UNIVERZITA
KOMENSKÉHO
V BRATISLAVE

Vnútorné predpisy Univerzity Komenského v Bratislave

Vnútorný predpis č. 41/2023

Smernica rektora
Univerzity Komenského v Bratislave

Zabezpečenie informačnej bezpečnosti na Univerzite Komenského v Bratislave

Ročník 2023

Obsah

Rektor Univerzity Komenského v Bratislave (ďalej len „UK") vydáva v súlade s čl. 65 ods. 2 vnútorného predpisu č. 5/2023 Štatút UK túto smernicu

PRVÁ ČASŤ
VŠEOBECNÉ USTANOVENIA

Čl. 1
Základné ustanovenia

(1) Cieľom tejto smernice je nastavenie vnútorných procesov na UK s účelom zabezpečiť informačnú bezpečnosť (ďalej len „IB").

(2) UK touto smernicou transponuje požiadavky v oblasti IB, ktoré jej vyplývajú zo všeobecne záväzných predpisov, a to najmä z:

a) zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti"),
b) vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
c) zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,
d) vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
e) nariadenie Európskeho parlamentu a rady (EÚ) 2016/ 679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES,
f) zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
g) smernica Európskeho parlamentu a rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148.

Čl. 2
Personálne zabezpečenie IB

Za účelom zabezpečovania IB sa na UK zriaďuje:

a) Grémium informačnej bezpečnosti (ďalej ako „GIB") a
b) pozícia manažéra informačnej bezpečnosti (ďalej aj „manažér IB").

Čl. 3
Definícia pojmov

Bezpečnostná politika UK (ďalej len „BP UK") je verejný dokument, ktorý sa v primeranej miere vzťahuje na všetky osoby, ktoré pristupujú k aktívam univerzity. Zamestnanci, externí spolupracovníci, spolupracujúce organizácie a ostatné osoby, ktorých sa týkajú povinnosti vyplývajúce z Bezpečnostnej politiky musia byť s Bezpečnostnou politikou a jej zmenami primeraným spôsobom včas oboznámení. Bezpečnostnú politiku schvaľuje vedenie univerzity.

DRUHÁ ČASŤ
GRÉMIUM INFORMAČNEJ BEZPEČNOSTI

Čl. 4
Účel zavedenia GIB

GIB sa zakladá ako poradný orgán rektora UK na zabezpečovanie IB v zmysle príslušných právnych predpisov a prevádzkovania jeho praktických dopadov podľa stanovených predpisov.

Čl. 5
Úlohy GIB

(1) GIB predovšetkým:

a) určuje ciele a stratégiu IB UK, koordinuje prípravu, implementáciu a rozvoj jednotnej BP UK,
b) kontroluje implementáciu IB na celej univerzite,
c) pomáha vytvárať celkový koncept IB,
d) vyjadruje sa k návrhom a implementácii bezpečnostných procesov,
e) je súčinné pri hodnotení účinnosti bezpečnostných opatrení, ich dôsledkov, ako aj vhodnosti. V prípade nutnosti hľadá alternatívne riešenia vhodné pre UK,
f) posudzuje prijateľnosť alebo neprijateľnosť identifikovaných bezpečnostných rizík, vrátane stanovenia prijateľnej miery rizika,
g) prerokováva informácie o nutných opatreniach v oblasti IB,
h) prerokováva správy z auditov.

(2) GIB ďalej prerokováva a predkladá Vedeniu UK:

a) návrhy vnútorných predpisov v oblasti IB,
b) koncepciu BP UK a ďalšiu dokumentáciu v oblasti IB,
c) strategické kroky v oblasti IB, ktoré by sa zásadným spôsobom dotýkali zamestnancov a študentov UK,
d) návrhy rozpočtu na zabezpečovanie oblasti IB,
e) minimálne raz ročne, spravidla k odovzdaniu výročnej správy o činnosti UK, správu o činnosti GIB.

(3) Súčasťou koncepcie BP UK je záväzná bezpečnostná dokumentácia v oblasti IB, ktorá obsahuje:

a) organizáciu a súvisiacu dokumentáciu BP UK,

b) zoznam informačných a komunikačných systémov, ktoré sú zahrnuté v BP UK,
c) správy zo skúmania BP UK,
d) prehlásenie o aplikovateľnosti BP UK.

(4) V oblasti ochrany osobných údajov GIB spolupracuje s poverenou osobou pre ochranu osobných údajov a konzultuje s ňou predkladané správy z testovania a hodnotenia účinnosti zavedených technických a organizačných opatrení na zabezpečenie spracovania dát a osobných údajov.

Čl. 6
Zloženie GIB

(1) GIB má najmenej 5 členov, ktorých po konzultácii s riaditeľom Centra informačných technológii UK menuje a odvoláva rektor.

(2) Členom GIB sú minimálne:

a) riaditeľ Centra informačných technológií UK, ktorý je predsedom GIB,
b) manažér IB – v prípade, že je táto funkcia vykonávaná právnickou osobou, zastupuje ju v GIB osoba na to splnomocnená,
c) ďalší členovia.

(3) GIB môže medzi seba pozvať ďalších relevantných hostí, ak je to v záujme UK, ktorý však v rámci GIB nemajú hlasovacie práva.

Čl. 7
Prijímanie rozhodnutí

(1) GIB prijíma rozhodnutia verejným hlasovaním. Verejné hlasovanie sa uskutočňuje zdvihnutím ruky. Hlas každého člena GIB má rovnakú váhu.

(2) GIB je schopné uznášať sa, ak je prítomná nadpolovičná väčšina jeho členov.

(3) GIB prijíma rozhodnutia vo forme uznesení, pričom na prijatie uznesenia je potrebná nadpolovičná väčšina hlasov všetkých členov GIB.

Čl. 8
Práva a povinnosti členov GIB

(1) Členovia GIB majú právo podieľať sa na aktivitách GIB, vznášať námety a pripomienky k prerokovávaným správam a návrhom, uplatňovať svoje stanoviská pri riešení problémov.

(2) Členovia GIB sú povinní sa zúčastňovať jeho schôdzí a plniť úlohy, ktorými boli poverení.

(3) Predseda GIB predovšetkým:

a) riadi a organizuje činnosť GIB,
b) po schválení GIB vydáva stanoviská, odporúčania a ďalšie dokumenty GIB,
c) prideľuje na základe rozhodnutia GIB, úlohy v oblasti IB a koordinuje ich splnenie s cieľom dosiahnutia súladu informačných a komunikačných systémov UK s požiadavkami právnych predpisov a vnútorných predpisov UK.

(4) V neprítomnosti predsedu GIB plní jeho úlohy iný, ním určený člen GIB.

(5) Chod GIB zabezpečuje po administratívnej a organizačnej stránke Centrum informačných technológií UK.

(6) Schôdze GIB sú zvolávané predsedom GIB, najmenej raz za 6 mesiacov.

TRETIA ČASŤ
MANAŽÉR INFORMAČNEJ BEZPEČNOSTI

Čl. 9
Práva a povinnosti manažéra IB

(1) Manažér informačnej bezpečnosti sa zaoberá riešením kybernetického bezpečnostného incidentu a má za úlohu zabezpečiť všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident. Pre univerzitu ako poskytovateľa digitálnej služby je koordinačnou a komunikačnou osobou Národným bezpečnostným úradom (ďalej len „NBÚ"),

(2) Činnosť manažéra IB môže byť vykonávaná zamestnancom UK alebo byť zabezpečená sprostredkovane cez externého dodávateľa.

(3) Manažér IB je priamo podriadený riaditeľovi Centra informačných technológii UK a je vždy členom GIB. V rámci organizačnej štruktúry rektorátu je zaradený v Centre informačných technológii UK.

(4) Manažér IB je poverený komunikáciou s NBÚ, vrátane prípadov riešenia kybernetických bezpečnostných udalostí a incidentov.

(5) Po schválení GIB vydáva metodické usmernenia týkajúce sa IB.

(6) Manažér IB predovšetkým:

a) zodpovedá za plánovanie a organizovanie realizácie kybernetických bezpečnostných projektov, ktoré schválilo GIB, a to tak, aby informačná a komunikačná infraštruktúra UK poskytovala služby v tejto oblasti v súlade s platnou legislatívnou úpravou v oblasti IB,
b) zodpovedá za vytvorenie a chod BP UK, vrátane priebežného testovania a prevencie, až po elimináciu následkov a vyhodnotenie kybernetických incidentov na UK,
c) priebežne analyzuje vývoj BP UK a vyhodnocuje identifikované kybernetické riziká, kybernetické bezpečnostné udalosti a odhalené kybernetické incidenty, o ktorých predkladá správu, ktorej obsahom sú aj návrhy na zmiernenie neprijateľných rizík a návrhy na zmenu priorít bezpečnostných projektov, a to pravidelne každých 6 mesiacov,
d) je oprávnený stanoviť:

1. rozsah a hranice BP UK (pričom berie ohľad na aktíva UK a organizačnú bezpečnosť), v ktorom určí najmä, akých organizačných častí a technických prvkov sa BP UK týka,
2. jednotnú metodiku pre identifikáciu a hodnotenie aktív a metodiku na stanovenie kritérií pre prijateľnosť rizík,

3. ciele činností a stratégií (plán) riadenia kontinuity iných činností pre oblasť IB,
4. prevádzkové pravidlá a postupy BP UK,
5. plán zvládania rizík, ktorý obsahuje ciele a prínosy bezpečnostných opatrení pre zvládanie rizík vrátane určení osoby zabezpečujúcej presadenie bezpečnostných opatrení,

e) pripravuje návrhy vnútorných predpisov UK na výber, unifikáciu a systemizáciu technických a programových prostriedkov informačných technológií UK,
f) zodpovedá za zabezpečenie schopnosti UK implementovať opatrenia, ktoré jej ukladá platná legislatíva,
g) v prípade projektov, ktoré sa týkajú informačných systémov sa podieľa na príprave a organizácii akceptačného riadenia, vrátane bezpečnostného testovania,
h) v rámci procesu verejného obstarávania, po vecnej stránke kontroluje formuláciu zadávaných požiadaviek zákaziek na výstavbu a modernizáciu informačných a komunikačných systémov UK, či na zabezpečenie dodávok alebo služieb, ktorých komponenty môžu mať vplyv na IB UK, z pohľadu štandardov IB a poskytuje súčinnosť zadávateľovi pri požiadavkách týkajúcich sa riešenia otázok súvisiacich s IB,
i) riadi proces riešenia kybernetickej bezpečnostnej udalosti, alebo kybernetického incidentu a rozhoduje o spôsobe riešenia,
j) rozhoduje o realizácii bezpečnostného opatrenia na základe informácií z monitorovacích systémov, rozhodnutí GIB alebo NBÚ,
k) zabezpečuje:

1. detekciu kybernetických bezpečnostných udalostí,
2. spracovanie správ o hodnotení aktív a rizík a prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad zavedených bezpečnostných opatrení,
3. pravidelné hodnotenie rizík, vykonávanie kontrol zavedených bezpečnostných opatrení u poskytovaných služieb a odstraňovanie zistených nedostatkov u dodávateľov,
4. aktualizáciu BP UK a príslušnú dokumentáciu podľa výsledkov auditov alebo významných zmien a vyhodnotenie účinnosti bezpečnostných opatrení,
5. aktualizáciu správy o hodnotení aktív a rizík bezpečnostnej politiky, plánu zvládania rizík a plánu rozvoja bezpečnostného povedomia,
6. realizáciu reaktívnych opatrení vydaných NBÚ,
7. súčinnosť pri prípadných kontrolných auditoch NBÚ,

l) navrhuje zmeny stratégie IB UK a BP UK,
m) vypracováva plán rozvoja bezpečnostného povedomia a s týmto plánom oboznamuje GIB,
n) v spolupráci so Školiacim strediskom Centra informačných technológií UK koordinuje opatrenia na zvýšenie bezpečnostného povedomia na univerzite vrátane školení a cvičení IB,
o) zodpovedá za stanovenie pravidiel pre dodávateľov, ktoré musia zohľadňovať potreby BP UK.

(7) Manažér IB je oprávnený od technických správcov vyžadovať identifikáciu informácií, systémov, aplikácií a hardvéru v majetku UK, ktoré sa používajú pri prevádzkových činnostiach a identifikáciu rizík, ktoré vyplývajú z ich používania.

(8) Zamestnanci UK, najmä technickí správcovia sietí, sú povinní rešpektovať pokyny Manažéra IB, predsedu GIB a ďalších zamestnancov Centra informačných technológií UK v oblasti IB.

Čl. 10
Prechodné ustanovenia

(1) Pozícia manažéra IB bude obsadená do 01.03.2024.

(2) Do 01.06.2024 predloží manažér IB analýzu bezpečnostných rizík.

Čl. 11
Záverečné ustanovenia

Táto smernica nadobúda platnosť dňom podpisu a účinnosť dňom 01.01.2024.

V Bratislave, 15.12.2023

prof. JUDr. Marek Števček, DrSc.
rektor UK