Budapest University of Technology and Economics

Chancellor's order No. 23/2017 (18/12)

SECURITY AND ASSET PROTECTION POLICY

Effective date: December 18 2017
To enable tracking of modifications of regulatory instrument(s) annulled as of the effective date:

a) a) University Order on Security issued on September 27 1989, Circular No. 100.968/1997 of the Director General
b) b) Circular No. 22/2009 of the Director General

(24/06) Revised by:

⇨ professional compliance: Directorate of Asset and Institutional Security
⇨ legal compliance: Legal Directorate

Person in charge: Zsolt Marinovszky
Issuer: Gyula Barta-Eke, chancellor

TABLE OF CONTENTS

Pursuant to the provisions of Act V of 2013 on the Civil Code, Act CCIV of 2011 on the National Higher Education, Act CXCV of 2011 on Public Finances, Government Decree 368/2011 (31/12) on the implementation of the Act on Public Finances, Act XXXIII of 1992 on the Legal Status of Public Servants and Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter: Security Services Act), I hereby approve the Security and Asset Protection Policy of the Budapest University of Technology and Economics (hereinafter: University) as follows.

Chapter I

GENERAL PROVISIONS

§ 1

(1) The personal scope of the Policy extends to:
   a) all persons employed by the University as civil servants or in other status (hereinafter: university staff) and the University's students,
   b) all persons performing work or any related activities on the University's premises as tenants, contractors or in other status or situated on the University's premises as visitors or for other purpose.

(2) The physical scope of the Policy extends to all properties controlled and used by the University.

(3) This Policy defines the asset protection responsibilities of the University's organisational units, the correct procedures to follow in case of a potential incident and the general security and asset protection requirements and responsibilities concerning work and other activities performed on the University's premises and buildings operated in public-private partnerships.

(4) Liability for any loss or damage resulting from non-compliance with the provisions of the Policy is governed by Chancellor's Order 10/2015 (30/09) on the Compensation Policy of Public Servants and the Regulations pertaining to BME Students on Disciplinary Action and Compensation for Damages.

Chapter II

SECURITY AND ASSET PROTECTION RESPONSIBILITIES

§ 2

(1) Security and asset protection is intended to facilitate the protection of the University's (public) assets and the personal property (belonging to the University's students, teaching and other staff) as well as to maintain order and security at the University.

(2) Security and asset protection responsibilities will be performed in a manner to ensure that:
   a) laws and regulations pertaining to asset protection are complied with and such compliance is monitored and that any actions violating or compromising such laws and regulations are prevented, blocked and detected;
   b) public and personal property is protected;
   c) any actions against public property are prevented, blocked and detected;
   d) a procedure to impose sanctions on the persons damaging public and personal property in harmony with the nature and the severity of the offence is initiated;

e) engagement in the establishment and maintenance of the University's order and security is provided for;
f) facilities are protected, such protection is organised and the security of facilities and storages is monitored;
g) human and other resources of security services as well as security devices and equipment are provided for and their working order is constantly checked;
h) rules concerning the traffic of people and assets are defined, such rules are caused to be met and are monitored;
i) record-keeping requirements concerning incoming and outgoing deliveries are met, the required delivery documents are checked;
j) requirements for cash transfer and cash registers are complied with and such compliance is monitored;
k) immediate action is taken in the event of incidents or criminal acts and that the scene and order is secured;
l) requirements for confidentiality are complied with and such compliance is monitored;
m) cooperation with the University's bodies and persons involved in other protection responsibilities is maintained; and
n) contacts with the law enforcement authorities, the prosecutor's office and courts are maintained.

§ 3

(1) The University performs its responsibilities concerning its security and asset protection activities and manages the persons involved as follows:
a) Senior officers with security and asset protection authority:
aa) the rector;
ab) the chancellor;
ac) the director of the Directorate of Asset and Institutional Security;
ad) the heads of the general organisational units.
b) Dedicated security and asset protection organisational units and service providers:
ba) Department of Asset Protection; bb) Asset Protection Service;
bc) security service, patrol service, security guard service, reception service.
(2) The chancellor is responsible for:
a) obtaining and allocating the funds required to perform university-wide security and asset protection responsibilities;
b) checking or delegating others to check compliance with the University's requirements concerning cash transfer and handling;
c) determining the University's requirements concerning cash transfer and handling.
(3) The director of the Directorate of Asset and Institutional Security is responsible for:
a) controlling the University's security and asset protection activities;
b) authorising activities outside normal opening and working hours (work activities, events etc. on public holidays and on days outside the University's normal opening hours);
c) if required, ordering tighter security controls and security services to enhance safety and security;
d) directly controlling the work of the head of the Department of Asset Protection;
e) making arrangements to report an incident to the police, if required, maintaining contact with law enforcement authorities and carrying out official communication tasks in their competence;
f) obtaining compensation for damage suffered by the University.

g)

(4) The heads of the general organisational units cause the heads of the organisational units under their control to comply with the rules adopted to protect the University's assets and property, they regularly review the measures taken by such heads and manage the asset protection resources at the level of the general organisational units;

(5) The main asset protection responsibilities of the heads of the organisational units:

a) they are responsible for the protection of physical assets, resources managed by the organisational units under their control and for safekeeping the property managed by the University. Pursuant to the Chancellor's Order 14/2015 (05/10) on the rules concerning inventory checking and recording tasks, they are responsible for setting up the procedures for the management and safekeeping of the physical assets and for the maintenance of workplace records within their organisational unit and for checking compliance with such procedures.

b) they are responsible for determining the asset protection tasks of their direct reports and for checking the performance of such tasks.

c) within their organisational unit, they are responsible for determining the scope of competence concerning cash handling for management and employees under their control and for checking compliance on a regular basis. within their area of competence, they are responsible for adopting measures to protect the University's property and for checking the implementation of such measures (procedures to issue keys, physical asset records etc.). In case they are not authorised to adopt the required measures, they must report this to the director of the Directorate of Asset and Institutional Security.

d) in case of damage to the University's property (in case of the necessity of urgent action, e.g. crime), they are responsible for notifying the security service. They must investigate the case and initiate a procedure to impose sanctions, if necessary.

e) in case of an incident, they are responsible for notifying the Dispatcher Service and the head of the Department of Asset Protection without delay and for taking any actions that prevent or mitigate any further loss or damage and do not compromise the normal procedures followed in such situations. (Incidents in particular include natural and industrial disasters, major instances of environmental pollution, epidemics, serious workplace accidents, acts of vandalism, crimes etc.)

f) they are responsible for maintaining the integrity and good working order of the asset protection systems managed by their organisational unit and for controlling and checking their use. No such equipment may be installed, decommissioned or altered without the consent of the director of the Directorate of Asset and Institutional Security.

g) they are responsible for informing the staff of the organisational unit under their control about responsibilities and obligations concerning asset and property protection.

h) they are responsible for informing the director of the Directorate of Asset and Institutional Security in writing on the persons to be notified in case of incidents and their contact information. Such information must be updated as required.

(6) The head of the Department of Asset Protection

a) professionally coordinates and controls the University's security and asset protection activities under the direct control of the director of the Directorate of Asset and Institutional Security.

b) The main responsibilities of the head of the Department of Asset Protection include:

ba) the professional supervision, review of the University's security and asset protection activities.

aa) control of receptions and security guard services.

bc) the professional supervision and control of the installation and operation of asset protection systems.

bd) in case of a crime, arrangements to secure the scene, if required, participation in the procedure.

be) in case of damage suffered by the University, participation in the preparation of a report.

bf) formulation of rules for the access of people and vehicles to the University and of vehicle parking and ensuring compliance with such rules.

bg) if the violation of the Policy results in damage to the University, caused by voluntary or negligent behaviour, participation in the investigation and proposal for sanctions to be imposed.

bh) checking compliance with this Policy.

bi) professional and organisational instruction of the employees of the Department of Asset Protection (Dispatch Service).

bj) liaising with external contractors carrying out asset protection responsibilities at the University.

§ 4

(1) The University's asset protection organisational unit is comprised of the direct employees and the Dispatch Service of the Department of Asset Protection of the Directorate of Asset and Institutional Security.

(2) The responsibilities of the various units of the Department of Asset Protection are described below:

a) The head and the Assistant(s) of the Department of Asset Protection are authorised to:

aa) require persons entering or situated on the University's premises to present some form of identification.

ab) require persons engaged in unlawful acts to discontinue such acts.

ac) detain persons caught in the act of committing a crime until the arrival of the police and use force against them, if necessary.

ad) access any room of the University and carry out any necessary asset protection actions there.

ae) request information or input from anybody, complete hearing records, if required, and receive the University's documents for review.

af) make recommendations for the prevention of offences and the adjustment of human and other resources necessary for the performance of security and asset protection responsibilities.

ag) instruct staff carrying out security guard and reception services.

b) The Dispatch Service of the Department of Asset Protection

ba) supervises and controls the University's strategic security, alarm and intrusion detection, fire alarm and access systems as well as surveillance camera network on constant duty, 24 hours each day.

bb) directly controls the Asset Protection Service and takes action as the specific situation requires.

bc) maintains direct contact with the University's operation and maintenance staff.

bd) takes action in situations requiring immediate technical intervention. (e.g. utility failure).

be) takes action autonomously outside of normal working hours according to the relevant regulations and policies.

bf) fulfils the reporting obligations specified in applicable regulations and policies.

bg) organises found property as specified in Annex 9 (in compliance with all applicable rules).

§ 5

(1) Security and asset protection services provided by external contractors:

a) The reception service

aa) participates in the management of asset protection responsibilities and crime prevention;

ab) issues keys under its control to authorised persons, receives returned keys, ensures the safekeeping of keys and maintains records of these activities;

ac) monitors pedestrian traffic, provides directions, information. ad) records events in an official reception log;

ae) checks incoming and outgoing deliveries based on relevant documents, maintains the required records; af) participates in the management of the guarding and security responsibilities of buildings, rooms;

ag) carries out the correct locking and unlocking of buildings;

ah) in case of an incident, notifies the Dispatch Service without delay;

ai) duly reports all actions taken and records such actions in the reception log.

b) Furthermore, the reception service is authorised to:

ba) require persons entering or situated on the University's premises to present some form of identification;

bb) refuse the entry of unauthorised persons or persons under influence and remove such persons from the premises;

bc) check luggage, delivery documents;

bd) require persons engaged in unlawful acts to discontinue such acts;

be) detain persons caught in the act of committing a crime.

c) The Asset Protection Service

ca) ensures, based on a contract, that all necessary human and other resources are available to perform the responsibilities of security guard and reception services (in the IT building).

cb) prepares the schedule of reception service staff of the IT building and ensures that the reception service is staffed at all times as required.

cc) reports all professionally relevant information to the head of the Department of Asset Protection. It requests professional opinion from the head of the Department of Asset Protection when anticipating any actions in the field of asset protection and they consult, if necessary.

cd) implements asset protection measures based on this Policy and the independently drafted order of Security Guard Services approved by the director of Asset and Institutional Security.

ce) ensures that the asset protection staff receives further training on a regular basis.

cf) must carry out its activities according to the provisions of the Act on Security Services.

d) The security service and patrol service

da) the University contracts an external contractor to carry out daytime patrol services, to protect its physical assets at night and on public holidays and to transfer and guard cash as required by applicable rules.

db) security guards are authorised to require the presentation of some form of identification and check luggage, vehicles and delivery documents on the University's premises. Furthermore, they are authorised to require persons engaged in unlawful acts to discontinue such acts and detain persons caught in the act of committing a crime. They are also authorised to carry a self-defence tool (baton) visibly and to patrol during night shifts and on public holidays with a dog (as required by applicable rules) on the University's premises.

dc) must carry out its activities according to the provisions of the Act on Security Services.

(1) University staff and students are responsible for:
   a) protecting and safekeeping the University's and personal property.
   b) handling tools and equipment used with due care and ensuring their safe storage.
   c) informing their direct superior, in case of university staff, and informing their instructor, in case of students if they become aware of proven information that the University's or personal property is compromised or has been damaged.
   d) in case of university staff leaving a room as the last person, switching off all electrical appliances in the room, safely locking the room and setting intruder detection (alarm) system, where available.
   e) in case of university staff and students, in accordance with the Regulations pertaining to BME Students on Disciplinary Action and Compensation for Damages, in case of students, in association with their academic obligations and during the period of their student status, for compensating the University for any unlawfully caused loss or damage and handling physical assets and property owned by the University with due care.

Chapter III

INCIDENT MANAGEMENT

§ 7

(1) In case of a burglary, signs of burglary or other serious crime:
   a) the Dispatch Service of the Department of Asset Protection, the head of the Department of Asset Protection and the person designated by the head of the affected organisational unit must be promptly notified.
   b) the police and, if required, other authorities must be notified with the involvement of the above mentioned persons.
   c) the scene must be secured until the police investigation begins; the crime scene must be guarded by a security guard or a public servant of the University. In such situations, even persons authorised to access the area are refused entry.
   d) when the police investigates the crime scene, the University's employee designated by the head of the affected organisational unit must be present and is authorised to make a statement (concerning the amount of loss, damage and identification of affected persons and physical assets) on behalf of the affected organisational unit.

(2) In case of a threat to detonate an explosive (bomb threat):
   a) the Dispatch Service of the Department of Asset Protection, the head of the Department of Asset Protection and, in case of an event, the organiser or its representative with powers to act must be promptly notified. The person detecting (receiving) the threat notification must promptly inform the person in charge of security and the Dispatch Service of the Department of Asset Protection via telephone.
   b) The employee of the Dispatch Service of the Department of Asset Protection must inform the police (if the person who first became aware of the threat is present, then that person must do so immediately after becoming aware of such threat).
   c) After the police has been informed, the procedure described in Annex 1 must be followed.
   d) The building(s) then must be evacuated and any panic must be prevented.
   e) Primarily the head of the Department of Asset Protection or any other member of the University's staff must inform police arriving at the scene if they noticed any persons at the scene who are acting in an odd manner and are particularly inquisitive.

(3) In case of a suspected explosive device, the Dispatch Service and the head of the Department of Asset Protection and the police must be informed.

(4) When a wartime explosive device is discovered, any work activities in and around the place where it was found must be promptly discontinued, the area must be closed down and guarded until the police arrives.

(5) If a letter bomb is found, it must be left untouched, the room and its surroundings must be evacuated and must be guarded until the police arrives.

a) Main characteristics of a letter bomb

aa) the name of the sender is not indicated or is unknown.

ab) the letter or package seems heavy for its size and is uneven.

ac) it feels stiff and rigid and suspected to potentially contain wires and unusual objects. ad) it has strong marzipan, almond or oil odours and the envelope has oily stains. ae) the wrapping is very precise, careful (adhesive tape, strings).

af) the envelope usually contains the restrictive marking "to be opened by addressee only".

(6) If any suspicious items or parcels are discovered (i.e. if a concealed explosive device, bomb, is suspected to have been found), the origin or owner of which is unknown, they must be left untouched. In such situations, the threatened area must be evacuated and the rooms, building must be guarded until the police arrives by leaving escape routes free. Required response:

a) inform emergency services and other entities (police, fire and emergency medical services, as required: the Gas Company of Budapest, Electricity Company etc.);

b) inform the Dispatch Service and the head of the Department of Asset Protection and the director of the Operation Directorate.

(7) In case of fire, explosion and major utility failure:

a) inform the Dispatch Service and the head of the Department of Asset Protection, the director of the Operation Directorate and the Maintenance Department or its employee on duty.

b) inform emergency services and other entities (police, disaster relief services, fire and emergency medical services, as required: the Gas Company of Budapest, Electricity Company etc.).

c) in case of fire, follow the procedures described in the Fire Safety Policy.

d) in case of a gas leak, the building must be evacuated without delay, disclosing the reason for the evacuation and ensuring that no lights and electrical equipment are turned on and no open flame is used.

e) turning power off across the building is only permitted at the electrical service panel located outside the building by involving the staff of the Maintenance Department.

f) in case of a plumbing failure, the main shut-off valve may only be switched off by the staff of the Maintenance Department.

(8) In case of signs of illegal drugs (Annex 2):

a) Please inform:

aa) the Dispatch Service of the Department of Asset Protection ab) and the head of the same department

ac) the police.

b) If a person selling, disseminating or consuming a substance suspected to be an illegal drug is detected, the Dispatch Service of the Department of Asset Protection must be promptly notified, preferably without the affected person noticing such action.

(9) Reporting responsibility

a) The reporting of any, voluntary or negligent, action causing damage in public property managed by the University to the competent authorities is the responsibility of the director of the Directorate of Asset and Institutional Security.

b) The director of the Directorate of Asset and Institutional Security files such written report with the involvement of the legal counsellor of the Legal Directorate and simultaneously they make claims for civil damages and, if possible, file a claim with the insurance

company for compensation.

Chapter IV

SECURITY RESPONSIBILITIES

§ 8
The University's opening hours

(1) The University is open from 6 a.m. to 10 p.m. on working days.

(2) Access outside normal opening hours is allowed through the receptions of the constantly operating Central Building, Building E, the IT Building
and Building Q with the written permission of the director of the Directorate of Asset and Institutional Security. A request for such permission must be submitted by the head of the affected organisational unit to the Directorate of Asset and Institutional Security preferably until 2 p.m., two working days prior to the requested date.

§ 9
Rules concerning the use of the University's card access control system

(1) In order to protect the University's physical assets and to respond to the request of the organisational units concerning the speeding up of access outside normal opening hours, proximity card access control systems are installed at the main entrances of the following buildings: Bldg. CH, Central Bldg., Bldg. F, Bldg. ÉL, Bldg. Z (entrance on Bertalan street), Bldg. D, Bldg. ST (entrance from the direction of Bldg. E), Bldg. G, J, E, H, T, R (entrance from inner courtyard), Bldg. A, IT Bldg. and Bldg. Q. Outside normal opening hours (from 10 p.m. to 6 a.m.) and on public holidays, the University's buildings may only be accessed with an access card in absence of the above mentioned written permission.

(2) Applications of the organisational units based in the buildings for access cards must be forwarded in writing, via fax or email to the director of the Directorate of Asset and Institutional Security. On public holidays, the access of student groups collectively is allowed with the access card of the person accompanying them provided that the Directorate of Asset and Institutional Security has been notified in advance in writing by the competent organisational unit.

(3) Access to areas equipped with an access control system is only allowed to persons, when the system is active, who have been supplied by their organisational unit both with an access card and permission to enter. Levels of access to access cards are defined by the head of the competent organisational unit. At the termination of their employment with the University, staff must return their access cards to the Directorate of Asset and Institutional Security.

(4) Access cards must solely be used by their holders, they may not be passed on to others or used to allow the entry of other persons except in cases referred to in paragraph 2 of the present section. Unauthorised or incorrect use of an access card leads to immediate cancellation and withdrawal of the card, the legal consequences of which must be fully borne by the card holder. The head of the competent organisational unit is notified of the cancellation in writing by the Directorate of Asset and Institutional Security.

(5) The reactivation of a withdrawn or cancelled card is subject to an application signed by the head of the competent organisational unit.

(6) The Dispatch Service of the Department of Asset Protection must be promptly informed if an access card is lost, has been stolen or destroyed or if there is a technical failure. To facilitate the intended use, each user must ensure that the door closes fully after they pass through.

(7) The rules concerning the use of the University's card access control system are disseminated by the head of the Directorate of Asset and Institutional Security in a circular.

§ 10
Rules concerning the control of keys

(1) Building keys must be safeguarded in the designated locations, which are normally the 24-hour receptions.
(2) The head of the competent organisational unit must provide an up-to-date list of names of persons authorised to receive keys defined in paragraph (1) (adding the names of persons with extraordinary authorisation).
(3) Reception staff may only issue keys to persons on such list and must record each issue in the keys log.
(4) No keys for personal use may be issued for building entrances.

§ 11

(1) As a general rule, room keys must be kept at the reception or a designated location within a building. The head of each organisational unit must be informed if a different arrangement is in place.
(2) Keys to the following rooms may only be issued by the reception service of the building:
   a) rooms where hazardous substances (flammable, explosive, radioactive, harmful to health etc.) are used, stored;
   b) rooms where confidential or secret information (research, personal data) is processed, recorded; where high value technical equipment is used.

   As a general rule, the rooms in this section must have "duplication prohibited" or at least security keys and, as much as practicable, must be equipped with supplementary mechanical and/or electronic protection. These rooms must be locked at all times when unattended.
(3) The reception staff may only issue keys from the reception based on the authorisation list from the competent organisational unit and the written permission of the directorate of the Directorate of Asset and Institutional Security and such issue must be recorded in the keys log in the person's own hand. The reception staff must check the identity and authorisation of the person requesting a key.
(4) The return of keys must also be recorded with handwritten signature. In case a key is returned not by the authorised person, the reception staff must also check this person's identity and record such return in the reception log.
(5) Rules concerning the control of keys are included in Annex 5. The requirements of mechanical asset protection are included in Annex 6.

§ 12
The locking and unlocking of buildings and rooms

(1) Each lock, security equipment (where available) must be carefully lock or switched on by the last person exiting the building, room.
(2) If a room cannot be locked due to a technical failure, it must be reported to the Dispatch Service of the Department of Asset Protection.

(3) When leaving a room, the last person leaving must ensure that all doors and windows are closed, all electrical appliances are switched off. A switched on appliance may only be left unattended if it is absolutely necessary and it must be communicated to the competent manager.

(4) If unattended, offices and laboratories must be locked and no keys are allowed to be left in the locks even for a short time.

(5) If a key, access card is lost (missing), another staff member within the same organisational unit must be contacted and asked to lock the room, the Dispatch Service of the Department of Asset Protection must be informed and the suspension of the access card must be requested. The lock must be replaced at the earliest convenience and the other keys must be returned. The valuables within the room must be more tightly protected until the lock is replaced.

§ 13
Extraordinary opening hours

(1) Working and other activities (events etc.) outside the normal opening hours of the University's buildings must be communicated to the director of the Directorate of Asset and Institutional Security in writing, three working days in advance who will decide at their own discretion based on the request. If the activities, working to be carried out outside normal opening hours are different from the intended use of the building and applicant, the request must include an explanation.

(2) Access outside normal opening hours requiring reception service must be requested in writing from the Directorate of Asset and Institutional Security three working days prior to the requested date.

(3) No visitors and students are allowed to stay in the University's buildings outside normal opening hours unless watched by the reception service, the University's designated responsible staff member or security guards.

(4) Rules concerning the locking and unlocking of buildings and rooms are included in Annex 7.

§ 14

Entry of personal property on the University's premises, removal of university property from the University's premises

(1) No privately owned assets, equipment (property of other business entity) may enter the University's premises without the consent of the head of the competent organisational unit. The safety of these assets, equipment is the owner's responsibility, the University refuses to assume any financial liability.

(2) Weapons, firearms or their replicas are STRICTLY PROHIBITED on the University's premises either carried visibly or concealed (in a package, clothing etc.). If such devices are detected, the Dispatch Service and the head of the Department of Asset Protection must be promptly notified.

(3) The University does not assume any financial liability for any high value personal property (jewellery, cash etc.) and vehicles left in the parking lot or other external area.

(4) No physical assets owned by the University may be removed from the buildings without a properly issued and signed removal permit. (Annex 8). The removal permit and the physical asset must be presented at the reception for registration both in case of incoming and outgoing delivery. The reception staff must prevent the removal of the University's property from the University's premises without a removal permit.

(5) The head of the organisational unit approving the removal must ensure that the University's physical assets (regardless of the purpose of the external use such as working, lending etc.) are returned in a timely manner.

(6) Each organisational unit must check the availability of the physical assets on a regular basis as required by the University's applicable regulatory instruments (inventory policy, rules concerning physical asset records etc.).

§ 15

Storage of high-value assets

0. The doors and windows of rooms where technical equipment with a combined worth of over HUF 2 000 000 is located must be equipped with proper mechanical and/or electronic security equipment. (Annex 6)
0. No electronic security equipment will be installed without the consent of the director of the Directorate of Asset and Institutional Security.

§ 16
Cash storage, cashtransfer

(1) Rules concerning cash handling at the University are included in Chancellor's order No 15/2015 (05/10) on the Financial and Cash Handling Policy.

§ 17
The opening of locked rooms

(1) If there is necessity to open a room the user of which is not available, approval may only be given by a committee except in extraordinary situations.
(2) The action and the reason of the opening as well as what is found in the room must be documented. The above mentioned committee must include the head of the affected organisational unit and a representative of the security service as a minimum.

§ 18
Rules concerning the recording of photos and videos

(1) Except for celebrations and events specified in policies and regulations approved by the Senate or the Faculty Board, no photos, film, audio and video recording will be made in the facilities managed or rented by the University and published without permission, which will be issued by the Chancellor based on a prior written application and in agreement with the director of the Directorate of Asset and Institutional Security.

§ 19
Access of motor and other vehicles to university premises, traffic and parking rules

(1) Access to the University's northern campus is only allowed for the purpose of delivery of goods, parking in this area is prohibited. Exceptions include the vehicles of persons with a valid permit to access the car park near the Hőközpont (Heating Centre) building and persons with a disability certificate who are allowed to park their vehicles near the Könyvtár (Library) building.
(2) Car parks in the University's central campus, between buildings H and R,
in the courtyard between buildings V/1 and V/2 and in the underground car park of the IT building and building Q in the University's southern campus may be used by persons with a valid parking permit (subject to the payment of parking charges) exclusively on working days from 6 a.m. until 10 p.m. Car parks must be vacated until the closing of the gates, 10 p.m. at the latest. Car parks are closed on public holidays.
(3) Access to designated parking areas is subject to the availability of a parking permit and the use of an access card. Access cards must solely be used by their holders, they may not be passed on to others or used to allow the entry of other persons. Card users are responsible for full compliance with the Conditions of Use and any damage caused by incorrect use. Unauthorised or incorrect use of an access card leads to the cancellation of the card by the Directorate of Asset and Institutional Security, the legal consequences of which must be fully borne by the card holder. The head of the competent organisational unit is notified of the cancellation in

writing by the Directorate of Asset and Institutional Security. The reactivation of a withdrawn or cancelled card is subject to an application signed by the head of the competent organisational unit.

(4) When parking on the University's premises, the "Identification Card" must be placed visibly, behind the vehicle's windshield allowing the checking of validity. In case of an emergency (e.g. utility failure, fire etc.), owners are notified based on the contact telephone number on such card.

(5) No bicycles, mopeds etc. are allowed in the University's buildings. Furthermore, bicycles, mopeds etc. are not allowed to be locked to the University's fences, utility poles and other objects and trees owned by the University. Bicycles must exclusively be stored in designated open or closed bicycle storages while mopeds and motorcycles must be stored in designated parking areas. Traffic on the University's premises is subject to the effective traffic code.

(6) The closed bicycle storages are locked with high security padlocks to which personal keys are issued by the Directorate of Asset and Institutional Security

based on a written application and subject to charges determined by the director of the Asset and Institutional Security. Such keys may be requested on a continuous basis and the application must include the number of the bicycle storage. The key issued may only be used for the bicycle storage the number of which was specified in the application. The passing of such keys for use to another person is strictly prohibited.

(7) The application of employees must include the signature of the head of the competent organisational unit and identification data (name, master number, organisational unit, telephone number) while the application of students must include the student status certificate issued by the Central Student Office and identification data (name, Neptun code, faculty, year, telephone number). When the authorisation for use terminates, in case of the termination of the student or public servant status, or is cancelled, such keys must be returned to the Directorate of Asset and Institutional Security after which the charges are partly repaid as defined by the director of the Directorate of Asset and Institutional Security.

(8) If a key is lost, it must be reported to the Dispatch Service of the Department of Asset Protection to be followed by the replacement of the padlock and the keys as a whole, the costs of which must be paid by the holder of the lost key in their entirety.

(9) Vehicle access and its conditions, parking rules and charges as well as the conditions of use of closed bicycle storages on the University's premises (hereinafter: Conditions of Use) are determined by the director of the Directorate of Asset and Institutional Security in agreement with the Directorate of Operation and Maintenance and disseminated in a circular.

Chapter V

CLOSING PROVISIONS

§ 20

(1) This Policy enters into force on the day when it is signed.

(2) At the entry into force of this Policy, the University Order on Security issued on September 27 1989, Circular No. 100.968/1997 of the Director General and the Circular No. 22/2009 of the Director General (24/06) are repealed.

(3) To access and/or to download this Policy and its Annexes, please visit the website of the Chancellery: www.kancellaria.bme.hu

(4) This Policy is managed by of the Chancellery's Directorate of Asset and Institutional Security

Budapest, 18 December 2017

Gyula Barta-Eke, chancellor

ANNEXES

1. Annex 1: Key actions in response to a bomb threat
2. Annex 2: Actions in response to signs of illegal substance (drug) use
3. Annex 3: Rules concerning entering, exiting and staying on the University's premises on working days between 10 p.m. and 6 a.m. and on public holidays

4. Annex 4: Rules concerning security and asset protection applicable to tenants, operators and contractors situated or working at the Budapest University of Technology and Economics
5. Annex 5: Rules concerning the control of keys
6. Annex 6: Requirements concerning mechanical asset protection
7. Annex 7: Opening hours of university buildings
8. Annex 8: Rules concerning inward and outward movement of materials and equipment
9. Annex 9: Management of found property

Key actions in response to a bomb threat

§ 1
Bomb threat received by phone

(1) Most bomb threats are received by phone. As the only point of contact in such cases is the person operating the phone, everybody must be aware of how to behave when such a call is received.

(2) Experience shows that callers try to end the call as quickly as possible except when they become confused about the identity of the target.

(3) Take the following actions when a bomb threat is received:
   a) if the phone has a display (digital telephones), copy the number of the caller.
   b) if available, immediately turn on any audio recorder.
   c) listen to the caller very carefully to be able to identify as many sounds, background and other noises as possible.
   d) try to repeat back the caller's data in a different, incorrect way in order to keep them on the phone as long as possible.
   e) say that you are not the competent person and try to redirect the call to another extension: (Department of Asset Protection phone number: 37-63 or 11-07) during normal business hours, the Dispatch Service (phone number: 44-44) outside normal business hours.
   f) if possible, try to ask specific questions (e.g. What type of bomb is it again? Who are you? Are you calling from out of town? etc.)

(4) The start and end time as well as the words of the bomb threat call must be recorded in writing immediately if that is the only possible option.

(5) The following should be preferably recorded in writing:
   a) the language used by the caller (it can be a foreign language);
   b) any dialect, accent;
   c) any incorrect language use;
   d) the caller's sex;
   e) the caller's estimated age;
   f) the caller's style of speech (fast, slow, distorted etc.);
   g) vocabulary reflecting the caller's qualification level;
   h) background noises.

§ 2

(1) After the call, promptly notify the Department of Asset Protection on extensions 37-63 and 11-07 during normal business hours and the Dispatch Service of the Department of Asset Protection on extension 44-44 outside normal business hours and the police every time calling 112.

§ 3

(1) The following practical measures are recommended:

   a) determine a meeting point with the police;
   b) complete the evacuation ordered by the police in a disciplined manner involving the Asset Protection Service and the available staff of the operation unit;

c) switch off all electric appliances (including elevators) as well as gas operated equipment; It is best to switch them off with the electrical service panel and main switchboard;
d) to reduce any potential detonation wave, the doors and windows should be opened;
e) closed cabinet doors and drawers, especially in rooms not in use at the time of the alarm signal, must not be opened;
f) "wireless telecommunication devices" (e.g. mobile phones, two-way radios etc.) should be switched off due to the potential use of a remotely controlled triggering device;
g) any persons carrying a portable radio or similar device walking inside or around the building evidently without an aim must be closely watched and reported to the police or the Asset Protection Service.

§ 4
Evacuation rules

(1) The evacuation of the building must not be subject to any considerations, it must be completed without delay taking into account Act XXXIV of 1994 on the Police stipulating that the police must order evacuation in such cases and any acts to prevent it are deemed a criminal offence.
(2) Rules to follow when evacuating a building:
a) Every person must leave the building through the main or the emergency exit in a calm and orderly manner. Walking is recommended, running may cause panic, injuries and accidents.
b) Persons must go to a designated assembly area after the evacuation.
c) The use of elevators is strictly prohibited.

§ 5

(1) Records of any incident occurring (bomb threat etc.) must be subsequently sent to the Directorate of Asset and Institutional Security.

§ 6

(1) Persons authorised to respond in such situations are required to
a) quickly inform affected persons.
b) provide short, simple, clear and few instructions.
c) ensure that people remain calm and to prevent a panic.

Annex 2

Actions in response to signs of illegal substance (drug) use

§ 1

(1) While working, anybody, cleaning, reception staff, security guards and staff working at events in particular, may detect the signs of drug use, consumption and substance residues. In general, these signs are found in washrooms and toilets as well as rarely used rooms and during and after events: their colour may be white, black or a brown shade while their texture may be fine powder, crystal grits, tarry sticky mass, cake like material or tobacco or tea grass like substance.

(2) Signs based on the manner of consumption:
   a) scattered tablets or capsules;
   b) injection needles;
   c) empty vials;
   d) tin foil folded into tub shape;
   e) cigarette butts without filter;
   f) substance residues with the above mentioned

   colours and textures scattered around.

(3) LSD in the form of blotter paper, lollipops and candy and amphetamine derivatives (SPEED, EXTASY, GHB, MDMA, XTC in the form of the so-called accelerator tablet, powder or liquid).

(4) The following substances need special attention: SPEED, EXTASY, GHB, MDMA, XTC etc.

(5) If a person selling or disseminating the above mentioned substances is detected,
   a) the Department of Asset Protection and
   b) the police

   must be notified without delay.

(6) Such notification is preferably made in a manner to ensure that such person does not notice being detected and does not escape.

Annex 3

Rules concerning entering, exiting and staying on the University's premises

§ 1

(1) In order to prevent unauthorised access between 10 p.m. and 6 a.m. on working days and on public holidays, the reception service working together with the security service may only allow people to enter who have proof, based on the access permit provided by the head of the organisational unit and signed by the director of the Directorate of Asset and Institutional Security, to demonstrate that they work at the University.

(2) Permits to access the University's premises outside normal business hours by external contractors working on the University's premises and by tenants working based on a lease agreement must be requested from the organisational unit ordering the services and directly from the Department of Operation respectively.

(3) In absence of such permits, university staff and students are not allowed to stay on the University's premises and inside its buildings and to assist unauthorised persons in accessing these areas.

(4) To enter:
   a) buildings with 24 hour, continuous reception service: use the reception services of the Central Building, Building E, the IT Building,
   and Buildings Q and Z;
   b) buildings with no reception service, use one of the following reception services:
      ba) to enter the Library Building and Buildings CH, F, Fa, L, Mg, MM, Mt, AE and ÉL, use the main reception at the Central Building (telephone: 10-00),
      bb) to enter Buildings R, T, H, D, J, St, G, A and V1, use the reception of Building E (telephone: 14-00).

(5) Buildings without a reception service may be entered with the assistance of the security guards after filling in the data in the log maintained by the reception service.

(6) The following buildings have entrances equipped with an access control system: Central Building, Buildings E, A
CH, F, ÉL, R, T, H, D, J, St, I, Q and Z.

(7) To exit:
   a) if you want to leave buildings without a reception service, call the Dispatch Service (telephone: 44-04) and security guards will be dispatched to open the door of the building.
   b) the time of exit must be recorded and signed in the log maintained by the reception service.

(8) Automated teller machines (in Buildings A and K) may be used without an access permit.

Annex 4

Rules concerning security and asset protection applicable to tenants, operators and contractors situated or working at the Budapest University of Technology and Economics

§ 1

(1) Prior to the commencement of their activities, contractors must contact the janitor of the building responsible for the area and provide information on the works, activities planned to be carried out in the area.

(2) Prior to the commencement of the work, a photocopy of the liability insurance policy must be made at the Department of Investment Planning.

(3) Contractors must protect their own physical assets and have them insured if necessary. The University cannot accept any liability for the physical assets and equipment of contractors.

(4) Contractors must protect the work area and rooms they use and lock them up at the end of the day recording it in the lock log.

(5) If a contractor wants to leave a key at the university reception service, the Department of Asset Protection must be notified first and then the key will be placed in a sealed key box. This key box must indicate the name of the locked building, the floor, the door number, the company name, its authorised senior official, the name of persons authorised to receive the key, address and telephone number where they can be contacted outside normal business hours and identity card number. The key box may only be issued to persons in the key issue log and must be recorded in there with the person's signature.

(6) Contractors must accept liability for the activities of persons employed by them. In this context, they must compensate the University for damage caused by them or a third person in the course of their activities.

(7) When moving materials and goods, contractors must complete the required documents and provide one copy to the reception service. If such documents are lacking, the entry or the exit may be denied. Trucks belonging to the contractors may only be located on the University's premises for the purpose of loading and delivery for up to an hour. Access permits are issued at the freight entrances in exchange for the truck's registration certificate. No entry or parking of passenger cars belonging to the contractors is allowed on the University's premises.

(8) Access outside normal business hours and on public holidays is authorised by the Directorate of Asset and Institutional Security based on the contractor's written request. The request for access must be submitted to the University's contracting organisational unit two working days prior to the requested date of access. The same procedure is applicable in the case of gates and doors equipped with an access control system. In such cases, access cards must be provided by the University's contracting party.

(9) Traffic on the University's premises is subject to the traffic code with the maximum speed limit of 5 km/h on the northern campus and 10 km/h on the central campus.

(10) Any incidents on the area used by contractors or taking place during their work activities must be investigated by the affected contractor and must be reported to the Directorate of Asset and Institutional Security. Building K, floor 3, telephone: 463-1107, 463-3763, in case of fire: 463-1105, 463-2990).

(11) Contractors must agree that:

a) the Department of Asset Protection of the Directorate of Asset and Institutional Security is authorised to carry out activities related to asset protection and to monitor compliance with asset protection and security rules on the University's premises.

b) If there is strong suspicion that an employee of a contractor is attempting to remove physical assets owned by the University from the University's premises, a person designated by the Department of Asset Protection is authorised

to search the suspected employee’s bags and vehicle and to take the necessary actions.

- Contractors must accept liability for any damage arising from the breach of this Policy even if it was not caused by their own employee but another person visiting the contractor for any other purpose.
- Contractors must ensure that their employees are familiar and comply with this Policy.
- The security organisation of the Budapest University of Technology and Economics:
  aa) the Chancellery, the Directorate of Asset and Institutional Security, the Department of Asset Protection ad) Budapest-1111, 3 Műegyetem rkp. Building K, floor 3, room 81.
  ae) Telephone: 463-1107-463-3763.

Rules concerning the control of keys

§ 1

(1) These rules are intended to ensure that no keys are issued to unauthorised persons and to be able to monitor which persons used the keys to each room and when. The reception service may only receive keys in key boxes with special identification seals used specifically for this purpose.

(2) Key boxes may only be returned to 24-hour receptions (Central Building, Building E, the IT Building, Building Q and Z) and on working days, in two shifts (from 6 a.m. to 10 p.m.) to Buildings A, CH and R, the reception services at the gate in Bertalan Lajos street. If the organisational unit wants to use the spare key on public holidays, the key box must be left at a 24-hour reception on the last working day or a spare key box must be made available at a 24-hour reception on a permanent basis. (No key box may be picked up at a non-functioning reception.)

(3) The head of the organisational unit must record in writing that the organisational unit makes available a spare key and the names of the persons authorised to receive such key. The list of authorised persons (including their ID numbers) must be sent to the Directorate of Asset and Institutional Security enclosing the authenticated key issue log.

(4) Keys to persons not included in the above mentioned list may only be issued by the reception in case of emergencies (fire, natural disaster, major operational failures etc.) and such issues must be recorded every time. The key box may only be received by the reception service if it has been relocked with the special identification seal.

(5) The head of the organisational unit determines the rules concerning the control of keys in their area of competence based on the following criteria:
   a) Used keys must be numbered and registered.
   b) The use of duplicated, not numbered keys is prohibited.
   c) Persons holding keys must sign a written statement that if the key is lost, they will bear the costs of the replacement of the lock.
   d) The availability of the keys must be checked on a regular basis.
   e) When the employment, student or other legal status ends, keys must be returned.
   f) Keys stored by organisational units must be kept in safe key cases to prevent unauthorised access.

§ 2

(1) The traditional cylinders that are widely used across the University including magnetic cylinders fail to meet the required level of safety. Rooms where high-value assets are kept must be equipped with certified safety locking systems. If a room is equipped with (an electronic) system that provides higher security, the locks do not have to be replaced.

(2) The above mentioned criteria must be met to ensure that if rooms where high-value assets are located are affected by burglary or theft committed using the room’s own key, the liability of the employees of the organisational unit may not be disputed.

(3) If you have questions about the control of keys, please contact the staff of the Department of Asset Protection (telephone: 37-63, 11-07).

Requirements concerning mechanical asset protection

§ 1

(1) Requirements concerning mechanical asset protection:
- a) windows located below 2 m must be equipped with grilles;
- b) door casings must be affixed to the wall in at least 3 places, in proportion with the height of the casing in order to prevent illegal forced entry;
- c) door panels must be safe from illegal removal, prying and latch manipulation;
- d) at least 2 security locks must be installed;
- e) doors must be affixed to their casings using at least 3 hinges;
- f) warping of the door or its casing may not compromise the locking;
- g) bolts must extend at least 18 mm into the strike plates;
- h) the permitted gap between the door panel and the casing is up to 5 mm;
- i) in case of an inside lock, the external, narrower side of the door panel must be secured with a metal plate;
- j) in case of wooden casings, reinforced strike plates must be provided;
- k) the stability of walls, slabs and floors must equal the stability of at least 12 cm thick traditional solid brick walls;
- l) instead of door reinforcement, grills may be installed in front of the doors;
- m) when refurbishment works are carried out, doors leading to public places must be equipped with cylinders where the duplication of keys is only allowed with a code card.

§ 2

(1) Security locks have the following features:
- a) additional locking;
- b) cylinder locks with at least 5 pins;
- c) magnetic locks with at least 6 armature plates;
- d) suvald locks, combination locks with numbers or letters where there must be more than 10 000 variations; and
- e) individually certified lamella locks.

(2) Criteria for security grilles:
- a) the division of the entire grille surface is at least 100 x 300 mm, i.e. the removal of one thread does not allow intrusion.
- b) they are made from welded round steel with a diameter of 12 (e.g. A34) or other material of equivalent stability.
- c) the instalment depth is at least 150 mm and they must be affixed to the wall with at least 4 mounting claws by every 300 mm along the vertical and horizontal threads.

(3) Criteria for armoured safes:
- a) metal coating, double walls (with concrete or aggregate material between the two layers) and
- b) double key locks or
- c) one key lock and one combination lock,
- d) permitted locking gap is up to 2 mm.

Metal cabinets of different parameters are considered as reinforced safes.

Annex 7

Opening hours of university buildings

§ 1

(1) Continuous reception service (24 hours), supervised by the Directorate of Asset and Institutional Security, is available at the Central Building, the IT Building and Buildings E, Q and Z.

(2) The following receptions work in two shifts (from 6 a.m. to 10 p.m.) on working days:
   a) Buildings A, CH and R,
   b) gated vehicle entrance at 7 Bertalan Lajos street,
   c) gated vehicle entrance at 4 Stoczek street.

(3) The reception service in Buildings D and J is managed by the competent faculty or department.

(4) Buildings without a reception service and with a card access control system are open from 6 a.m. until 10 p.m. on working days unless the head of the organisational unit located in the building otherwise specifies.

(5) The opening hours of buildings without a card access control system are specified by the head of the organisational unit located in the building.

(6) The director of the Directorate of Asset and Institutional Security is authorised to make any changes in the opening hours of buildings and gates.

Annex 8

Rules concerning inward and outward movement of physical assets

§ 1

(1) Removal of any physical assets managed by the University from the University's premises is only allowed in strongly justified cases and in compliance with any applicable laws and regulations as well as the provisions of the Security and Asset Protection Policy.
(2) Items listed in paragraph 1 may only be lent with the written permission of the head of the organisational unit.
(3) Such permit must be issued in three copies. The first and second copy is retained by the applicant and the organisational unit respectively. The third copy must be handed to the reception service when the item lent is removed.
(4) The permit template is available for download at the Chancellery's website.
(5) The permit must include information to identify the item (name, type, serial number) and the date of return.
(6) Lending operations (justification, compliance with agreed dates, any cost reimbursement, technical condition) are supervised by staff designated by the head of the organisational unit.
(7) Record-keeping requirements for lending operations must be fully met.
(8) In case of inward deliveries to the University's premises, delivery notes or invoices must be presented to the reception service. In absence of the above mentioned documents, access may be denied.

Annex 9

Management of found property

§ 1

(1) Property found on the University's premises must be handed in to the Dispatch Service of the Department of Asset Protection or the reception of the nearest building.
(2) When found property is handed in, it is recorded and the found items must be delivered to the Dispatch Service within 8 hours where they are registered in a dedicated log and stored in a cabinet.
(3) Found property must be claimed by their owner in person or through a representative (holding an authorisation) subject to the presentation of some form of identification and signing the delivery record.
(4) If found property is left unclaimed for 3 months and the identity of the owner is unknown, it will be disposed of in accordance with the provisions of Act V of 2013 on the Civil Code.
(5) Any personal documents found must be handed in the competent office of personal documents.