virus events and virus incidents that are considered to be security events, take appropriate measures if needed and perform preventive and defensive tasks,
f) support the virus protection activities of users.

In addition to the above, the coordinator appointed by the Director of Information Technology of METU is responsible for

a) the professional management and supervision of the virus protection systems,
b) the determination and fulfillment of professional requirements pertaining to the virus protection of METU,
c) the management and supervision of tasks related to virus protection technologies,
d) ensuring that the updates of virus protection devices are downloaded and accessible in accordance with the requirements and on an as-needed basis,
e) submitting proposals for outlining the directions for the development of virus protection systems,
f) contributing to the description of the technological specifications of devices to be purchased for virus protection,
g) preparing the installation and configuration guides and the maintenance procedures of virus protection devices.

Virus protection documents:

a) Annual report addressed to the Deputy CFO prepared not later than the 1st of February each year.

b) Virus protection protocol that has to be prepared after investigation into any virus incident occurring on any workstation or server in the internal network.
c) Single reports on cases and periods specified by the Director of Information Technology.

Virus protection rules related to workstations provided by METU in the internal network of METU:

a) Only workstations equipped with virus protection can be connected to the internal network of METU.
b) Real-time virus protection devices shall be used.
c) The virus protection device provided by METU for that purpose shall be used.
d) The option for individual virus infection scans shall be provided including the scanning of attachable data carriers and each piece of input data.
e) The virus sample database and anti-virus software of the workstation shall be automatically updated.
f) Workstations shall be set up in a way that the user cannot turn off its virus protection system, thus it is strictly forbidden to stop virus protection except for forced deliberate shutdowns or when there is a need to eliminate and prevent failures.
g) Workstations without working virus protection cannot be used.
h) A monitoring tool shall be provided for the IT personnel monitoring workstations so that computers working without properly operating anti-virus software or without the proper updates may be identified.

Virus protection rules related to servers:

a) It is compulsory to protect network servers that are threatened by viruses if there is an available virus protection device which is compatible with the system, has been checked by METU and proven to provide sufficient protection.
b) It is compulsory to use virus protection devices on each Windows server.
c) It is compulsory to use real-time virus protection which shall be provided for each input and output device and channel.
d) Virus protection shall be set up in a way that a virus scan of each data set is performed directly before it is written on the server.
e) A virus scan of the full system shall be performed as a scheduled idle-state task at least once in every two weeks.
i) Updates shall be performed with the frequency of at least 24 hours.

Virus protection rules related to electronic mail services:

a) Each e-mail received by the system of METU shall be scanned for viruses.
b) In case of centrally detected virus incidents, infected emails are not forwarded to the addressee but he/she has to be informed about the incident. Any such virus incident shall be logged.
c) External emails reaching the METU network shall be checked by applying a central (system-level) virus scan which shall be set up in a way that prevents the delivery of emails marked as spam.

General rules related to the scan of external data carriers:

a) External data carriers shall be scanned for viruses in case the loading or use of data takes place on a personal computer. Virus scan in this case shall be performed by the user who loads the content into the information system at the input point. Responsibility for the above virus scan shall lie with the user.
b) In case the data carrier is infected with a virus, it cannot be forwarded to or processed by the information systems of METU.

The user shall report the following cases either directly or through his/her supervisor:

a) the user recognizes that the virus protection is not running or working properly on his/her workstation while performing his/her working activities, the software sends error signals, the user cannot launch a custom scan to check individual files or data carriers for infiltration,
b) the virus protection of the workstation sends a notification on infiltration,
c) the user experience an irregularity indicating a potential threat.

To-do-list when virus incidents occur:

The user shall report the virus incident he/she has become aware of without delay to the Directorate of Information Technology directly or through his/her supervisor. The Directorate of Information Technology shall immediately take the necessary measures to handle the threat, thus it

a) investigates the situation in case of virus incidents report and automatically eliminated virus events,
b) scans and monitors the workstation or the server and its connections in case of repeated incidents,
c) directly eliminates threats in case automatic removal fails,
d) informs users affected by the incident,
e) prohibits work on the infected workstation if needed (and grants permission to continue work once the virus incident is resolved),
f) ensures that the virus incident is investigated and a virus protection protocol is prepared in cases when automatic removal fails.

XVI. Closing Provisions

1. The Senate of Budapest Metropolitan University discussed and approved the Information Technology Security Regulations at its session of 17 March 2017.

2. The present Regulations shall be published in Hungarian and English and shall be made available for each citizen of the University.

3. The present Regulations enter into effect on 21 March 2017.

Dr. habil. László Vass CSc

Rector

Budapest Metropolitan University