UNIVERZITA PARDUBICE	
Směrnice č. 7/2021	
Věc:	Základní politika bezpečnosti informací - způsob zajištění kybernetické bezpečnosti na Univerzitě Pardubice
Působnost:	Všechny organizační útvary univerzity a její součásti
Účinnost:	11. května 2021
Číslo jednací:	RPO/0025/21
Vypracoval:	Ing. Jiří Slanina, vedoucí OSSS (CITS)
Předkládá:	Ing. Olga Klápšťová, ředitelka CITS
Schválil:	prof. Ing. Miroslav Ludwig, CSc., prorektor pro vnitřní záležitosti

Článek 1
Předmět úpravy

1. Tato směrnice je vydána na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), a jeho prováděcích předpisů, zejména vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti, dále jen „vyhláška o kybernetické bezpečnosti“).
2. Tato směrnice je součástí bezpečnostní politiky v oblasti systému řízení bezpečnosti informací v rámci Univerzity Pardubice (dále jen „Univerzita“).
3. Tato směrnice určuje v rámci Univerzity složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role, jejich odpovědnosti a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

Článek 2
Výklad základních pojmů

1. „Bezpečnostní politikou“ se rozumí soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
2. „Primárním aktivem“ se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.
3. „Podpůrným aktivem“ se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.
4. „Technickým aktivem“ se rozumí takové technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém.
5. „Systémem řízení bezpečnosti informací“ (dále jen „SŘBI“) se rozumí část systému řízení Univerzity založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.
6. „Bezpečností informací“ se rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat.

7. „Kybernetickou bezpečnostní událostí“ je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
8. „Kybernetickým bezpečnostním incidentem“ je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické události.

Článek 3
Organizace bezpečnosti informací

1. Za účelem celkového řízení a rozvoje SŘBI se ustanovuje Výbor pro řízení kybernetické bezpečnosti (dále také jen „Výbor“).
2. V souvislosti se zavedením SŘBI se určuje bezpečnostní role Manažer kybernetické bezpečnosti.

Článek 4
Výbor

1. Výbor je pětičlenný a sestává z:
    a. Prorektora pro vnitřní záležitosti coby předsedy Výboru,
    b. Kvestora coby místopředsedy Výboru,
    c. Manažera kybernetické bezpečnosti,
    d. Ředitele Centra informačních technologií a služeb,
    e. Akademického pracovníka Univerzity, odborně způsobilého pro celkové řízení a rozvoj SŘBI, jmenovaného rektorem, a to na dobu 4 let.
2. Členství předsedy a/nebo místopředsedy ve Výboru zaniká dnem skončení funkčního období, odvoláním nebo vzdáním se funkce.
3. Členství ostatních členů Výboru zaniká dnem jejich odvolání na návrh rektora po předchozím projednání ve Výboru, případně odstoupením.
4. Administrativní činnosti Výboru zajišťuje tajemník Výboru, kterým je zaměstnanec Univerzity pověřený předsedou Výboru. Tajemník není členem Výboru.

Článek 5
Činnost Výboru

1. Výbor zejména:
    a. stanovuje cíle a strategii kybernetické bezpečnosti Univerzity a koordinuje přípravu, implementaci a rozvoj SŘBI v oblasti kybernetické bezpečnosti,
    b. projednává a doporučuje ke schválení rektorem Základní politiku bezpečnosti informací – způsob zajištění kybernetické bezpečnosti na Univerzitě Pardubice a kontroluje její implementaci v rámci Univerzity,
    c. pomáhá vytvářet koncept kybernetické bezpečnosti,
    d. vyjadřuje se k návrhům a implementaci bezpečnostních procesů,
    e. podílí se na hodnocení účinnosti bezpečnostních opatření, jejich důsledků i vhodnosti, jakož i na identifikaci jim odpovídajících alternativ vhodných pro Univerzitu,
    f. projednává zprávy z realizovaných auditů kybernetické bezpečnosti, které jsou prováděny v souladu s § 16 vyhlášky o kybernetické bezpečnosti,

g. informuje vedení Univerzity o opatřeních v oblasti kybernetické bezpečnosti.

2. Výbor dále projednává a předkládá rektorovi:
   a. posouzení přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika,
   b. návrhy na přidělení finančních prostředků pro oblast kybernetické bezpečnosti navržených Výboru Manažerem kybernetické bezpečnosti,
   c. návrhy na stanovení pořadí důležitosti realizace jednotlivých bezpečnostních opatření a bezpečnostních projektů navržených Výboru Manažerem kybernetické bezpečnosti.
3. Výbor projednává a předkládá rektorovi závaznou bezpečnostní dokumentaci v oblasti kybernetické bezpečnosti, a to zejména:
   a. organizaci SŘBI,
   b. dokumentaci SŘBI,
   c. seznam informačních a komunikačních systémů zahrnutých do rozsahu SŘBI,
   d. zprávy z přezkoumání SŘBI (nejméně 1x ročně),
   e. prohlášení o aplikovatelnosti SŘBI.
4. V oblasti ochrany osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále také jen „nařízení“ nebo „obecné nařízení“) Výbor spolupracuje s Pověřencem pro ochranu osobních údajů a bere na zřetel jeho stanoviska.

Článek 6
Práva a povinnosti členů Výboru

1. Členové Výboru mají právo podílet se aktivně na jeho činnosti, vznášet dotazy, náměty, připomínky k projednávaným zprávám a návrhům, či uplatňovat svá stanoviska k řešení problémů.
2. Členové Výboru jsou povinni účastnit se jeho zasedání a plnit úkoly, kterými je Výbor pověřil.
3. Předseda Výboru zejména:
   a. řídí a organizuje činnost Výboru,
   b. vydává stanoviska, doporučení a další dokumenty Výboru,
   c. na základě rozhodnutí Výboru ukládá úkoly v oblasti kybernetické bezpečnosti a koordinuje jejich plnění s cílem dosažení souladu informačních a komunikačních systémů Univerzity s požadavky zákona o kybernetické bezpečnosti, souvisejícími platnými právními předpisy a vnitřními předpisy Univerzity.
4. Na základě jednání Výboru předkládá předseda Výboru rektorovi schválené návrhy dokumentů, či požadavků na uskutečnění výdajů z finančních zdrojů Univerzity na zabezpečení nutné míry kybernetické bezpečnosti dle článku 5 odst. 2 a 3.
5. V nepřítomnosti předsedy Výboru plní jeho úkoly místopředseda Výboru.

Článek 7
Zasedání Výboru

1. Zasedání Výboru jsou svolávána, na návrh Manažera kybernetické bezpečnosti, předsedou Výboru podle potřeby, nejméně však jednou za 3 měsíce.

2. Návrh programu zasedání Výboru navrhuje předseda Výboru. Vychází přitom z materiálů předložených k projednání, z návrhů členů Výboru a úkolů uložených na jeho předchozích zasedáních. Návrh programu je projednán a schválen na začátku každého zasedání Výboru.
3. Zasedání Výboru jsou neveřejná.
4. Kromě členů Výboru se zasedání účastní tajemník a dále se zasedání může účastnit rektor a Pověřenec pro ochranu osobních údajů, kteří rovněž obdrží podklady k zasedání. V případě potřeby může předseda Výboru rozhodnout i o přítomnosti dalších osob.
5. Zasedání mohou být realizována v distanční podobě pomocí vhodného prostředku komunikace na dálku, který umožňuje přenos zvuku a obrazu (dále jen „distanční zasedání"). O formě zasedání rozhoduje předseda Výboru.
6. Výbor je způsobilý zasedat a usnášet se, je-li přítomna nadpoloviční většina všech členů Výboru. Usnesení je přijato v případě, že pro něj hlasují alespoň tři členové Výboru.

Článek 8
Manažer kybernetické bezpečnosti

1. Manažera kybernetické bezpečnosti jmenuje a odvolává rektor. Kvalifikační požadavky Manažera kybernetické bezpečnosti stanovuje vyhláška o kybernetické bezpečnosti.
2. Manažer kybernetické bezpečnosti je podřízen přímo rektorovi.
3. Manažer kybernetické bezpečnosti odpovídá za následující činnosti:
    a. plánování a řízení realizace kybernetických bezpečnostních projektů schválených Výborem tak, aby informační a komunikační infrastruktura Univerzity poskytovala služby v této oblasti v souladu s platnými právními předpisy v oblasti kybernetické bezpečnosti, zejména v souladu se zákonem o kybernetické bezpečnosti a s vyhláškou o kybernetické bezpečnosti,
    b. vytvoření SŘBI od průzkumu a analýz, přes průběžné testování, prevenci až po vyhodnocení následků kybernetických incidentů na Univerzitě, a jako takový je i osobou komunikující s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") pro případy řešení kybernetických bezpečnostních událostí a incidentů,
    c. zajištění schopnosti Univerzity implementovat opatření ukládaná platnými právními předpisy v oblasti kybernetické bezpečnosti a za včasnou a hospodárnou implementaci těchto opatření,
    d. projednání směrnice Základní politika bezpečnosti informací – způsob zajištění kybernetické bezpečnosti na Univerzitě Pardubice Výborem.
4. Role Manažera kybernetické bezpečnosti není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů a s dalšími provozními či řídicími rolemi.
5. V případě dlouhodobé nepřítomnosti Manažera kybernetické bezpečnosti pověří rektor dočasně jeho zastupováním jiného vhodného zaměstnance.

Článek 9
Odpovědnost a pravomoci Manažera kybernetické bezpečnosti

1. Manažer kybernetické bezpečnosti má následující odpovědnost za činnosti:
    a. řízení systému bezpečnosti informací v souladu se zákonem a požadavky Univerzity,
    b. pravidelnou komunikaci a reporting pro vrcholové vedení,
    c. řízení aktiv a analýzy rizik a předkládání Zpráv o hodnocení aktiv a rizik, Plánů zvládání rizik, návrhy na akceptaci rizik a Prohlášení o aplikovatelnosti Výboru,

d. poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT,
e. komunikuje s GovCERT/CSIRT, NÚKIB a sleduje jeho pokyny, výzvy a předkládá dokumentaci,
f. koordinuje proces řízení bezpečnostních událostí a incidentů,
g. posuzuje projekty s vlivem na kybernetickou bezpečnost,
h. určuje rozsah a způsob vzdělávání zainteresovaných stran,
i. vyhodnocuje vhodnost a účinnost bezpečnostních opatření,
j. spolupracuje při provádění auditů a penetračních testů a
k. spolupracuje při tvorbě politik kybernetické bezpečnosti.

2. Manažer kybernetické bezpečnosti má následující pravomoci:
   a. požadovat od zaměstnanců informace a podklady týkající se kybernetické bezpečnosti,
   b. ve stavu ohrožení rozhodnout o odstavení systémů.

Článek 10
Závěrečná ustanovení

1. Tato směrnice nabývá platnosti dnem podpisu rektora a účinnosti dnem 11. května 2021.

V Pardubicích dne

prof. Ing. Jiří Málek, DrSc.
rektor