Zabezpečení kybernetické bezpečnosti

Kód:	FSv_PD_2023_05_V01
Druh:	Příkaz děkana
Č. j.:	CVUT00021748/2023
Oblast normy:	ISMS
Organizační závaznost:	FSv
Garant:	11375 vedoucí VIC Ing. Tomáš Líbenek
Vydavatel:	prof. Ing. Jiří Máca, CSc. děkan
Počet stran:	5
Počet příloh:	0
Rozdělovník:	Martina Vavřinová (B-11000-DEKAN-SEKRETARKA)
Dotčené osoby:	všichni (B-11000-SUMA-OSOBA-CVUT)
Forma zveřejnění:	intranet
Nahrazuje:	Opatření děkana č. 12/2022
Datum vydání:	04.12.2023
Účinnost:	04.12.2023 – do zrušení
Platnost:	04.12.2023 – do zrušení
Další informace:	
Podpis vydavatele:	v.r. prof. Ing. Jiří Máca, CSc. děkan fakulty

Přehled změn

Nejsou.

Seznam příloh

Nejsou.

Seznam souvisejících dokumentů

Nejsou.

Pursuant to Art. 18 par. 4 of the Statute of the Faculty of Civil Engineering of the Czech Technical University in Prague, I hereby issue the following Order:

Článek 1
Basic provisions

This order directs all FCE departments and workplaces to adopt and implement organisational and technical measures to minimize cyber threats and the occurrence of a cyber incident in the communication and information infrastructure of FCE or CTU in Prague.

Článek 2
Organisational measures

2.1 The devices connected to the FCE fixed-line data network will be centrally registered in the Information Systems operated by the FCE Computing and Information Centre (hereinafter referred to as "FCE CIC") (hereinafter referred to as "FCE CIC IS"). The device will be registered with its network identifiers, device type, operating system, inventory number, location, organisational unit and a responsible person with a valid relationship to FCE.

2.2 FCE CIC will periodically inform the responsible persons and the secretariats of FCE departments and workplaces about detected discrepancies in FCE CIC IS with a call for their correction.

2.3 The responsible person is mainly accountable for:

a) maintaining up-to-date information in FCE CIC IS,
b) application of this instruction in all devices entrusted to them,
c) ensuring that all available steps are taken to eliminate vulnerabilities on the entrusted devices and the software installed in them.

2.4 Periodic training of the Faculty staff and partners in cyber security topics will be conducted in two stages:

a) face-to-face training, intended for the management and managerial staff of the Faculty, Departments and Centres, as well as the departmental staff members and grant researchers relevant in terms of cyber security,
b) on-line training intended for all the other employees and selected Faculty partners.

The assignment to the above groups is at the Faculty Treasurer´ s discretion.

2.5 FCE CIC operates a website on the FCE Web Portal to summarise and explain in more detail the Faculty cyber security measures, where relevant.

Článek 3
Technical measures

3.1 The devices not supported by the manufacturer, or the software not supported by the manufacturer installed in these devices are not allowed to be operated in the FCE data network.

3.2 The devices from the manufacturers that the National Cyber and Information Security Agency has warned against are not allowed to be acquired and operated in the FCE data network.

3.3 A centrally operated and monitored FCE CIC security solution must be installed in all devices connected to the FCE data network.

3.4 The so-called temporary access to the FCE data network (WG server) is not supported. All computers that access the FCE data network via a fixed connection must be registered in FCE CIC IS.

3.5 All inbound traffic from data networks outside FCE is blocked on the devices in the FCE fixed-line data network. Outbound traffic remains unchanged.

3.6 Only a remote access VPN operated by CTU or FCE is possible on the devices in the FCE data network. Only Remote Desktop can be used for access on the devices with the MS Windows operating system, and the SSH protocol for the Linux operating system. All other methods (TeamViewer, VNC, etc.) are prohibited and blocked.

3.7 The servers managed by departments must be marked as servers in the FCE CIC IS records, connected via a dedicated address space and must have EDR software installed in them, managed and monitored by FCE CIC or CTU CIC.

3.8 Local data arrays (NAS) managed by departments must be marked as NAS in the FCE CIC IS records, must be connected via a dedicated address space and must follow the security policy defined for them.

3.9 The employees who use the Thin Client virtualization platform for their work must use it exclusively, including for working from home. They are not allowed to copy their work-related data to other, private or business devices or install software required for their work in them. All activity shall take place in a virtual environment using a remote connection.

3.10 FCE CIC is authorized to disconnect from the data network the device:

a) whose responsible person does not respond to calls from FCE CIC,
b) for which the responsible person is not known or has terminated his/her relationship with FCE,
c) where a serious security threat has been identified, the responsible person of the respective device has been informed of the situation, together with a proposal for a solution,
d) which does not comply with the requirements of this instruction and has not been granted an exemption.

3.11 Exemptions from technical measures No. 3.1, 3.2, 3.3 and 3.5 are possible. These exemptions are recorded in FCE CIC IS and approved by FCE CIC authorized representatives. The purpose of the exemptions is, above all, to allow the operation of publicly operated services (web servers, etc.), to allow the operation of devices that provide a unique service or that cannot be brought into compliance with the measures for technical reasons, but whose utility value outweighs the risk arising from their use. The exemption cannot be granted without taking technical measures to reduce this risk.

Článek 4
Final provisions

4.1 This Order replaces the Dean´ s Measure No. 12/2022.

4.2 The measures taken to bring the status quo into compliance with this Order will be implemented without delay but will be phased and will take place under the FCE CIC´ s responsibility.

4.3 The implementation status of the measures will be assessed no later than in June 2024.

4.4 This Order comes into force on 4. 12. 2023.

prof. Ing. Jiří Máca, CSc.
Faculty Dean