

Opatření rektora č. 44/2021

Název:	Zajišťování kybernetické bezpečnosti na Univerzitě Karlově
K provedení:	-
Gestor:	Bezpečnostní odbor, Ústav výpočetní techniky
Účinnost:	15. listopadu 2021
	[zrušeno OR č. 35/2024]

Zajišťování kybernetické bezpečnosti na Univerzitě Karlově

Čl. 1 - Úvodní ustanovení

- Cílem tohoto opatření je nastavení vnitřních procesů na Univerzitě Karlově (dále jen „univerzita“) za účelem zajišťování kybernetické bezpečnosti (dále jen „KB“).
- Univerzita tímto opatřením provádí požadavky v oblasti KB vyplývající z obecně závazných právních předpisů¹.

Čl. 2 - Personální zajištění oblasti KB

Za účelem zajišťování KB na univerzitě se zřizují:

- výbor pro řízení kybernetické bezpečnosti na univerzitě (dále jen „výbor KB“) a
- pozice manažera kybernetické bezpečnosti univerzity (dále jen „manažer KB“).

Výbor KB

Čl. 3 - Účel zřízení výboru KB

Výbor KB je zřízen k zajištění řízení kybernetické bezpečnosti ve smyslu zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů.

Čl. 4 - Činnost výboru KB

- Výbor KB zejména:
 - stanovuje cíle a strategii KB univerzity a koordinuje přípravu, implementaci a rozvoj jednotného Systému řízení bezpečnosti informací univerzity v oblasti KB (dále jen „SŘBI“),
 - projednává a doporučuje ke schválení rektorem koncepci bezpečnostní politiky a další dokumentaci v oblasti KB a kontroluje její implementaci v rámci univerzity,
 - pomáhá vytvářet koncept KB,
 - vyjadřuje se k návrhům a implementaci bezpečnostních procesů,
 - podílí se na hodnocení účinnosti bezpečnostních opatření, jejich důsledků i vhodnosti, jakož i na identifikaci jim odpovídajících alternativ vhodných pro univerzitu,
 - projednává zprávy z auditů, vydané a schválené auditorem KB univerzity,
 - informuje vedení univerzity o opatřeních v oblasti KB.
- Výbor KB dále projednává a předkládá rektorovi:
 - posouzení přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika,
 - návrhy rozpočtu na opatření pro oblast KB,
 - návrhy na stanovení pořadí důležitosti realizace jednotlivých bezpečnostních opatření a bezpečnostních projektů navržených manažerem KB.
- Výbor KB projednává a předkládá rektorovi závaznou bezpečnostní dokumentaci v oblasti KB, a to zejména:

¹ Zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

- a. organizaci a související dokumentaci SŘBI,
 - b. seznam informačních a komunikačních systémů zahrnutých do rozsahu SŘBI,
 - c. zprávy z přezkoumání SŘBI,
 - d. prohlášení o aplikovatelnosti SŘBI.
4. O své činnosti výbor KB předkládá rektorovi informativní zprávu nejméně jednou ročně. V případě identifikace kybernetického bezpečnostního incidentu podá rektorovi zprávu manažer KB.
 5. V oblasti ochrany osobních údajů výbor KB spolupracuje s pověřencem pro ochranu osobních údajů a projednává zprávy z auditu vydané a schválené auditorem pro ochranu osobních údajů a zprávy z testování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Čl. 5 - Složení výboru KB

1. Výbor KB má nejméně 3 členy, které jmenuje a odvolává rektor.
2. Členy výboru KB jsou minimálně:
 - a. prorektor pro IT nebo člen kolegia rektora zodpovědný za oblast KB – předseda výboru KB,
 - b. manažer KB – v případě, že je tato funkce vykonávána právnickou osobou, zastupuje tuto osobu ve výboru KB jím zmocněná fyzická osoba nebo člen jejího statutárního orgánu,
 - c. vedoucí nebo člen bezpečnostního týmu CSIRT-CUNI počítačové sítě univerzity.
3. Výbor může na své schůzi zvat další relevantní osoby.

Čl. 6 - Práva a povinnosti členů výboru KB

1. Členové výboru KB mají právo podílet se aktivně na činnosti výboru KB, vznášet dotazy, náměty, připomínky k projednávaným zprávám a návrhům, uplatňovat svá stanoviska k řešení problémů.
2. Členové výboru KB jsou povinni účastnit se jeho schůzí a plnit úkoly, kterými je výbor KB pověřil.
3. Předseda výboru KB zejména:
 - a. řídí a organizuje činnost výboru KB,
 - b. vydává stanoviska, doporučení a další dokumenty výboru KB,
 - c. ukládá, na základě rozhodnutí výboru KB, úkoly v oblasti KB a koordinuje jejich plnění s cílem dosažení souladu informačních a komunikačních systémů univerzity s požadavky právních předpisů a interními normativními akty.
 - d. na základě jednání výboru KB předkládá rektorovi schválené návrhy dokumentů, či požadavků na uskutečnění výdajů z finančních zdrojů univerzity na zabezpečení nutné míry KB.
4. V nepřítomnosti předsedy výboru KB plní jeho úkoly jím určený jiný člen výboru KB.
5. Chod výboru KB zajišťuje po administrativní a organizační stránce Ústav výpočetní techniky univerzity.
6. Schůze výboru KB jsou svolávány podle potřeby, nejméně však jednou za 6 měsíců.
7. Výbor KB může usnesením přijmout Jednací řád výboru KB univerzity.

Manažer KB

Čl. 7

1. Činnost Manažera KB může být vykonávána zaměstnancem univerzity, případně zajišťována prostřednictvím externího subjektu – právnické nebo podnikající fyzické osoby.
2. Manažer KB je přímo podřízen rektorovi a je vždy členem výboru KB. V rámci organizační struktury rektorátu je zařazen v kanceláři rektora.
3. Manažer KB je pověřen komunikací s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“), včetně případů řešení kybernetických bezpečnostních událostí a incidentů.
4. Manažer KB zejména:
 - a. odpovídá za plánování a řízení realizace kybernetických bezpečnostních projektů schválených výborem KB tak, aby informační a komunikační infrastruktura univerzity poskytovala služby v této oblasti v souladu s právní úpravou v oblasti KB,
 - b. odpovídá za vytvoření a chod SŘBI, včetně průběžného testování prevence až po eliminaci následků a vyhodnocení kybernetických incidentů na univerzitě,
 - c. odpovídá za zajištění schopnosti univerzity implementovat opatření ukládaná kybernetickým zákonem,
 - d. průběžně analyzuje vývoj SŘBI a vyhodnocuje identifikovaná kybernetická rizika, detekované kybernetické bezpečnostní události a odhalené kybernetické incidenty a předkládá o tom zprávu, jejímž obsahem jsou i návrhy na zmírnění nepřijatelných rizik a návrhy na změnu priorit bezpečnostních projektů, a to pravidelně každé pololetí výboru KB,
 - e. je oprávněn stanovit
 - i. rozsah a hranice SŘBI (s ohledem na aktiva a organizační bezpečnost), ve kterém určí, kterých organizačních částí a technických prvků se SŘBI týká,
 - ii. jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik,
 - iii. cíle kontinuity činností a strategii (plán) řízení kontinuity další činnosti pro oblast KB,
 - iv. provozní pravidla a postupy SŘBI,
 - v. plán zvládnutí rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládnutí rizik včetně určení osoby zajišťující prosazování bezpečnostních opatření,

- f. podílí se na schvalování závazných norem pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií univerzity,
 - g. v případě projektů týkajících se informačních systémů se podílí se na přípravě a organizaci akceptačního řízení, včetně bezpečnostního testování,
 - h. kontroluje po věcné stránce formulaci zadávacích požadavků veřejných zakázek na výstavbu a modernizaci informačních a komunikačních systémů univerzity, či na pořízení dodávek či služeb, jejichž komponenty mohou mít vliv na KB univerzity, z hlediska standardů KB a poskytuje součinnost zadavateli v zadávacích řízeních týkající se vyřešení otázek souvisejících s KB,
 - i. řídí proces řešení kybernetické bezpečnostní události, nebo kybernetického incidentu a rozhoduje o způsobu řešení,
 - j. rozhoduje o realizaci bezpečnostního opatření na základě informací z monitorovacích a dohledových systémů, rozhodnutí výboru KB, nebo NÚKIB,
 - k. zajišťuje
 - i. detekci kybernetických bezpečnostních událostí,
 - ii. zpracovávání zpráv o hodnocení aktiv a rizik a prohlášení o aplikovatelnosti, které obsahuje přehled zavedených bezpečnostních opatření,
 - iii. u dodavatelů pravidelné hodnocení rizik, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků,
 - iv. aktualizaci SRBI a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení účinnosti bezpečnostních opatření,
 - v. aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky; plánu zvládnání rizik a plánu rozvoje bezpečnostního povědomí,
 - vi. realizaci reaktivních opatření vydaných NÚKIB,
 - vii. součinnost při provádění kontrolních auditů prováděných NÚKIB,
 - l. navrhuje změny strategie KB univerzity a bezpečnostní politiky SRBI,
 - m. vypracovává plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje výbor KB,
 - n. koordinuje opatření ke zvýšení bezpečnostního povědomí v organizaci včetně školení a cvičení KB,
 - o. odpovídá za stanovení pravidel pro dodavatele, která zohledňují potřeby SRBI.
5. Manažer KB je oprávněn vyžadovat:
- a. od rektora
 - i. určení osob pro výkon rolí garantů aktiv a provedení základní identifikace aktiv,
 - b. od garantů primárních aktiv zpracování a předložení
 - i. účelu systému a podmínek jeho provozování,
 - ii. identifikovaných primárních aktiv a jejich rizik,
 - iii. ohodnocení přijatelnosti těchto rizik,
 - iv. stanovení bezpečnostních parametrů (úrovní) systémem poskytovaných služeb,
 - c. od garantů podpůrných aktiv a administrátorů (tzv. power users)
 - i. identifikování podpůrných aktiv a jejich rizik,
 - ii. ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik,
 - iii. vyhodnocení účinnosti kybernetických bezpečnostních opatření.

Přechodná a závěrečná ustanovení

Čl. 8 - Přechodná ustanovení

1. Pozice manažera KB bude obsazena do konce ledna 2022.
2. Pozice garantů aktiv, architekta KB a auditora KB budou obsazeny do konce dubna 2022.
3. Do konce dubna 2022 předloží manažer KB analýzu bezpečnostních rizik.

Čl. 9 - Závěrečné ustanovení

Toto opatření nabývá účinnosti dne 15. listopadu 2021.

V Praze dne 11. listopadu 2021

	prof. MUDr. Tomáš Zima, DrSc., MBA
	rektor

[.pdf ke stažení](#)