Security of Employee User Accounts by Multi-Factor Authentication

Article 1

Introductory provisions

1) The Rector of the University of Hradec Králové (hereinafter referred to as the *"University"*) issues this Rector's Decree in order to increase the security of the University's information systems for the following reasons:

   a) In its activities within the scope of its competences in the area of public administration, the University is a public authority to which the provisions of Act No. 181/2014 Sb., on cybersecurity and on amendments to related acts (the Cybersecurity Act), as amended, and its implementing regulations apply.

   b) As part of its preventive measures, the National Cyber and Information Security Agency (hereinafter referred to as the *"NCISA"*) has issued a warning in connection with the critical threat of cyber espionage and other cyber attacks, urging organizations in accordance with the Cybersecurity Act, to be vigilant against the most commonly used attack techniques and to update information systems and their components to avoid exploiting known vulnerabilities.

   c) The assessment of cyber incidents published by the NCISA on its website mentions the growing trend of threats in the area of *phishing*, *spear-phishing* and social engineering with subsequent compromise of user accounts. Threats are also regularly detected by automated systems for checking incoming mail communications within the university infrastructure. The introduction of multi-factor authentication reduces the risks of misuse of user accounts and mailboxes.

   d) Following the recommendation of the Cybersecurity Committee, the University management has entrusted the Head of the Department of Information Technology Services (hereinafter referred to as DITS) with the coordination of increasing the security of the University's information systems by gradually deploying multi-factor authentication (hereinafter referred to as the *"MFA"*) for secure login.

Article 2

Schedule of MFA deployment

1) By this Decree, the Rector instructs the University units to:

   a) Determine, within 60 days of the entry into force of this measure, the method of security for each employee within the meaning of Article 3(1) of this Decree and forward the information as indicated to:

      uhk.cz/m365-mfa-form;

   b) Ensure, no later than May 1, 2025, that employees have the security method established under paragraph (a) of this Article registered in the Microsoft 365 portal according to the instructions available at:

      uhk.cz/m365-mfa.

   c) If the multi-factor authentication is not required for a specific employee for objective reasons (a person who does not have a computer network account, access to the mailbox, access to other University information systems, or a person with a serious health disability), this information should be forwarded to the head of the DITS. Legitimate exception requests will be reviewed by the Cybersecurity Committee which may request additional information.

2) The Rector instructs the Bursar and the Vice-Rector for Strategy, Development and Digitalization to ensure that the Head of the Human Resources and Payroll Office, in collaboration with the Head of the DITS, proposes and implements changes to documents and procedures relating to the creation and termination of employment no later than 1 March 2025 to include the setting up of the MFA method and the administration of security tokens provided in the University's standard processes.

3) The Rector further instructs the Head of the DITS to determine the hardware needs and prepare a schedule for the MFA deployment at individual faculties and University and Rectorate departments (hereinafter referred to as the *"Schedule"*) based on the data obtained pursuant to paragraph 1 of this Article. On the basis of the Schedule, the Rector directs the DITS to take the necessary steps for its implementation.

4) All procedures and details related to this Decree will be available on the University's website at:

   uhk.cz/m365-mfa

Article 3

Method of MFA implementation

1) The multi-factor authentication will be implemented at the University using one of the methods listed above:
   a) By using an authentication application installed on smartphones; or
   b) By using a physical device for electronic authentication of the user's identity (a security token);
   c) By sending SMS confirmation codes (recommended only as a backup method).
2) Employees may register multi-factor authentication methods under paragraph 1(a) or (b) by following the detailed instructions available at:

   uhk.cz/m365-mfa-navod.
3) Employees will be allowed to use multi-factor authentication via both business and private telephone as referred to in paragraph 1(a) or (c) of this Article, or a security token as referred to in paragraph 1(b) of this Article.
4) Technical requirements and support for the MFA are provided by the DITS staff. Employees can contact the end-user support staff via the helpdesk web application (helpdesk-cit.uhk.cz), e-mail (helpdesk-oit@uhk.cz), or in person.
5) The standard process for the acquisition and management of the University-owned security tokens under paragraph 1(b) of this Article shall be provided by the DITS. A request for a security token shall be made by the relevant senior member of staff via a binding purchase order registered in the Magion EIS. Information on recommended tokens and contact details for the vendor can be found at:

   uhk.cz/m365-mfa.
6) The costs associated with the acquisition of a security token or a business telephone shall be borne by the department at which the employee is employed.

Article 4

Final provisions

This Decree shall enter into force on the date of the Rector's signature and shall take effect on 1 March 2025.

In Hradec Králové on 04. 03. 2025

Assoc. prof. RNDr. Jan Kříž, Ph.D.
Rector