HODNOCENÍ RIZIKA

Hodnocené podpůrné aktivum (předmět dodávky)	Primární aktivum[1]	Hodnocení důležitosti primárního aktiva	Hodnocení důležitosti podpůrného aktiva[2]			Hodnocení rizika podpůrného aktiva	Hrozba[3]	Zkratka	Hodnocení závažnosti hrozby[2]	Hodnocení závažnosti dopadů (tj. dopad porušení důvěrnosti, dostupnosti nebo integrity aktiva)[2] [1]				Riziko, včetně korekce hodnocením primárního aktiva[2]
			Důvěrnost	Dostupnost	Integrita					Ochrana osobních údajů	Zákonné a smluvní povinnosti	Ztráta důvěryhodnosti	Finanční ztráty	
zakázkový vývoj software, nezahrnuje služby podpory a údržby software v produkčním prostředí. Nepředpokládá se předání osobních údajů Nepředpokládá se přístup dodavatele na produkční prostředí.	*Primární aktivum 1*	1	4	1	3	Technická aktiva (hardwarové a softwarové vybavení, média a dokumenty)[4]	porucha zařízení nebo chybné fungování aplikačního programového vybavení	H1	4	2	2	3	3	3
	Primární aktivum 2	3					nedbalostní nebo úmyslné poškození, chyba použití	H2	1	1	1	1	1	1
							ztráta, odcizení médií nebo dokumentů	H3	2	1	1	1	3	3
							zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění	H4	0					0
							zneužití identity, falšování zpráv	H5	0					0
							zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	H6	1	1	1	1	1	1
							zneužití vyměnitelných technických nosičů dat a mobilních zařízení	H7	2	1	1	1	3	3
							poškození dat použitím aplikačních programů na špatná data z hlediska času	H8	0					0
							provedení neoprávněných činností, tj. činností k nimž uživatel nemá oprávnění	H9	0					0
							zneužití oprávnění ze strany uživatelů[5] a administrátorů	H10	2	2	1	3	3	3
							vzdálená špionáž	H11	1	1	1	1	1	1
							odposlech	H12	1	1	1	1	1	1
							cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	H13	2	1	1	1	1	2
							instalace zákeřného kódu	H14	3	2	3	1	3	3
							neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	H15	4	1	3	1	3	3
							dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky el. energie nebo jiných důležitých služeb	H16	2	1	1	1	2	2
							přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	H17	0					
							porušení bezpečnostní politiky	H18	3	1	1	1	1	2
							chybná identifikace technických aktiv	H19	2	1	1	1	1	2
						Personální aktiva	nedodržení smluvního závazku ze strany subdodavatele	H20	3	1	1	1	1	2
							pochybení ze strany zaměstnanců (včetně trestné činnosti)	H21	4	1	1	1	1	3
							nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	H22	4	2	1	1	2	3
							přechod klíčového personálního aktiva ke konkurenci	H23	3	1	1	1	1	2
							vyzrazení informací	H24	4	1	1	3	2	3
							nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	H25	3	1	1	1	2	3
							chybná identifikace personálních aktiv	H26	2	1	1	1	1	2

POZNÁMKY POD ČAROU

1 Primárním aktivem je vždy služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

2 viz. návod pro vyplnění

3 Hrozby, kterými jsou ohrožena daná aktiva, nikoli hrozby, jejichž aktéry jsou daná aktiva. Př. Zaměstnanci mohou být původci většiny hrozeb, které ohrožují technická aktiva.

4 Zahrnuje hrozby ohrožující fyzická média, data na nich uložená, jakož i dokumentu ve fyzické podobě

5 Uživatelé zahrnují jak zaměstnance povinné osoby, tak jejích dodavatelů

PERSONÁLNÍ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																									
		ORGANIZAČNÍ OPATŘENÍ													TECHNICKÁ OPATŘENÍ												
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídící a obdobné systémy
nedodržení smluvního závazku ze strany subdodavatele	2				3		4	3																			
pochybení ze strany zaměstnanců (včetně trestné činnosti)	3				4			4																			
nedostatečná odborná úroveň	3					2		4																			
přechod klíčového personálního aktiva ke konkurenci	2				4																						
vyzrazení informací	3				4			4																			
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele	3				4			4																			
chybná identifikace personálních aktiv	2	4																									

TECHNICKÁ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																									
		ORGANIZAČNÍ OPATŘENÍ													TECHNICKÁ OPATŘENÍ												
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního programového vybavení	3				2			2	4	3		4	3												2	
nedbalostní nebo úmyslné poškození, chyba použití	1							4																		
ztráta, odcizení médií nebo dokumentů	3		2					4	2				3			3		4	4	3	3	3	3		2		
zničení nebo poškození zařízení v důsledku změn prostředí	1															4											
zneužití vyměnitelných technických nosičů dat	3		3					4			2									2							
zneužití oprávnění ze strany uživatelů a administrátorů	3				4			4	4		4								2								
vzdálená špionáž	1																	4									
odposlech	1																4										
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	2							4									3	3									
instalace zákeřného kódu	3							4	4	2		4	2				3			4		2	2				
neoprávněné užití technického aktiva	3				4		4																				
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2						4		4				3	3							3		3			3	
porušení bezpečnostní politiky	2							4																			
chybná identifikace technických aktiv	2	4																									

SEZNAM OPATŘENÍ K IMPLEMENTACI

ORGANIZAČNÍ OPATŘENÍ			
Kategorie opatření	Potřebná úroveň	Hrozba	Požadavky na dodavatele
Systém řízení bezpečnosti informací	4	H19	Pravidelně vyhodnotuje organizační části a aktiva, která jsou využívaná k poskytování plnění odběratelské společnosti
Organizační bezpečnost	4	H15	Stanovil pravidla pro užití statků chráněných právy duševního vlastnictví.
			Vede evidenci platných licencí, vč. data jejich expirace.
	4	H10	Stanovil pravidla pro určení administrátorů a osob zastávajících bezpečnostní role
	4	H21	Stanovil pravidla pro výběr zaměstnanců.
			Ověřuje kvalifikaci uchazečů o zaměstnání (př. testování).
			Ověřuje reference předchozích zaměstnavatelů uchazečů o zaměstnání.
			Zaměstnanci mají jasně definovanou pracovní náplň a zodpovědnosti.
	4	H23	V pracovních smlouvách klíčových zaměstnanců a sub-dodavatelů je upravena konkurenční doložka zakazující práci pro subjekt v konkurečním postavení k dodavateli po určitou dobu po skončení smluvního vztahu s dodavatelem.
	4	H24	Zaměstnanci a dodavatelé jsou vázáni zákonnou povinností mlčenlivosti.
			Zaměstnanci a dodavatelé jsou vázáni smluvní povinností mlčenlivosti.
			Zaměsnanci a dodavatelé byli poučeni o důvěrnosti zpracovávaných informací.
	4	H25	Sub-dodavatelé jsou smluvně vázáni poskytnout podporu dodavateli při ukončení spolupráce.
			Zajišťuje předání práce zaměstnancem při ukončení pracovního poměru.
			Odcházející zaměstnanec je povinen zaškolit zaměstnance, kterému jsou předávány úkoly odcházejícího zaměstnance.
	3	H20	Stanovil pravidla pro výběr dodavatelů.
			Ověřuje reference potenciálního dodavatele.
			Ověřuje kvalifikaci (dostupné zdroje - personální i finační) potenciálního dodavatele.
	2	H1	Osoby zastávající bezpečnostní role mají dostatečné zdroje (vč. finančních).
			Osoby zastávající bezpečnostní role mají dostatečné pravomoci.
			Dodavatel prosazuje systém řízení bezpečnosti informací a věnuje mu dostatečné zdroje.
Bezpečnostní role	2	H22	Osoby zastávající bezpečnostní role mají předepsanou kvalifikaci.
Řízení dodavatelů	4	H15	Smlouvy se sub-dodavateli zajišťují oprávnění k užívání dat.

			Smlouvy s sub-dodavateli obsahují dostatečné licenční ujednání.
	4	H20	Stanovil pravidla pro sub-dodavatele, která zohledňují požadavky řízení bezpečnosti informací.
			Seznamuje sub-dodavatele s pravidly týkajícími se řízení bezpečnosti informací
			V případě významných dodavatelů, provádí v průběhu výběrového řízení a před uzavřením smlouvy, provádí hodnocení rizik.
			Zajišťuje, aby se jeho významní dodavatele zavázali dodržovat pravidla bezpečnosti informací ve stejném rozsahu, v jakém je zavázán dodavatel ve vztahu k objednateli.
	4	H16	Stanovil pravidla pro sub-dodavatele (zejm. z hlediska dostupnosti služeb).
			V případě významných dodavatelů smluvně upravuje řízení kontinuity činností souvisejících s dodavateli.
Bezpečnost lidských drojů	4	H1, H2, H3, H7, H10, H13, H14, H18	Zajišťuje pravidelná školení zaměstnanců, uživatelů, administrátorů, osob zastávajících bezpečnostních role o jejich povinnostech a bezpečnostní politice.
	4		Zajišťuje pravidelná bepečnostní školení sub-dodavatelů o jejich povinnostech a bezpečnostní politice.
	4		Provádí pravidelné ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.
	4		Zajišťuje pravidelná odborná školení osob zastávajících bezpečnostní role.
	4		Zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
	4		Zajišťuje, aby v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role byla předána odpovědnost osobě, která bude nadále pozici zastávat.
	4		Určil pravidla a postupy řešení případů porušení stanovených bezpečnostních pravidel.
Řízení provozu a komunikací	4	H1	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastavajících bezpečnostní role.
			Řídí technické zranitelnosti
			Stanovil postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.
	2	H3	Vývojové, testovací a provozní prostředí jsou oddělené.
			Provádí pravidelné zálohování dat
			Provádí pravidelnou kontrolu použitelnosti provedených záloh.
			Stanovil pravidla a postupy pro ochranu informací a dat v průběhu celého životného cyklu.
	4	H10	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastavajících bezpečnostní role.

	4	H14	Stanovil pravidla a postupy pro zajištění bezpečnosti síťových služeb.
			Stanovil pravidla a postupy pro ochranu před škodlivým kódem.
	4	H16	Stanovil postupy pro sledování kybernetických bezpečnostních událostí.
			Přijal opatření pro ochranu přístupu k záznamům o kybernetických bezpečnostních událostech.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.
Řízení změn	3	H1, H14	Při provádění změn v rámci plnění přezkoumává mořné dopady změn.
			Určuje významné změny.
			U významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření ke snížení nepříznivých dopadů změny
			Provádí testování před provedením významné změny.
			V případě významné změny zajišťuje možnost navrácení do původního stavu.
Řízení přístupu	2	H7	Stanovil bezpečnostní opatření pro používání mobilních zařízení a jiných technických zařízení, které nejsou ve správě dodavatele.
	4	H10	Při ukončení smluvního vztahu odebírá přístupové oprávnění.
			Při ukončení změně smluvního vztahu změní přístupové oprávnění.
Akvizice, vývoj a údržba	2	H1, H14	Řídí rizika plnění dle VKB
			Řídí významné změny plnění dle VKB
			Stanovil bezpečnostní požadavky a zahrnul je do projektu vývoje.
			zajišťuje bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.
			Provádí bezpečnostní testování významných změn před jejich zavedením do provozu, ev. předáním objednateli.
Zvládání kybernetických bezpečnostních událostí a incidentů	3	H1, H3, H14, H16	Zavedl proces detekce a vyhodnocování bezpečnostních událost a zvládání kybernetických bezpečnostních incidentů
Řízení kontinuity činností	3	H16	Vypracal, pravidelně aktualizuje a testuje plány kontinuity činností.

TECHNICKÁ OPATŘENÍ			
Fyzická bezpečnost	4	H3	Předchází poškození, krádeži nebo zneužití aktiv využívaných pro poskytování plnění nebo přerušení poskytování plnění
	4	H6	Stanovil fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a umístěna technická aktivy využívaná pro poskytování plnění.
Bezpečnost komunikačních sítí	4	H12, H14	Vyčlenil komunikační síť využívanou pro poskytování plnění.

			Zajišťuje řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě
			Zajišťuje důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií pomocí kryptografie.
			Aktivně blokuje nežádoucí komunikaci
			Při segmentaci sítě a řízení komunikace mezi jejími segmenty využívá nástroj, který zajistí ochranu integrity komunikační sítě.
Správa a ověřování identit	4	H3, H11	Používá autentizační mechanismus založený na vícefaktorové autentizaci nejméně s 2 různými typy faktorů
			Používá autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů zajišťující obdobnou úroveň jako vícefaktorová autentizace s 2 různými typy faktorů
			Identity uživatelu, administrátoru a aplikaci, je ověřována pomocí nástroje, který používá k autentizaci identifikátor účtu a heslo, vynucuje 12 znaků u uživatelů a 17 znaků u administrátorů a vymáhá povinnou změnu hesla v intervalu
			Implementace nástroje pro správu a ověření identity uživatelů, administrátorů a aplikací
Řízení přístupových oprávnění	4	H3	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro přístup k jednotlivým aktivům využívaným pro poskytování plnění povinné osobě.
	2	H10	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro pro čtení, zápis dat a změnu oprávnění.
Ochrana před škodlivým kódem	3	H3, H14	Implementoval nástroj zajišťující nepřetržitou automatickou ochranu před škodlivým kódem.
			Řídí oprávnění ke spouštění kódu
			Řídí automatické spouštění obsahu výměnných zařízení a datových nosiců
			Provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.
	2	H7	Monitoruje používání výměnných zařízení a datových nosičů.
Zaznamenávání událotí informačního a komunikačního systému	3	H3, H16	Zaznamenává bezpečnostní a potřebné provozní události aktiv důležitých pro poskytování plnění povinné osobě.
Detekce kybernetických bezpečnostních událostí, Sběr a vyhodnocování kybernetických bezpečnostních událostí	3	H3, H14	V komunikační síti užívané pro poskytování plnění povinné osobě používá nástroj pro detekci kybernetických bezpečnostních událostí.
			Nasadil nástroj pro ověření a kontrolu přenášených dat v rámci komunikační sítě nebo mezi komunikačními sítěmi využívanými pro poskytování plnění.
			Nasadil nástroj pro ověření a kontrolu přenášených dat na perimetru komunikační sítě využívané k poskytování plnění.
			Blokuje nežádoucí komunikaci.

Kryptografické prostředky	2	H3	Používá aktuálně odolné kryptografické algoritmy a kryptografické klíče pro ochranu aktiv užívaných k poskytování plnění.
Zajišťování úrovně dostupnosti informací	2	H1	Zajišťuje redundanci aktiv nezbytných pro poskytování plnění povinné osobě.