R e c t o r
of the Matej Bel University in Banská Bystrica
Národná 12, 974 01 Banská Bystrica
doc. Ing. Vladimír Hiadlovský, CSc.

Statement on the guarantee of sufficient security related to personal data which undergoes processing in accordance with the GDPR requirements, by introducing a security policy

The Matej Bel University administration ("hereinafter MBU") declares the following **strategic security objectives** for the purposes of the security policy:

1. Build and sustainably maintain high level protection and security of information systems with personal data, mainly in accordance with the Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR"), Law No 18/2018 Coll. on the protection of personal data, with Law No 275/2006 Coll. on information systems of public administrations and on the change and amendment of certain laws as amended, by the Notice of the Ministry of Finance of the Slovak republic No 55/2014 Coll. on standards for information systems of public administrations as amended.
2. Create conditions and implement safe placement of the most important components and sustainably ensure technological and regime protection.
3. Procure and implement information systems of only high quality, professional level and utility which will create and protect the good reputation of the MBU.
4. Apply the property principle during the development of the security system.
5. Protect personal data and rights of data subjects.
6. Ensure the necessary protection of MBU property.
7. Introduce a system which shall control work performance and the compliance with rules of all departments, divisions as well as employees themselves, in order to reveal low-quality, unprofessional or other work performance incompatible with university interests.
8. Create emergency plans and MBU information system functionality restoring plans.
9. Create and maintain a functional security structure which shall guarantee achieving and maintaining a laid down target security level in all requested areas.
10. Introduce and constantly provide a report system on the status of the security system and reports on security incidents.

MBU shall adopt appropriate technical and organisational measures in order to ensure processing of personal data **in accordance with the GDPR**. The following principles and objectives shall apply to security measure suggestions intended to protect key activities and their implementation into existing systems and technological chains:

1. <u>The protection of important systems and information system components principle</u>
   Important systems and information system components are elements the failure, destruction or any other reason for unavailability, of which would affect strategic interests of the MBU. The objective is to minimise the default risk of important elements of MBU information systems, communication and security infrastructure.

2. <u>The data protection in accordance with the GDPR principle</u>
   The data shall be protected in all forms – voice, written and electronic, in the course of processing and transfer by means of computers, phones or computer networks and as long as they are archived. The objective is to achieve an economically adequate and at the same time reliable protection of personal and economic data, student and MBU employee data. In order to achieve this objective, the security management, which consists of data protection officers entrusted with the supervision of the protection of personal data, security managers and asset

managers, was introduced. The adopted and implemented measures to ensure the protection of personal data are described in the MBU Security Project which was updated under the GDPR regulations.

3. The protection of individual and personal security principle

   MBU employees and employees of MBU business partners, who are on its premises with its consent, are considered subjects. MBU wants and shall protect the rights of subjects whose data is undergoing processing. For these purposes, it shall adopt measures to protect processed personal data against unauthorised activities of unauthorised persons and measures to ensure adherence to the rights of data subjects whose data it is processing. The MBU is interested in stabilising key employees, primarily those who are involved in the development and operation of information technologies, which support its strategic interests.

4. The protection of tangible property and financial funds principle

   The MBU property represents a significant value, therefore, it is necessary to ensure that these values are treated in a manner that shall prevent their damage, failure or other loss.

5. The protection of good reputation principle
   Appropriate attention is focused on the protection of the good reputation of the MBU. The objective is to maintain and improve the good reputation.

6. The assignment of safety responsibility principle
   The protection of MBU assets is based on the property principle (asset manager, authorised person). Property shall, in this case, have the meaning of an information, data, precisely defined set of data or other asset assigned to an employee, who shall have a personal interest in their protection. Each "owner" of the asset has defined rights and obligations which enable him or her to ensure a reliable protection of data and assets "assigned" to him or her.

7. The reporting of the security system status principle
   The MBU administration and employees shall be prepared to react appropriately to an emergency in order to minimise its consequences. The activity of the security system and information system users is monitored, security incidents are observed and regularly evaluated. Appropriate measures, in accordance with the existing legislation, shall be introduced against security system intruders.

8. The security system implementation process principle
   The security system shall be implemented on the basis of elaborated principles in a manner which respects the options and needs of the MBU. Security mechanisms which are or will be implemented in the MBU environment shall have the security level that complies with legislation requirements, primarily in the area of personal data protection, intellectual property protection and standards for information system security.

This Statement is a public document and a document of the MBU security policy within the meaning of the MBU Security Project for the protection of personal data.

Banská Bystrica 25. 5. 2018.

doc. Ing. Vladimír Hiadlovský
rektor UMB