Politika řízení změn

I. Úvodní ustanovení

1) Politika řízení změn stanovuje pravidla a postupy řízení významných změn tak, aby byl zajištěn minimální negativní dopad změn na informace, služby a procesy informačních systémů a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„zákon o kybernetické bezpečnosti*") 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), ve znění pozdějších předpisů (dále také *„vyhláška o kybernetické bezpečnosti*") v podmínkách Univerzity Hradec Králové (dále také *„UHK*").

2) Účelem této politiky je definovat základní pravidla a postupy procesu řízení významných změn v rámci celého životního cyklu tzn. od návrhu, přes posouzení a testování až po nasazení významné změny. Postup je zaměřen na identifikaci významných změn a jejich následné řízení včetně provedení analýzy rizik.

3) Tato politika je platná pro všechny provozované části a subsystémy informačních systémů UHK.

4) Zaměstnanci UHK, postupují podle této politiky v případech:

   a) nezbytnosti úprav v programovém vybavení, které vyplývají ze změn legislativy, obecně závazných předpisů, interních předpisů UHK, optimalizací vnitřních procesů nebo z jiných závažných důvodů,

   b) přípravy nových služeb nebo produktů, jejichž komplexní zabezpečení vyžaduje i odpovídající podporu v informačním systému UHK,

   c) při vzniku požadavku na úpravu nebo doplnění funkcí informačního systému nebo při zjištění nedostatků nebo chyb, které se vyskytnou v provozu stávajícího, již používaného informačního systému UHK a jeho softwarových či hardwarových součástí.

II. Druhy a oblasti změn

Významná změna v oblasti bezpečnosti informací

1) Podle §2 písm. o) vyhlášky o kybernetické bezpečnosti je významná změna taková, která může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko pro UHK.

2) Pokud definujeme bezpečnost podle §2 zákona o kybernetické bezpečnosti jako zajištění důvěrnosti, dostupnosti a integrity informací a služeb, můžeme rozdělit změny následovně:

Změna bezpečnosti informací	**Popis změny**	**Změny bezpečnostních opatření**
Změna důvěrnosti	Dochází ke změně vedených dat (rozšíření, přidání osobních údajů nebo osobních údajů zvláštní kategorie). Dochází ke změně příjemců dat (nový typ příjemců, zveřejnění části dat nebo celku, sdílení dat mimo s třetími stranami aj.) Dochází ke změně důvěrnosti poskytovaných služeb.	Změna řízení přístupu. Změny uživatelských oprávnění. Změna zaznamenávání přístupu. Změny v šifrování dat. Změny bezpečnostních prvků vnějšího i vnitřního perimetru.
Změna dostupnosti	Dochází ke změně dostupnosti vedených dat. Požadovaná dostupnost se zvyšuje, anebo snižuje. Dochází ke změně dostupnosti poskytovaných služeb.	Změna v rozsahu zálohování a obnovy. Změna v koncepci záložního systému. Změna v oblasti redundance systému.
Změna integrity	Dochází ke změně integrity dat. Dopady na primární aktiva při narušení integrity jsou jinak hodnoceny z hlediska oprávněné osoby, dopady mohou být více či méně významné. Dochází ke změně integrity poskytovaných služeb.	Změny v zaznamenání změn. Změny v oblasti autentizačních prvků. Změny bezpečnostních prvků vnějšího i vnitřního perimetru.

3) Změny v oblasti důvěrnosti, dostupnosti a integrity jsou vždy změnami významnými a jsou Garanty primárního nebo podpůrného aktiva vždy hlášeny podle postupu uvedeného níže Manažerovi kybernetické bezpečnosti (dále také *„Manažer KB*") jako návrhy na významné změny.

Oblasti změn a významných změn v kybernetické bezpečnosti

1) Vzhledem k tomu, že významná změna může zahrnovat celou oblast kybernetické bezpečnosti, je nezbytné k oblasti bezpečnosti informací doplnit rovněž významné změny, které jsou realizovány na úrovni technických a podpůrných aktiv a přímo ovlivňují kybernetickou bezpečnost primárního aktiva.

2) V následující tabulce jsou vymezeny změny v jednotlivých oblastech kybernetické bezpečnosti, které mohou být změnami významnými a jsou Garanty příslušného aktiva vždy hlášeny podle postupu uvedeného níže Manažerovi KB.

Oblast změny	Příklad běžné změny	Příklady změny, která může být významná změna
Aplikační bezpečnost	– změna User interface – změna nastavení prováděná Garantem aktiva – změna postupů administrace systému – využití nových knihoven nebo frameworků	– každá změna, která ovlivňuje stávající aktiva aplikační a komunikační bezpečnosti – zásadní nová funkce systému využívaná většinou koncových Uživatelů – zásadní změny funkcí systému (změny procesů a postupů schvalování) – nové služby poskytované veřejnosti
Změna infrastruktury	– výměna disků v diskovém poli – výměna serveru nebo jeho části – výměna aktivních prvků vyjma jmenovaných – servisní obměna komponent kapacitní, výkonové či komunikační kapacity	– každá změna, která mění, rozšiřuje nebo jinak upravuje objemovou, výkonovou či komunikační kapacitu kromě běžné údržby a obměny – nové diskové pole – nová farma serverů nebo její část – nové core switche, firewall – změna výrobce OS nebo hypervizoru nebo databáze

Změna zajišťování úrovně dostupnosti	– změna verze OS, DB, hypervizoru – změna certifikátu – změna nastavení zálohování. – změna schématu D/R	– koncepční změna konfigurace oprávnění administrátorů – koncepční změna způsobu připojení k centrálním službám – změna způsobu zálohování – změna způsobu ukládání záloh – výměna systému D/R – změna procesů D/R
Bezpečnost lidských zdrojů	– změna Uživatele – změna klíčového Uživatele – změna Garanta aktiva – změna frekvence rozšiřování bezpečnostního povědomí	– změna verze či konfigurace IDM – koncepční změna politiky hesel – nasazení vícefaktorové autentizace
Změna v oblasti organizace KB	– procesní změna při hlášení incidentů – procesní změna při schvalování externích přístupů – změna pravidel při implementaci a provozu	– zařazení IS do VIS, KII, PZS – každá změna, která ovlivňuje procesy Systému řízení bezpečnosti informací
Bezpečnost dodavatelů	– změna dodavatele dílčí činnosti či komponenty – změna konzultanta či poradce – změna dodavatele internetového připojení	– změna významného dodavatele – změna provozovatele – změna podmínek zajištění kybernetické bezpečnosti významného dodavatele
Fyzická bezpečnost	– oprava UPS, dieselgenerátoru, chlazení, čidel – změny kabeláže, přemístění racků – instalace nových zařízení do racku	– změna místa serverovny – změna centrální UPS – změna dieselgenerátoru – zásadní změna zabezpečení serverovny – změna místa provozu technické infrastruktury nebo IS

Bezpečnost komunikačních sítí	– výměna switche, routeru –změna firmware zařízení – změna konfigurace sítě – změna nastavení internetového připojení – změna monitoringu – změna nastavení vnitřního směrování sítí – výměna síťového HW 1:1	– koncepční změna konfigurace VLAN, DMZ – bezpečnostní změna pravidel na firewallu – koncepční změna způsobu propojení datových center nebo připojení poboček – změna pravidel vnějšího směrování komunikace či změna pravidel IPS/IDS
Ochrana před škodlivým kódem	– reinstalace antiviru na stanici/zařízení – zajištění prostupu pro dodavatele – aktualizace verze antivirového/antispamového systému	– výměna antivirového/antispamového systému – koncepční změna v oblasti ochrany před škodlivým kódem – změna pravidel nastavení antivirového/antispamového systému
Cloudové služby	– změna rozsahu a nastavení cloudových služeb	– změna dodavatele cloudových služeb
Zaznamenávání událostí včetně jejich korelace	– změna struktury logování – uchování logů na jiné infrastruktuře včetně migrace – změna korelačních pravidel – zapojení nových IS nebo technických aktiv do dohledového a logovacího systému	– koncepční změna pořizovaných logů – koncepční změna ochrany pořizovaných logů – koncepční změna nejméně 10 korelačních pravidel – výměna či rozšíření kapacity dohledového a logovacího systému – změna schématu logování a uchovávání logů, změna eskalačních procesů
Kryptografické prostředky	– změna hash nebo šifrovacího algoritmu – rozšíření rozsahu či typu šifrovaných dat	– koncepční změna zabezpečení všech zařízení (např. notebooků) – změna klíčových prvků interní CA – změna hashe či změna algoritmů šifrování

III. Obecné principy řízení změn

1) Služby poskytované UHK musí být dostatečně zajištěny prostřednictvím SLA, které by mělo být v souladu s BCM požadavky, a mělo by obsahovat dostatečně jasná práva a povinnosti na straně dodavatele a UHK. Kromě toho by zde měly být uvedeny vhodná bezpečnostní opatření pro zajištění bezpečnosti služeb a informací.

2) Při veškerých změnách musí být postupováno v souladu s procesem řízení významných změn za účelem jednotného a strukturovaného přístupu. Tím by mělo být dosaženo skutečnosti, že odpovědné osoby budou mít kompletní přehled o všech změnách a tím budou moci lépe řídit kybernetickou bezpečnost UHK.

3) Proces řízení významných změn by měl být v souladu se zásadami projektového řízení. Změna je totiž ve své podstatě specifický druh projektu v rámci akvizice, vývoje a údržby. Pomocí tohoto provázání dojde k uchopení bezpečnosti informací v celkovém pojetí napříč UHK.

4) Při řízení významných změn by mělo dojít k identifikaci a zaznamenávání významných změn. Tím bude dosaženo naplnění velké části legislativních požadavků (disponovat informacemi v dokumentované formě) a také k možné revizi významné změny.

5) Již v rámci plánování by mělo dojít k ohodnocení významné změny v rámci rizik, které z ní plynou včetně odhadu potenciálních dopadů na IS a na UHK. Tím bude dosaženo souladu s principem založeným na rizicích, kdy musíme znát, čemu čelíme a následně volíme vhodná bezpečnostní opatření, abychom snížili pravděpodobnost, že riziko nastane nebo odstraníme zranitelnosti apod.

6) Součástí procesu řízení významných změn musí být formální schvalovací procedury pro plánované významné změny. Prostřednictvím toho by mělo být dosaženo situace, kdy osoby provádějící významné změny jsou pod dohledem na základě zvýšené kontroly.

7) Změny by měly být dostatečně komunikovány všem dotčeným osobám takovým způsobem, aby nedošlo k neadekvátnímu narušení kontinuity činností IS a UHK v souladu s BCM. Odpovědné osoby by měly vědět, že dojde např. k pozastavení služby (provozu IS) na dobu 8 hodin s dostatečným předstihem v tomto případě jeden týden dopředu. Na základě této informace by měli mít dostatek času si přizpůsobit své činnosti, a hlavně se tímto předejde neočekávaným nepříjemnostem.

8) V rámci významných změn, by na základě výsledků analýzy rizik mělo dojít k dostatečnému testování významných změn v testovacím prostředí na testovacích datech. Tím je myšleno např. penetrační testování nebo jiné testování zranitelností. Cílem je odhalit zranitelnosti a slabé stránky již v době návrhu před implementací.

9) Při návrhu významné změny a následném zavádění významné změny by měla být zajištěna možnost obnovy/navrácení významné změny do původního stavu. Měly by tedy existovat návratové procedury a odpovědnosti pro rušení a obnovu stavu z neúspěšných významných změn nebo nepředvídatelných událostí.

10) V rámci celého procesu řízení změn musí být napříč politikou a dalšími operačními dokumenty stanoveny jasné role a odpovědnosti na straně zainteresovaných rolí (zaměstnanců), které se podílejí na procesu řízení významných změn. Čím detailněji jsou role a odpovědnosti popsány, tím lépe lze pak docílit optimálního stavu řízení významných změn, jelikož každá role zná své povinnosti a ví, jak se má chovat.

IV. Role a odpovědnosti

1) Jedním ze základních požadavků na efektivně nastavený a fungující proces řízení významných změn je dostatečně detailně a odděleně definované role a jejich odpovědnosti napříč celým procesem.

2) Garant aktiva:
   a) Odpovídá za významnou změnu po věcné stránce,
   b) podílí se na klasifikaci významné změny,
   c) podílí se na posuzování významnosti běžné změny,
   d) dokumentuje požadavek na změnu v požadovaném rozsahu,
   e) zajišťuje, že došlo k předložení a schválení požadavku na odpovědnou osobu před implementací významné změny,
   f) aktualizuje interní dokumentaci,
   g) podává požadavek na významnou změnu,
   h) poskytuje součinnost v průběhu procesu řízení významných změn.

3) Manažer KB:
   a) posuzuje požadavek na významnou změnu z pohledu významnosti a dopadů,
   b) podílí se na klasifikaci významné změny,
   c) podílí se na posuzování významnosti běžné změny,
   d) podílí se na rozhodnutí o provedení penetračního testování a/nebo skenování zranitelností.

4) Aplikační správce:
   a) rozhoduje o klasifikaci významné změny,
   b) rozhoduje o významnosti běžné změny,
   c) rozhoduje požadavek na významnou změnu z pohledu významnosti a dopadů,

d) rozhoduje o provedení penetračního testování a/nebo skenování zranitelností,

e) vede seznam významných změn.

5) Vedoucí oddělení informačních technologií (dále také *„OIT"*) řídí požadavky na změny, které nejsou vyhodnoceny jako významné změny.

6) Výbor pro kybernetickou bezpečnost (dále také *„Výbor KB"*) bere na vědomí seznam významných změn řízených v předcházejícím roce.

7) Uživatel v případě jakýchkoliv dotazů, obav, zjištěných nefunkčností IS či dalších relevantních narušení eskaluje tyto informace na svého nadřízeného nebo využije stanovených komunikačních kanálů v rámci UHK a dále generuje požadavky na významné změny.

V. Proces řízení změn

Krok č. 1: Dokumentovaný požadavek na změnu

1) Prvním krokem je definování požadavku na změnu. Cílem je identifikace potřeby, proč je daná změna potřeba a jaké pro ni existují relevantní důvody. V rámci tohoto kroku dochází ke sběru podnětů a požadavků.

2) Nový požadavek na změnu mohou provést všichni Uživatelé.

3) Na dokumentaci změny Uživatel spolupracuje s Garantem příslušného aktiva a výsledkem je dokumentace změny v rozsahu:

a) popis požadavku na změnu,

b) vyjádření Garanta příslušného aktiva k navrhované změně,

c) termín provedení,

d) popis dopadů na současné řešení/dodavatele/Uživatele.

4) Garant příslušného aktiva je povinen dokumentovat změnu a udržovat ji aktuální.

Krok č. 2: Posouzení, zda se může jednat o významnou změnu

5) Garant příslušného aktiva ve spolupráci s Uživatelem zhodnotí navrhovanou změnu podle kapitoly II této politiky. V případě, kdy Garant příslušného aktiva shledá, že by změna mohla být změnou významnou, informuje e-mailem Manažera KB a do e-mailu přiloží dokumentaci změny.

Krok č. 3: Klasifikace a schválení změny

6) Každý přijatý podnět na významnou změnu od Garanta příslušného aktiva zaznamená a vede Manažer KB. Manažer KB vyhodnotí podnět na významnou změnu a provede ve spolupráci s aplikačním správcem analýzu rizik s cílem identifikace možných negativních dopadů změny.

7) Vyhodnocení podnětu na významnou změnu včetně provedené analýzy rizik předloží Manažer KB aplikačnímu správci v každém případě v rámci výsledku hodnocení rizik.

8) V případě zjištění vysokého rizika významné změny pro UHK a současně v případě, kdy je příslušná změna relevantní s ohledem na kapitolu II této politiky, rozhoduje o klasifikaci změny aplikační správce. V případě, kdy je výsledné riziko analýzy rizik pro UHK vyhodnoceno Manažerem KB jako nízké či střední, je aplikační správce oprávněn toto hodnocení změnit. V případě zjištění vysokého rizika Manažerem KB, není oprávněn toto hodnocení změnit.

9) O klasifikaci změny informuje aplikační správce Manažera KB, Garanta příslušného aktiva a rovněž Uživatele, který je navrhovatelem významné změny.

10) V případě, že došlo ke klasifikaci významné změny, musí být ze strany Garanta příslušného aktiva navržena vhodná bezpečnostní opatření, aby byla snížena vysoká rizika významné změny. Následně aplikační správce posoudí bezpečnostní opatření a případně v součinnosti Garanta příslušného aktiv navrhne nová. Bezpečnostní opatření jsou následně předložena Manažerovi KB ke schválení realizace významné změny. Po schválení může dojít k realizaci významné změny.

Krok č. 4: Realizace významné změny

11) V rámci realizace významné změny Uživatel a Garant příslušného aktiva řídí významnou změnu a dokumentují provádění řízení.

12) V případě potřeby Manažer KB poskytuje Garantu příslušného aktiva nezbytnou součinnost.

13) Manažer KB aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci v případě potřeby.

Krok č. 5: Testování významné změny

14) Součástí významné změny musí být provedeno testování před uvedením do produkčního provozu. Garant příslušného aktiva kontaktuje Manažera KB s návrhem na provedení testování změny. Manažer KB ve spolupráci s aplikačním správcem vyhodnotí návrh a v případě potřeby jej doplní. Garant příslušného aktiva zajistí provedení testování dle požadavku Manažera KB. Po provedení testování Garant příslušného aktiva předloží Manažerovi KB výsledky provedených testů.

Krok č. 6: Nasazení významné změny

15) Po úspěšném testování výsledků následuje implementace změny do produkčního prostředí UHK. Pro implementaci změny by měl být navržen dostatečně detailní a časově definovaný plán nasazení. Součástí plánu musí být možnost navrácení významné změny do původního stavu. Plán Garant příslušného aktiva předkládá Manažerovi KB, který ho musí schválit. Plán bude obsahovat nejméně řešení následujících oblastí:

    a) oznámení o plánovaném výpadku poskytovaných služeb IS,

    b) provedení zálohy dat IS,

    c) realizace významné změny v produkčním prostředí,

d) ověření funkčnosti IS dodavatelem změny,

e) ověření funkčnosti IS Garantem příslušného aktiva (popř. dalšími Uživateli),

f) rozhodnutí o úspěšně/neúspěšně provedené významné změně, popř. návrat a obnova dat ze zálohy,

g) oznámení o funkčnosti IS všem uživatelům.

VI. Závěrečná ustanovení

Politika řízení změn vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor