Univerzita Karlova

Opatření rektora č. 35/2024

Název: **Politika systému řízení bezpečnosti informací**

Gestor:

Odbor kybernetické bezpečnosti RUK

Účinnost:

1. listopadu 2024

Politika systému řízení bezpečnosti informací

ČÁST I.
ÚVODNÍ USTANOVENÍ

Čl. 1
Základní ustanovení

1. Toto opatření rektora upravuje hlavní zásady, cíle, bezpečnostní potřeby a práva a povinnosti ve vztahu k řízení kybernetické bezpečnosti na Univerzitě Karlově (dále jen „univerzita“) a jejích součástech.
2. Toto opatření stanovuje politiku systému řízení bezpečnosti informací (dále také „ISMS“) na univerzitě dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a 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), a dle stanoveného rozsahu a pokrytí ISMS v rámci univerzity.

Čl. 2
Cíle v oblasti řízení bezpečnosti informací

1. Cílem ISMS na univerzitě je zajistit spolehlivost a bezpečnost informačních a komunikačních technologií provozovaných pro podporu činností na univerzitě a nakládání s informacemi při zachování dostupnosti, integrity a důvěrnosti zpracovávaných informací a poskytovaných služeb.
2. Hlavním cílem a účelem tohoto opatření je zajistit ochranu zpracovávaných informací a poskytovaných služeb na univerzitě tak, aby byla zachována jejich důvěrnost, integrita a dostupnost. Současně je cílem zajištění bezproblémového a bezvýpadkového poskytování vědeckých a vzdělávacích služeb a činností. Univerzita
   a) integruje požadavky ISMS do svých vnitřních procesů,
   b) zajišťuje dostupnost zdrojů potřebných pro zajištění kybernetické bezpečnosti,
   c) přiděluje odpovědnost za jednotlivé oblasti kybernetické bezpečnosti s využitím systému bezpečnostních funkcí a rolí,
   d) ve vztahu k zaměstnancům univerzity
      i. vysvětluje potřebu zajištění kybernetické bezpečnosti s důrazem na pochopení jejich individuálního podílu,
      ii. zvyšuje znalost bezpečnostních postupů s využitím bezpečnostního školení a
      iii. zabezpečuje odpovídající kvalifikaci zaměstnanců pověřených výkonem bezpečnostních rolí formou bezpečnostního vzdělávání,
   e) uplatňuje relevantní bezpečnostní kritéria při výběru dodavatelů výrobků a služeb a při uzavírání obchodních vztahů k zajištění nejvyšší možné míry bezpečnosti dodávaných služeb a
   f) zajišťuje pravidelné přezkoumání stavu kybernetické bezpečnosti na univerzitě a prosazovat neustálé zlepšování zajištění kybernetické bezpečnosti.

Čl. 3
Rozsah systému řízení bezpečnosti informací

1. Systém řízení bezpečnosti informací je zaváděn pro celou univerzitu a všechny její součásti, které se podílejí na provozu, fungování a zpracování informací a poskytování služeb v určených významných informačních systémech.
2. Rozsah systému řízení bezpečnosti informací je zpracován v samostatném dokumentu, který je součástí bezpečnostní dokumentace podle čl. 22 tohoto opatření.

ČÁST II.
ORGANIZACE SYSTÉMU ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Čl. 4
Určení bezpečnostních rolí

1. V rámci organizace systému zajištění kybernetické bezpečnosti jsou definovány následující role a orgány, zapojené do systému řízení bezpečnosti informací:
   a) rektor,
   b) Výbor pro řízení kybernetické bezpečnosti,
   c) vedoucí představitelé fakult, vysokoškolských ústavů a jiných pracovišť,
   d) vedoucí zaměstnanci,
   e) vedoucí odboru kybernetické bezpečnosti Rektorátu univerzity,
   f) architekt kybernetické bezpečnosti,
   g) specialista kybernetické bezpečnosti,
   h) auditor kybernetické bezpečnosti,
   i) garant primárního aktiva,
   j) garant podpůrného aktiva,
   k) provozovatel informačního systému,
   l) zaměstnanec,
   m) ostatní organizační útvary univerzity.
2. Provádění povinností plynoucích z Politiky ISMS zajišťují všichni vedoucí zaměstnanci na univerzitě dle jim stanovené působnosti a odpovědnosti. K naplňování úkolů souvisejících s kybernetickou bezpečností jsou zavázáni všichni zaměstnanci univerzity.
3. Role Auditora kybernetické bezpečnosti je neslučitelná s výkonem jiných rolích a působením v orgánech uvedených v odstavci 1.
4. Osoby vykonávající role uvedené v odst. 1 písm. e) až h) nesmí být organizačně zařazeny v útvarech zajišťujících správu, rozvoj a podporu provozu informačních a komunikačních technologií na univerzitě.

Čl. 5
Kontakt s orgány veřejné správy

Vedoucí odboru kybernetické bezpečnosti

a) udržuje potřebné kontakty s regulačními orgány státní správy v oblasti kybernetické bezpečnosti a nastavit procesy pro adekvátní reakce na avizované hrozby, zejména v návaznosti na opatření vydaná Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“),
b) zajišťuje komunikaci univerzity s NÚKIB a
c) je oprávněn pro komunikaci s NÚKIB určit také další osoby.

Čl. 6
Kontakt se zájmovými skupinami

Vedoucí odboru kybernetické bezpečnosti, případně další jím pověření zaměstnanci, udržují potřebné kontakty s odbornou komunitou a s poskytovateli externích služeb a sledují vývoj v oblasti kybernetické bezpečnosti.

ČÁST III.
ODPOVĚDNOSTI KYBERNETICKÉ BEZPEČNOSTI

Čl. 7
Rektor

1. Rektor univerzity je vrcholovým orgánem v oblasti kybernetické bezpečnosti.
2. Rektor
   a) podporuje budování a zlepšování ISMS,
   b) zajišťuje pro systém řízení bezpečnosti informací dostatečné zdroje,
   c) na návrh vedoucího odboru kybernetické bezpečnosti jmenuje členy Výboru pro řízení kybernetické bezpečnosti a vydává Statut a jednací řád Výboru pro řízení kybernetické bezpečnosti.

Čl. 8
Výbor pro řízení kybernetické bezpečnosti

1. Zřizuje se Výbor pro řízení kybernetické bezpečnosti. Při své činnosti se řídí Statutem a jednacím řádem Výboru pro řízení kybernetické bezpečnosti.
2. Výbor pro řízení kybernetické bezpečnosti
   a) odpovídá za celkové řízení a rozvoj systému řízení bezpečnosti informací a kybernetické bezpečnosti univerzity,
   b) vytváří rámec kybernetické bezpečnosti, směřování a zásad kybernetické bezpečnosti univerzity,
   c) kontroluje a přezkoumává aktuální stav kybernetické bezpečnosti,
   d) se vyjadřuje k návrhům a implementaci organizačních a technických opatření a
   e) schvaluje bezpečnostní dokumentaci.

Čl. 9
Vedoucí představitelé fakult a dalších součástí univerzity

Vedoucí představitelé fakult a dalších součástí univerzity
   a) účastní se projednávání bezpečnostních záležitostí na stanovených poradách v oblasti kybernetické bezpečnosti,
   b) uskutečňují rozhodnutí rektora univerzity, Výboru pro řízení kybernetické bezpečnosti a vedoucího odboru kybernetické bezpečnosti a doporučení ohledně kybernetické bezpečnosti v rámci své součásti univerzity a
   c) řídí implementaci přijatých bezpečnostních opatření v příslušné součásti univerzity.

Čl.10
Vedoucí zaměstnanci

1. Vedoucí zaměstnanci všech stupňů řízení na univerzitě odpovídají za uskutečňování pravidel, procesů a bezpečnostních opatření v rámci své působnosti. Jsou povinni prosazovat kybernetickou bezpečnosti do praxe, vést své podřízené k dodržování tohoto

opatření a navazující bezpečnostní dokumentace a k plnění stanovených zásad kybernetické bezpečnosti v praxi.

2. Vedoucí zaměstnanci
   a) dbají na dodržování pravidel, postupů a bezpečnostních opatření při nakládání s informacemi při poskytování služeb a zajišťování jejich dostupnosti, důvěrnosti a integrity,
   b) sledují aktuální informace v oblasti řízení kybernetické bezpečnosti na univerzitě a sdělují je svým podřízeným,
   c) dohlížejí na dodržování bezpečnostních pravidel podřízenými zaměstnanci,
   d) instruují podřízené zaměstnance k nahlášení kybernetické bezpečnostní události a incidentu, jehož je podřízený zaměstnanec účasten nebo jej odhalil, pokud se o něm dozví,
   e) spolupracují na procesu identifikace a hodnocení aktiv a rizik a poskytují další potřebnou součinnost osobám zastávajícím bezpečnostní role při výkonu jejich úkolů na poli kybernetické bezpečnosti,
   f) řídí se pokyny vedoucího odboru kybernetické bezpečnosti při zavádění a optimalizaci procesů, pravidel a bezpečnostních opatření a
   g) poskytují v potřebném rozsahu součinnost Architektovi kybernetické bezpečnosti a Specialistovi kybernetické bezpečnosti při zavádění a optimalizaci procesů, pravidel a bezpečnostních opatření.

Čl. 11
Vedoucí odboru kybernetické bezpečnosti

1. Vedoucí odboru kybernetické bezpečnosti plní roli manažera kybernetické bezpečnosti univerzity.
2. Vedoucí odboru kybernetické bezpečnosti navrhuje rektorovi členy Výboru pro řízení kybernetické bezpečnosti a předkládá k vydání Statut a jednací řád Výboru pro řízení kybernetické bezpečnosti.
3. Vedoucí odboru kybernetické bezpečnosti odpovídá za plánování, organizování a řízení realizace opatření, projektů a programů pro zajištění kybernetické bezpečnosti na univerzitě tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu a přidělených a dostupných zdrojů.
4. Vedoucí odboru kybernetické bezpečnosti
   a) schvaluje, doporučuje a plánuje technická a organizační opatření,
   b) prosazuje téma kybernetické bezpečnosti a Politiku systému řízení bezpečnosti informací,
   c) navrhuje a vydává bezpečnostní dokumentaci,
   d) řídí systém řízení bezpečnosti informací,
   e) iniciuje, sleduje a vyhodnocuje implementaci technických a organizačních opatření kybernetické bezpečnosti,
   f) informuje rektora univerzity a Výbor pro řízení kybernetické bezpečnosti o aktuálním stavu systému řízení bezpečnosti informací,
   g) koordinuje projekty spojené s kybernetickou bezpečností,
   h) koordinuje opatření ke zvýšení bezpečnostního povědomí na univerzitě a školení o kybernetické bezpečnosti,
   i) kontroluje plnění plánovaných úkolů v oblasti kybernetické bezpečnosti,
   j) připravuje přezkoumání systému řízení bezpečnosti informací,

k) dokumentuje systém řízení bezpečnosti informací,
l) informuje rektora univerzity o technických a organizačních opatřeních v oblasti kybernetické bezpečnosti,
m) zpracovává a předkládá návrh na personální a finanční kapacity a zdroje, včetně rozpočtu na dodávky a služby v oblasti kybernetické bezpečnosti,
n) komunikuje s příslušnými státními orgány ve věcech kybernetické bezpečnosti a
o) je pověřen komunikací s NÚKIB včetně případů řešení kybernetických bezpečnostních událostí a incidentů; výkon této pravomoci může pro jednotlivé záležitosti přenést na jinou osobu.

Čl. 12
Architekt kybernetické bezpečnosti

1. Architekt kybernetické bezpečnosti je určen a řízen vedoucím odboru kybernetické bezpečnosti.
2. Architekt kybernetické bezpečnosti posuzuje všechny prvky tvořící podpůrná aktiva na univerzitě v jejich souvislostech a navrhuje možné cesty, případně způsoby dalšího rozvoje řízení kybernetické bezpečnosti jako podklad pro rozhodování rektora. Určuje a komunikuje klíčové podmínky, principy a modely, které popisují budoucí stav řízení kybernetické bezpečnosti na univerzitě.
3. Architekt kybernetické bezpečnosti se podílí na iniciaci změny, dává podněty, které vyplývají z koncepčně řízené bezpečnostní architektury, spoluiniciuje vznik strategických projektů, které naplňují požadavky legislativy v oblasti kybernetické bezpečnosti. Navrhuje rovněž základní bezpečnostní architektury informačních systémů a informačních a komunikačních technologií, jejich jednotlivých komponent, vzájemných vazeb a dohlíží na soulad implementace základní architektury informačních a komunikačních systémů se systémem řízení bezpečnosti informací.
4. Architekt kybernetické bezpečnosti je odpovědný za návrh implementace technických opatření.
5. Hlavní úlohou architekta kybernetické bezpečnosti je navrhnout a metodicky dozorovat implementaci odpovídajících bezpečnostních opatření na univerzitě a existující opatření průběžně analyzovat a s výsledky seznamovat vedoucího Odboru kybernetické bezpečnosti.
6. Úkoly architekta kybernetické bezpečnosti dále zahrnují popis stávajícího stavu bezpečnostních opatření, formulování požadovaného stavu kybernetické bezpečnosti na univerzitě a identifikaci kroků vedoucích k jeho dosažení.
7. Architekt kybernetické bezpečnosti
   a) definuje klíčové projekty, které vedou k naplnění požadavků kybernetické bezpečnosti a k cílovému stavu modelu architektury kybernetické bezpečnosti na univerzitě, dohlíží na jejich realizaci a vyhodnocení,
   b) analyzuje úrovně architektury kybernetické bezpečnosti na univerzitě, definuje pro ni metriky, identifikuje existující rizika a navrhuje strategii na zmírnění rizik,
   c) vytváří plány implementace architektury kybernetické bezpečnosti na univerzitě, určuje části a milníky k dosažení očekávaného cílového stavu,
   d) navrhuje bezpečnostní opatření pro snižování rizik, připravuje pravidla a standardy pro oblast kybernetické bezpečnosti na univerzitě,
   e) vybírá a implementuje nástroje pro zajištění technických opatření kybernetické bezpečnosti na univerzitě,

f) podílí se na pravidelném plánování v souladu se strategickými cíli univerzity a na aktualizaci strategie kybernetické bezpečnosti univerzity,
g) vytváří a udržuje model architektury kybernetické bezpečnosti na univerzitě (procesní model, organizační struktura, aplikační architektura, technologie apod.) a
h) vyhodnocuje průběžně aktuální stav úrovně kybernetické bezpečnosti na univerzitě podle stanovených metrik.

Čl. 13
Auditor kybernetické bezpečnosti

1. Auditor kybernetické bezpečnosti provádí audit systému řízení bezpečnosti informací na univerzitě, zpracovává požadovanou dokumentaci, včetně tvorby výstupních auditních zpráv a vyjádření k naplnění požadavků legislativy v oblasti kybernetické bezpečnosti. Tato role přispívá k efektivnější ochraně systému řízení bezpečnosti informací na univerzitě. Je zpravidla zajišťován z odborníků mimo univerzitu.
2. Auditor kybernetické bezpečnosti
   a) prověřuje fungování systémů řízení bezpečnosti informací na univerzitě v souladu s legislativou v oblasti kybernetické bezpečnosti a jeho prováděcími předpisy, platnými mezinárodními ISO normami, případně se zásadami, standardy a směrnicemi univerzity a
   b) kontroluje aktuálnost a dodržování platných zákonných i interními akty řízení stanovených procesních postupů, evidencí, školení a reportování identifikovaných kybernetických bezpečnostních událostí.
3. Auditor kybernetické bezpečnosti je odpovědný za provádění auditů systému řízení bezpečnosti informací.
4. Auditor kybernetické bezpečnosti odpovídá za formální i věcně správné a úplné provedení auditu kybernetické bezpečnosti.
5. Auditor kybernetické bezpečnosti dále
   a) plánuje činnost auditu podle specifických podmínek univerzity,
   b) vede dokumentaci o průběhu auditu podle stanovených metodik,
   c) vyhodnocuje shromážděné nálezy z auditu a srovnává je s kritérii auditu,
   d) sděluje výsledky auditu oprávněný osobám a navrhuje doporučení a
   e) zpracovává závěrečnou zprávu z auditu.

Čl. 14
Specialista kybernetické bezpečnosti

1. Specialista kybernetické bezpečnosti je organizačně zařazen v odboru kybernetické bezpečnosti a je řízen vedoucím odboru kybernetické bezpečnosti.
2. Specialista kybernetické bezpečnosti je role, jejímž úkolem je průběžně rozvíjet metodiky, navazující postupy a plány pro praktickou implementaci organizačních a technických opatření a dohlížet na jejich plnění v jednotlivých organizačních částech univerzity Specialista se také podílí na projektovém řízení a koordinaci projektů.
3. Specialista kybernetické bezpečnosti
   a) poskytuje součinnost vedoucímu odboru kybernetické bezpečnosti a auditorovi kybernetické bezpečnosti v rámci bezpečnostních projektů,
   b) zajišťuje zavádění technických a organizačních opatření s cílem posílení kybernetické bezpečnosti na univerzitě,
   c) podílí se na projektovém řízení a koordinačních činnostech a
   d) zajišťuje obsluhu a správu vybraných bezpečnostních technologií.

Čl. 15
Garant aktiva

1. Garant aktiva, skupiny aktiv nebo třídy aktiv je osobou zařazenou v systému řízení bezpečnosti informací na univerzitě na nejnižším stupni řízení tak, že jeho pravomoci a odpovědnosti jsou vždy vztaženy na konkrétní aktivum.
2. Povinnosti týkající se aktiv směřují k nastavení pravidel pro jejich řízení, zajištění důvěrnosti, integrity a dostupnosti aktiva, rozsahem a způsoby odpovídajícími jeho povaze.
3. Garant aktiva
   a) zajišťuje dodržování pravidel bezpečnosti přidělených aktiv,
   b) navrhuje úpravy těchto pravidel,
   c) komunikuje a spolupracuje s bezpečnostními rolemi ISMS podle čl. 4 odst. 1 písm. a) až h) tohoto opatření, kterým při jejich činnosti poskytuje potřebnou součinnost,
   d) řídí se pokyny vedoucího odboru kybernetické bezpečnosti při zavádění a optimalizaci procesů, pravidel a bezpečnostních opatření a
   e) poskytuje součinnost a informace vedoucímu odboru kybernetické bezpečnosti, architektovi kybernetické bezpečnosti a specialistovi kybernetické bezpečnosti při zavádění a optimalizaci procesů, pravidel, bezpečnostních opatření a kybernetických bezpečnostních událostech a incidentech.

Čl. 16
Garant primárního aktiva

1. Primárními aktivy jsou informace, služby a procesy, které zajišťují fungování univerzity, bez kterých se univerzita neobejde a bez kterých není schopna zajišťovat funkčnost významných informačních systémů a dále informace, které jsou zpracovávány v rámci klíčových procesů. Primárním aktivem jsou procesy, prostřednictvím kterých dochází ke zpracování jedné nebo více informací.
2. Garant primárního aktiva zajišťuje rozvoj, použití a bezpečnost primárního aktiva, zejména jeho důvěrnosti, dostupnosti a integrity.
3. Garant primárního aktiva definuje požadavky na zabezpečení primárního aktiva.

Čl. 17
Garant podpůrného aktiva

1. Podpůrnými aktivy jsou technické vybavení, komunikační prostředky dotčeného systému a jeho programové vybavení, objekty, ve kterých je tento systém umístěn, dále zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti aktiva.
2. Garant podpůrného aktiva
   a) zajišťuje rozvoj, použití a bezpečnost podpůrného aktiva a funkčnost vazby podpůrného aktiva na primární aktiva,
   b) odpovídá za funkčnost podpůrného aktiva a určení funkčních a bezpečnostních požadavků na podpůrné aktivum,
   c) odpovídá za dostupnost svěřeného informačního systému v případě výpadku, důvěrnost dat v něm uchovávaných a jeho integritu (bezchybnost fungování),
   d) nastavuje pravidla pro správu a bezpečnost svěřeného podpůrného aktiva (důvěrnost, dostupnost a integritu) po technické stránce a
   e) je jím zpravidla osoba odpovědná za chod zařízení s dodržením nastavených parametrů poskytovaných služeb.

Čl. 18
Provozovatel informačního systému

1. Provozovatel informačního systému zajišťuje svěřený informační systém po stránce obsahu funkcí a rozvoje informačního systému.
2. Provozovatel informačního systému je odpovědný za to, že informační systém obsahuje všechny funkce potřebné pro zajištění procesu, který informační systém podporuje. Provozovatel informačního systému potvrzuje možnosti změnových požadavků na funkcionalitu informačního systému.
3. Provozovatel informačního systému
   a) dodržuje pokyny a bezpečnostní opatření určené univerzitou v rozsahu stanovených práv a povinností,
   b) odpovídá za plnění a dodržování veškerých pravidel, postupů a bezpečnostní opatření v rozsahu stanovených práv a povinností,
   c) komunikuje, spolupracuje a poskytuje součinnost bezpečnostním rolím ISMS podle čl. 4 odst. 1 písm. a) až j) tohoto opatření,
   d) poskytuje součinnost při provádění auditu kybernetické bezpečnosti v rámci provozovaného informačního systému,
   e) po obdržení informace o svém určení provozovatelem informačního systému od univerzity neprodleně oznamuje své kontaktní údaje pomocí určeného formuláře NÚKIB a dává je na vědomí univerzitě a zároveň tyto údaje zachovává aktuální a v případě změny je hlásí NÚKIB a dává je na vědomí univerzitě,
   f) ohlašuje jakékoliv podezření na vznik kybernetických bezpečnostních událostí a incidentů prostřednictvím komunikačních kanálů,
   g) poskytuje součinnost vedoucímu Odboru kybernetické bezpečnosti nebo dalším pověřeným osobám při vyhodnocování kybernetických bezpečnostních událostí a
   h) poskytuje součinnost a řídí se pokyny vedoucího Odboru kybernetické bezpečnosti nebo dalších pověřených osob při zvládání kybernetických bezpečnostních událostí a incidentů.

Čl. 19
Zaměstnanec

Zaměstnanci univerzity jsou povinni

a) seznamovat se prostřednictvím vstupních a pravidelných školení s požadavky na kybernetickou bezpečnost na univerzitě a dodržovat je,
b) hlásit podezřelé chování informačních systémů užívaných na univerzitě a další skutečnosti, které by mohly naznačovat porušení důvěrnosti, integrity či dostupnosti informací neboli kybernetické bezpečnostní události,
c) při zjištění kybernetického bezpečnostního incidentu spolupracovat s osobami oprávněnými vyšetřovat kybernetický bezpečnostní incident a předložit jim své pracovní technické zařízení a další pracovní prostředky, jsou-li k tomu vyzváni a
d) spolupracovat při auditech a kontrolních činnostech kybernetické bezpečnosti.

Čl. 20
Specifické odpovědnosti vybraných odborů Rektorátu univerzity, fakult a dalších součástí univerzity

1. V rámci ISMS jsou kladeny nároky zejména na:

a) Ústav výpočetní techniky – při provozu významných informačních systémů, zajištění jejich ochrany,
b) CSIRT-CUNI – při zajištění monitoringu a ochraně síťového provozu a při řešení kybernetických bezpečnostních událostí a incidentů,
c) právní odbor Rektorátu univerzity – při zajištění informací o právních předpisech v oblasti kybernetické bezpečnosti a konzultace právních náležitostí smluv s dodavateli,
d) odbor veřejných zakázek Rektorátu univerzity – při prosazování kybernetické bezpečnosti do relevantních výběrových a zadávacích řízení,
e) odbor vnějších vztahů Rektorátu univerzity – při poskytování informací médiím o zvládání vzniklých bezpečnostních incidentů a krizových situací,
f) personální oddělení ekonomického, personálního a mzdového odboru Rektorátu univerzity – při zajištění zavedení opatření v oblasti bezpečnosti lidských zdrojů s důrazem na organizaci školení a vzdělávání v oblasti bezpečnosti informací,
g) bezpečnostní odbor Rektorátu univerzity – při zajištění fyzické bezpečnosti a kontinuity činností univerzity,
h) fakulty a další součásti univerzity – při organizaci ISMS v rámci své podřízenosti,
i) Správu budov a zařízení – při zajištění fyzické bezpečnosti a kontinuity činností.

ČÁST IV.
OBLASTI ISMS

Čl. 21
Seznam oblastí systému řízení bezpečnosti informací

1. Zavádění systému řízení bezpečnosti informací zahrnuje
   a) systém řízení bezpečnosti informací, který tvoří základní organizační rámec pro řízení kybernetické bezpečnosti na univerzitě,
   b) řízení rizik, které spočívá v identifikaci významných rizik, zvolení vhodného způsobu jejich snížení, včetně plánování konkrétních opatření ke sledování úrovní rizik a k vyhodnocování účinnosti zvoleného způsobu snížení rizik,
   c) bezpečnostní politika, kterou je míněna komplexní řídící bezpečnostní dokumentace upravující všechny uvedené oblasti ISMS,
   d) organizační bezpečnost, v jejímž rámci jsou stanoveny a zaváděny řídící bezpečnostní procesy na univerzitě a jsou určeny osoby, které jsou pověřeny výkonem bezpečnostních rolí na univerzitě,
   e) stanovení bezpečnostních požadavků pro dodavatele, jejichž cílem je stanovit minimální bezpečnostní požadavky pro všechny dodavatele a určit významné dodavatele, vyhodnotit rizika spojená s těmito významnými dodavateli a stanovit a zavázat významné dodavatele k plnění speciálních bezpečnostních podmínek a toto plnění kontrolovat a pravidelně vyhodnocovat,
   f) řízení aktiv, jehož smyslem je identifikace, udržování přehledu a klasifikace aktiv a stanovení vhodných ochranných opatření k manipulaci, likvidaci a používání aktiv a zajištění dodržování těchto opatření,
   g) bezpečnost lidských zdrojů, která stanoví pravidla a postupy pro zajištění bezpečnostního povědomí zaměstnanců univerzity, uživatelů významných informačních systémů, administrátorů, osob zastávajících bezpečnostní role a také zaměstnanců významných dodavatelů,

h) řízení provozu a komunikací, které stanoví pravidla a postupy pro bezpečný provoz významných informačních systémů,
i) řízení změn, které stanoví pravidla pro určení významných změn významných informačních systémů a pro hodnocení a řízení rizik spojených s těmito změnami, pro testování změn a pro možnost navrácení do původního stavu před změnou,
j) řízení přístupu, které stanoví pravidla pro řízení přístupu k primárním aktivům a k významným informačním systémům jako takovým,
k) akvizice, vývoj a údržba, které stanoví způsob bezpečného pořízení nových významných informačních systémů a provedení jejich změny,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, které stanoví odpovědnosti a postupy pro sledování, analyzování a vyhodnocování potenciálních bezpečnostních problémů a pokud se potvrdí, aby byly včas potlačeny a aby byla provedena opatření pro eliminaci obdobných problémů v budoucnu,
m) řízení kontinuity činností, které upravuje postupy a pravidla pro zajištění nepřetržitého výkonu důležitých činností univerzity, pokud dojde k závažnému omezení dostupnosti služeb významných informačních systémů,
n) kontrola a audit, které stanoví pravidla pro provádění pravidelných interních auditů a kontrol dodržování bezpečnostní politiky univerzity,
o) fyzická bezpečnost, díky níž jsou určeny prostory univerzity, kterým je třeba poskytnout zvýšenou ochranu z hlediska zabezpečení významných informačních systémů, a jsou stanovena pravidla pro ochranu těchto prostor,
p) aplikační bezpečnost, která stanoví pravidla pro zajištění provádění penetračních testů významných informačních systémů před jejich uvedením do provozu a při významných změnách a která stanoví další opatření k zajištění nepopiratelnosti a neoprávněné činnosti aplikací a informací,
q) kryptografické prostředky, které stanoví pravidla pro zajištění bezpečného a dostatečně silného šifrování důležitých aktiv,
r) bezpečnost průmyslových a řídících systémů, která stanoví pravidla pro používání nástrojů pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických systémů.

2. Pravidla, procesy a bezpečnostní opatření oblastí ISMS jsou dále specifikovány v dalších dokumentech bezpečnostní dokumentaci ISMS.

Čl. 22
Bezpečnostní dokumentace ISMS

1. V rámci univerzity jsou pravidla, procesy a bezpečnostní opatření dokumentována napříč bezpečnostní dokumentací.
2. Bezpečnostní dokumentace je tvořena na základě principu need-to-know. Tedy aby jednotlivé dokumenty byly dostupné pouze relevantním zaměstnaneckým pozicím, které zde mají povinnosti a odpovědnosti.
3. Bezpečnostní dokumentace obsahuje pravidla, postupy a bezpečnostní opatření potřebná pro vybudování a provoz systému řízení bezpečnosti informací v souladu s legislativními požadavky.

Čl. 23
Řízení zdrojů pro zajištění kybernetické bezpečnosti

1. Finanční zdroje na kybernetickou bezpečnost tvoří zdroje na zajištění výkonu rolí, zajištění vzdělávání a školení, provoz a projekty podporující zajištění kybernetické bezpečnosti na univerzitě.
2. Požadavky na finanční zdroje pro konkrétní kalendářní rok zpracovává a předkládá vedoucí odboru kybernetické bezpečnosti v rámci schvalování rozpočtu univerzity s přihlédnutím k dosavadnímu dosažení cílů tohoto opatření.

Čl. 24
Audit, kontrola a přezkoumávání ISMS

1. Za účelem dosažení cílů ISMS musí být zajištěny kontrolní a monitorovací aktivity účinnosti a dostatečnosti pravidel, postupů a bezpečnostních opatření. Kontrolními a monitorovacími aktivitami ISMS jsou
   a) audit,
   b) kontrola a
   c) přezkoumávání.

Čl. 25
Audit

1. Audit ISMS nebo jeho jednotlivých pravidel, procesů a bezpečnostních opatření zajišťuje auditor kybernetické bezpečnosti. Audit může být zajištěn externím dodavatelem.
2. Audit ISMS se na univerzitě provádí
   a) pravidelně alespoň jednou za tři roky, nebo
   b) mimořádně při změnách, které mohou mít negativní dopad na kybernetickou bezpečnost nebo pokud dojde k bezpečnostnímu incidentu se závažným dopadem na vybrané informační systémy.
3. Výsledky auditu ISMS předkládá auditor kybernetické bezpečnosti vedoucímu odboru kybernetické bezpečnosti a tyto výsledky slouží jako vstupy pro průběžné vyhodnocování ISMS a pro plánování zlepšování.

Čl. 26
Kontrola a nápravná opatření

1. Kontrola ISMS probíhá prostřednictvím interní a externí kontroly.
2. Interní kontrola ISMS představuje kontrolu účinnosti a plnění nastavených bezpečnostních opatření a stav jejich skutečné realizace. Interní kontrola ISMS musí být prováděna průběžně odpovědnými zaměstnanci dle požadavků a postupů popsaných v jednotlivých bezpečnostních politikách a v navazující dokumentaci.
3. Externí kontrola ISMS představuje kontrolu plnění povinností ISMS a dalších povinností stanovených rozhodnutími a opatřeními obecné povahy NÚKIB.
4. Systém řízení bezpečnosti informací je průběžně monitorován prostřednictvím nastavených pravidel, procesů, bezpečnostních opatření a prostředků.
5. Systém řízení bezpečnosti informací je udržován a zlepšován také prostřednictvím identifikace neshod a incidentů.

Čl. 27
Přezkoumání

1. Přezkoumání systému řízení bezpečnosti informací je prováděno průběžně.

2. Cílem přezkoumání je vyhodnocování účinnosti systému řízení bezpečnosti informací. Přezkoumání je promítnuto do dalších aktivit a plánů zlepšování ISMS.

ČÁST VI.
ZÁVĚREČNÁ USTANOVENÍ

Čl. 28
Závěrečná ustanovení

1. Zrušuje se opatření rektora č. 44/2021, Zajišťování kybernetické bezpečnosti na Univerzitě Karlově.
2. Toto opatření nabývá platnosti dnem jeho podpisu a účinnosti dne 1. listopadu 2024.

V Praze dne 23. října 2024

prof. MUDr. Milena Králíčková, Ph.D.