Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 6. ZÁŘÍ 2023

VERZE DOKUMENTU: 1.0

ŘÍZENÍ DODAVATELŮ

Základní metodika

Obsah

1 Úvod

Tento podpůrný materiál se zabývá řízením dodavatelů v průběhu celého životního cyklu dodávky, tedy od výběru dodavatele, přes průběh realizace plnění, po splnění smluvního závazku, ukončení smlouvy a závěrečné hodnocení zkušeností s dodavatelem.

Jedná se především o výchozí metodický dokument pro povinné osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), tedy správce a provozovatele informačních systémů **kritické informační infrastruktury**, **významných informačních systémů** a **informačních systémů základní služby**.

Proces řízení dodavatelů je v dokumentu rozebrán podle pravidel obsažených v ZKB a vyhlášce 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 „VKB“), s akcentem na jeho aplikaci v procesu zadávání veřejných zakázek podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“), s ohledem na skutečnost, že osoby spadající do působnosti ZKB jsou v mnoha případech též osobami spadajícími do působnosti zákona č. 134/2016 Sb. a proces výběru jejich dodavatelů je tak svázán určitými pravidly.

Součástí materiálu jsou též doporučení a praktické postupy pro tvorbu politik pro řízení dodavatelů, jejichž vytvoření, schválení, pravidelné přezkoumávání a aktualizaci jakožto součásti bezpečnostní politiky požadují § 3, § 6, § 30 a příloha č. 5 VKB.

Materiál je založen na případech dobré praxe, rozhodně se nejedná o jediný správný způsob řízení rizik spojených s dodavateli, přílohy slouží pouze pro ilustraci a měly by být modifikovány podle potřeb konkrétní organizace. Každé odvětví a každá organizace mají svá specifika a tento materiál nemá ambici stanovit jednotný způsob řízení dodavatelů pro všechny z nich.

Tento materiál byl vyhotoven za součinnosti a spoluautorství Ministerstva financí, Ministerstva vnitra a české pobočky AFCEA.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Proces řízení dodavatelů

Řízení dodavatelů je jedním z organizačních bezpečnostních opatření, k jejichž provádění jsou povinny vybrané osoby spadající do působnosti ZKB, konkrétně povinné osoby podle § 3 písm. c) až f) ZKB (modifikovaně pak též osoby podle § 3 písm. h) ZKB[1]), dále jen „povinné osoby“. Tyto osoby jsou současně povinny zohlednit požadavky vyplývající ze všech bezpečnostních opatření podle § 5 ZKB při výběru dodavatele pro informační nebo komunikační systém podléhající režimu ZKB a relevantní část těchto požadavků zahrnout do smlouvy, kterou s dodavatelem uzavřou. Řízení dodavatelů je proces, který by měl být primárně prováděn správci komunikačních a informačních systémů. Podrobnosti k podobě řízení dodavatelů stanovuje § 8 VKB.

V rámci řízení všech svých dodavatelů povinná osoba musí:

- stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací – § 8 odst. 1 písm. a) VKB,
- seznamovat své dodavatele s těmito pravidly a vyžadovat jejich plnění – § 8 odst. 1 písm. d) VKB,
- řídit rizika spojená s dodavateli – § 8 odst. 1 písm. e) VKB,
- zajistit poučení dodavatelů o jejich povinnostech a o bezpečnostní politice v rámci řízení bezpečnosti lidských zdrojů – § 9 odst. 1 písm. a) bod 1. VKB,
- zajistit oznamování neobvyklého chování systému a podezření na jakékoliv zranitelnosti v rámci zvládání kybernetických bezpečnostních incidentů – § 14 odst. 1 písm. f) VKB.

Dále povinná osoba musí:

- vést evidenci svých významných dodavatelů – § 8 odst. 1 písm. b) VKB, a o vedení v evidenci významné dodavatele prokazatelně písemně informovat – § 8 odst. 1 písm. c) VKB,
- u významných dodavatelů v rámci výběrových řízení a před uzavřením smlouvy provádět hodnocení rizik souvisejících s plněním předmětu výběrového řízení – § 8 odst. 2 písm. a) VKB,
- v rámci uzavíraných smluvních vztahů stanovit způsoby a úrovně realizace relevantních bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření – § 8 odst. 2 písm. b) VKB,
- provádět pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a v reakci na rizika a zjištěné nedostatky zajistit jejich řešení – § 8 odst. 2 písm. c) a d) VKB,

[1] Poskytovatelé digitálních služeb jsou vázáni prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

- zajistit, aby smlouvy, které jsou s významnými dodavateli uzavírány, obsahovaly relevantní oblasti uvedené v příloze č. 7 k VKB – § 8 odst. 1 písm. f) VKB,
- pravidelně přezkoumávat plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací – § 8 odst. 1 písm. g) VKB.

Proces řízení dodavatelů, stejně jako pravidla, která budou od dodavatelů vyžadována, a požadavky, které budou zanášeny do smluv, budou ukotveny především v bezpečnostních politikách povinné osoby, jejichž součástí je v souladu s požadavky přílohy č. 5 k VKB politika řízení dodavatelů.

Celá bezpečnostní dokumentace, stejně jako samotná politika řízení dodavatelů, musí být v souladu s požadavky § 30 VKB dostupná v listinné nebo elektronické podobě, komunikována v rámci povinné osoby, přiměřeně dostupná dotčeným stranám a řízena. Nadto musí být pravidelně přezkoumávána a aktualizována, chráněna z pohledu důvěrnosti, dostupnosti a integrity, a vedena tak, aby informace v ní obsažené byly úplné, čitelné, snadno identifikovatelné a snadno dohledatelné. Je přitom lhostejno, zda je bezpečnostní dokumentace vedena v jednom souhrnném dokumentu, v relativně samostatných dokumentech tvořících konzistentní celek nebo v samostatných a nezávisle uchovávaných dokumentech. Stěžejní je, aby ve výsledku vedla povinná osoba kompletní dokumentaci obsahující všechny podsložky stanovené přílohou č. 5 VKB a aby byla bezpečnostní dokumentace jako celek (tvořená jednotlivými dokumenty) **kompletní, přezkoumatelná, přehledná a dohledatelná**. Zároveň je žádoucí zajistit provázanost a koherenci jednotlivých dokumentů.

Stejně tak pokud se jedná o subjekty, které se např. teprve v nedávné době staly povinnými osobami a uvádí svou dosavadní bezpečnostní dokumentaci do souladu s požadavky VKB, není nezbytné, aby tyto osoby tvořily kompletně novou dokumentaci, naopak je možné dosavadní dokumentaci využít a aktualizovat ji o oblast kybernetické bezpečnosti podle požadavků ZKB a VKB.

Co se týče samotného obsahu politiky řízení dodavatelů, VKB stanovuje oblasti, které musí být nezbytně v dokumentaci obsaženy. Konkrétní podoba politiky je v dispozici povinné osoby a bude se odvíjet především od specifik konkrétní organizace a požadavků, které jsou na ni při její činnosti kladeny, zejména právními předpisy, akty nadřízených orgánů, pravidly koncernu apod. Optimálním řešením je mít v politikách zanesena kompletní pravidla, která se budou uplatňovat při řízení dodavatelů a rizik s nimi spojených, primárně tedy bezpečnostní pravidla upravená v ZKB a VKB a dále specifické požadavky na výběr dodavatele podle jiných právních předpisů. Přijatelným, a v praxi využívaným postupem, je vyhotovení samostatného dokumentu pro řízení dodavatelů podle ZKB a VKB, vedle něj bude vyhotoven samostatný dokument regulující procesní stránku výběru dodavatelů (typicky podle ZZVZ) a případně další doplňující dokumenty (např. obecné koncernové politiky).

2.1 Analýza dosavadního stavu

Samotné tvorbě politiky řízení dodavatelů by měla předcházet analýza dosavadního stavu, a to zejména za účelem zhodnocení, zda existující dokumentované procesy a smlouvy vyhovují požadavkům ZKB a VKB. Na základě této analýzy je možné určit, zda je potřeba pouze doplnit či upravit dílčí části procesu, příp. zda bude nutné jej definovat zcela od začátku. Dalším krokem by mělo být zhodnocení, zda by celková změna byla skutečným přínosem a nebylo by naopak vhodnější zachovat funkční části, i kdyby se jednalo pouze o dílčí část celkového procesu. Zejména v oblasti smluv je potřeba vyhodnotit, které části smluv naplňují požadavky kybernetické bezpečnosti a požadavky na řízení dodavatelů.

2.2 Nastavení procesu

Samotné nastavení procesu řízení dodavatelů souvisí s nastavením postupu v jednotlivých etapách životního cyklu řízení služeb:

a) Během definování předmětu plnění budoucí smlouvy je nezbytné provést hodnocení rizik souvisejících s předmětem plnění, jedná-li se o smlouvu na provoz, rozvoj nebo akvizici informačního systému, nákup hardware, software či služeb. Hodnocení rizik souvisejících s předmětem plnění je nezbytné zohlednit již v zadávací dokumentaci a následně ve smlouvě s dodavatelem.

b) Po definování předmětu plnění lze na základě veřejně dostupných zdrojů či průzkumu trhu odhadnout potenciální okruh dodavatelů a v daný okamžik realizovat hodnocení rizik souvisejících s potenciálními dodavateli a zohlednit výsledky hodnocení ve smlouvě či zadávací dokumentaci.

c) Je-li předmětem smlouvy provoz či rozvoj informačního systému, je nezbytné po uzavření smlouvy provést hodnocení rizik souvisejících s akvizicí nového informačního systému a provozem, které se realizuje společně s dodavatelem. Pokud bude vyhodnoceno riziko, stanovuje se způsob opatření k ošetření nebo zmírnění rizika a harmonogram vypořádání.

d) V průběhu plnění smlouvy by mělo docházet k pravidelnému hodnocení rizik ať již z důvodu zohledňování nově vydaných opatření NÚKIB, významných změn v provozním prostředí, organizačních nebo obchodních změnách prostředí dodavatele služeb nebo produktů, nebo jako pravidelné vyhodnocení stavu plnění smlouvy.

e) Po ukončení smluvního vztahu by mělo dojít ke konečnému vyhodnocení dodavatele, které může být využito pro další smluvní vztahy a veřejné zakázky.

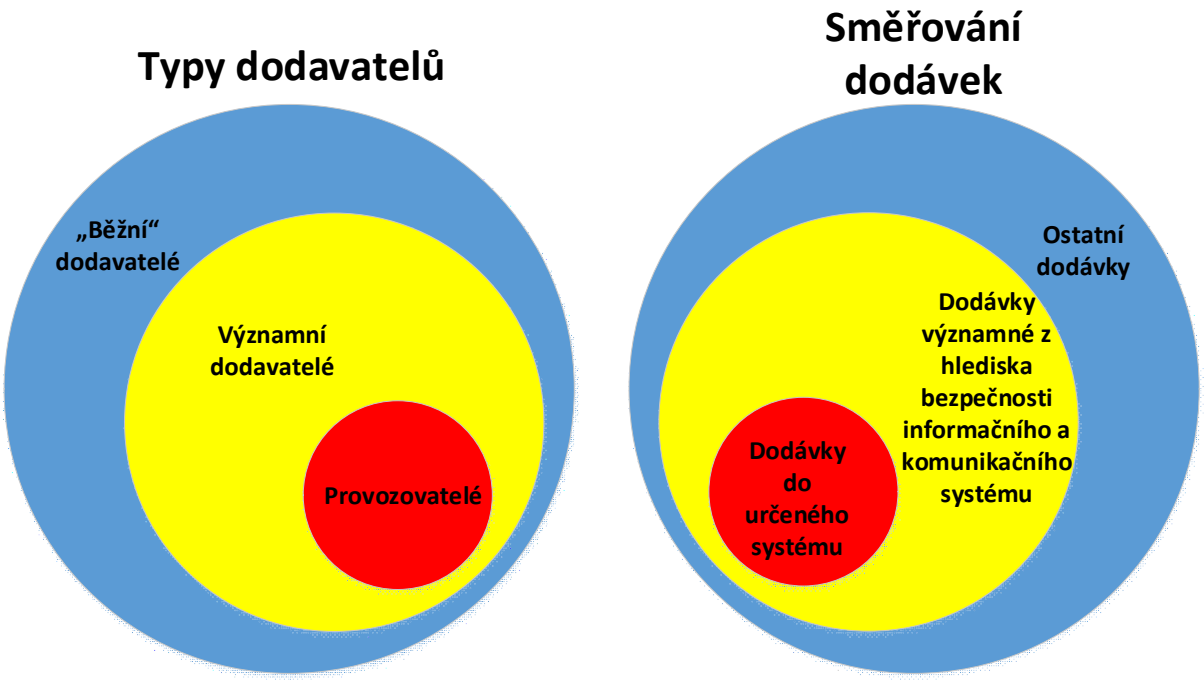
3 Typy dodavatelů a povinnosti s nimi související

VKB rozlišuje tři základní typy dodavatelů:

- „běžní“ dodavatelé,
- významní dodavatelé,
- provozovatelé (podmnožina významných dodavatelů).

Následující obrázek popisuje vztahy mezi jednotlivými typy dodavatelů a návaznost na typ dodávek, které tito dodavatelé poskytují.

V levé části jsou zobrazeny množiny dodavatelů a v nich znázorněny jednotlivé typy dodavatelů. V pravé části obrázku je pak zobrazena množina všech dodávek, které jsou shodným způsobem rozděleny na množiny dodávek zajišťovaných jednotlivými typy dodavatelů z levé části.



Obrázek 1: Schéma typů dodavatelů

Výše uvedené schéma je orientační, ne vždy je dodavatel dodávek do určeného systému automaticky provozovatelem. Tuto problematiku blíže rozvádí podpůrný materiál NÚKIB k provozovateli informačního nebo komunikačního systému, který se mj. věnuje právě rozlišení provozovatele systému a významného dodavatele.[2]

[2] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf.

3.1 Povinnosti související se všemi dodavateli

U všech svých dodavatelů povinná osoba musí:

- stanovit pravidla pro dodavatele zohledňující požadavky systému řízení bezpečnosti informací – § 8 odst. 1 písm. a) VKB,
- zpřístupnit dodavatelům v listinné nebo elektronické podobě relevantní bezpečnostní dokumentaci – § 8 odst. 1 písm. d) VKB,
- kontinuálně řídit rizika spojená s dodavateli – § 8 odst. 1 písm. e) VKB,
- stanovit způsob poučení dodavatele o jeho povinnostech a o bezpečnostní politice – § 9 odst. 1 písm. a) bod 1. VKB,
- stanovit způsob a formu vstupních a pravidelných školení pro dodavatele v souladu s plánem rozvoje bezpečnostního povědomí – § 9 odst. 1 písm. c) VKB,
- stanovit, jakým způsobem budou dodavatelé oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti – § 14 odst. 1 písm. f) VKB.

Dobrou praxí je zařazení dodavatele do evidence dodavatelů (vzor Příloha č. 1).

3.2 Povinnosti související s významným dodavatelem

Ve vztahu ke svým významných dodavatelů povinná osoba musí:

- řídit se všemi povinnostmi souvisejícími s dodavateli podle podkapitoly 3.1,
- zařadit významného dodavatele do evidence významných dodavatelů – § 8 odst. 1 písm. b) VKB (vzor Příloha č. 1), která obsahuje seznam všech významných dodavatelů, základní informace o smluvních vztazích s významnými dodavateli a informace o přístupnosti jednotlivých formulářů hodnocení významných dodavatelů (lze doporučit i pro evidenci dodavatelů, kteří nejsou identifikováni jako významní),
- prokazatelně písemně informovat významného dodavatele o jeho evidenci jako významného dodavatele – § 8 odst. 1 písm. c) VKB, prokazatelné písemné informování významného dodavatele je možné provést již ve smlouvě, nebo samostatným dokumentem (vzor je dostupný v podpůrném materiálu Provozovatel informačního nebo komunikačního systému[3]), a musí obsahovat identifikaci správce nebo provozovatele, identifikaci informačního nebo komunikačního systému, identifikaci významného dodavatele a obsah pravidel zohledňujících požadavky systému řízení bezpečnosti informací – § 8 odst. 3 VKB,
- zajistit soulad smluv uzavíraných s významnými dodavateli s požadavky uvedenými v příloze č. 7 VKB – § 8 odst. 1 písm. f) VKB,
- pravidelně přezkoumávat plnění smluv uzavřených s významnými dodavateli, a to včetně zavedených bezpečnostních opatření u poskytnutého plnění – § 8 odst. 1 písm. g) VKB,

[3] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf.

- provést v rámci výběrového řízení, příp. před uzavřením smlouvy hodnocení rizik souvisejících s plněním předmětu výběrového řízení – § 8 odst. 2 písm. a) VKB,
- stanovit v uzavíraných smlouvách způsob a úrovně realizace bezpečnostních opatření a určit obsah vzájemné odpovědnosti za zavádění a kontrolu bezpečnostních opatření – § 8 odst. 2 písm. b) VKB,
- provádět pravidelné hodnocení rizik – § 8 odst. 2 písm. c) VKB,
- v reakci na rizika a zjištěné nedostatky zajistit jejich řešení – § 8 odst. 2 písm. d) VKB.

3.3 Povinnosti související s provozovatelem informačního nebo komunikačního systému

3.3.1 Povinnosti správce

Ve vztahu k provozovateli informačního nebo komunikačního systému je správce tohoto systému povinen:

- řídit se všemi povinnostmi souvisejícími s dodavateli a významnými dodavateli uvedenými v podkapitolách 3.1 a 3.2,
- zařadit provozovatele do evidence významných dodavatelů – § 8 odst. 1 písm. b) VKB (vzor Příloha č. 1),
- prokazatelně písemně informovat provozovatele o jeho evidenci jako provozovatele – § 8 odst. 1 písm. c) VKB, prokazatelné písemné informování provozovatele je možné provést již ve smlouvě, nebo samostatným dokumentem (vzor je dostupný v podpůrném materiálu Provozovatel informačního nebo komunikačního systému[4]), a musí obsahovat identifikaci správce nebo provozovatele, identifikaci informačního nebo komunikačního systému, identifikaci významného dodavatele a obsah pravidel zohledňujících požadavky systému řízení bezpečnosti informací – § 8 odst. 3 VKB,
- dohodnout se na rozsahu plnění požadavků ZKB a VKB.

Dobrou praxí je informování provozovatele o povinnosti nahlásit kontaktní údaje formou uvedenou v § 34 VKB.

3.3.2 Povinnosti provozovatele

Identifikovaný a informovaný provozovatel je povinen plnit povinnosti podle ZKB a VKB. V rámci plnění se bude jednat především o povinnosti:

- hlásit kontaktní údaje NÚKIB – § 8 odst. 4 VKB,
- zavádět bezpečnostní opatření požadovaná správcem – § 4 odst. 2 ZKB,
- hlásit kybernetické bezpečnostní incidenty – § 8 odst. 1 ZKB,
- provádět opatření podle § 11 ZKB.

[4] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf.

Mezi další povinnosti patří např. povinnost předávat správci data, provozní údaje a informace na jeho vyžádání – § 6a odst. 2 ZKB, při ukončení spolupráce – § 6a odst. 3 ZKB, a na základě rozhodnutí vydaného NÚKIB – § 15a ZKB.

Dále má provozovatel povinnost provádět audit kybernetické bezpečnosti a jeho výsledky předkládat správci – § 16 VKB.

S identifikovaným a informovaným provozovatelem je nutné si dohodnout rozsah zavádění a provádění bezpečnostních opatření, a to tak, jak je to nezbytné pro zajištění kybernetické bezpečnosti informačního nebo komunikačního systému. V podrobnostech se problematice povinností provozovatelů informačních a komunikačních systémů věnuje podpůrný materiál NÚKIB k provozovateli informačního nebo komunikačního systému[5].

3.4 Stanovení pravidel bezpečnosti pro dodavatele zohledňující požadavky systému řízení bezpečnosti informací

Pravidla bezpečnosti pro dodavatele by měla být stanovena ve formě dokumentace upravené speciálně pro dodavatele, která obsahuje všechny relevantní informace.

Některé organizace nemají speciální bezpečnostní pravidla pro dodavatele, ale seznamují je s relevantními bezpečnostními pravidly obsaženými v interních politikách, které se netýkají pouze dodavatelů, ale např. také vlastních zaměstnanců. Mohou to být dokumenty jako Politika řízení přístupů, Řízení změn, Politika bezpečného používání kryptografické ochrany, Politika zálohování, obnovy a dlouhodobého ukládání, Akvizice, vývoj a údržba atd.

Oba způsoby jsou přípustné a záleží na samotné organizaci, co je pro ni vhodnější. Podstatné však je, aby tyto požadavky a podmínky byly pro dodavatele závazné, a to i v případě, že dodavatel vůči dodávanému systému uplatňuje vlastní pravidla bezpečnosti.

Z hlediska kybernetické bezpečnosti je vhodnější vytvoření speciální dokumentace pro dodavatele, a to z toho důvodu, že dodavatelé v takovém případě nemají přístup k interním informacím organizace, nejsou zahlcováni množstvím informací, které pro ně nejsou relevantní (pokud jde pouze o interní postupy), nebo množstvím dokumentů, ve kterých sami musejí vyhledávat informace, které se jich týkají.

3.5 Způsob a forma seznámení dodavatele s pravidly

V režimu VZ zadavatel (objednatel) jako součást zadávací dokumentace veřejné zakázky předloží potenciálním dodavatelům obchodní a platební podmínky plnění veřejné zakázky (např. ve formě závazného textu návrhu smlouvy nebo jiného samostatného dokumentu), jehož znění dodavatelé nebudou oprávněni měnit ani doplňovat (s výjimkou výslovně označených míst). Součástí zadávací dokumentace musí být informování o významnosti dodavatele, tedy zda bude dodavatel

[5] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf.

provozovatelem, významným dodavatelem nebo dodavatelem (aby měli dodavatelé kompletní informace o předmětu plnění a rozsahu jejich povinností plynoucích jak ze smlouvy, tak ze ZKB).

Mimo režim VZ objednatel specifikuje požadavky na předmět plnění, včetně vyhláškou požadovaných ustanovení, zapracuje je do návrhu smlouvy (nebo do jiného samostatného dokumentu) a ten následně předloží dodavateli. Níže je zobrazen zjednodušený proces tvorby ICT smlouvy.

V případě, že dodavatel uplatňuje vlastní bezpečnostní politiku, objednatel ověří, zda tato politika odpovídá jeho požadavkům a příp. navrhne příslušné změny prostřednictvím smluvního návrhu.

Obrázek 2: Proces tvorby ICT smlouvy

4 Životní cyklus dodavatelského vztahu

Hodnocení dodavatelů a rizik s nimi spojených by mělo probíhat v průběhu celého životního cyklu dodavatelského vztahu, tzn. ve fázi formulace požadavků na předmět smlouvy, výběru dodavatele, ve fázi plnění smluvního vztahu a po jeho skončení.

Životní cyklus dodavatelského vztahu je graficky znázorněn v Příloze č. 2.

Níže uvedené schéma zohledňuje specifika **zadávacího řízení** u smluv s jednorázovým plněním:

Fáze 1: Vymezení předmětu veřejné zakázky

Fáze 2: Stanovení vazeb na jiné systémy

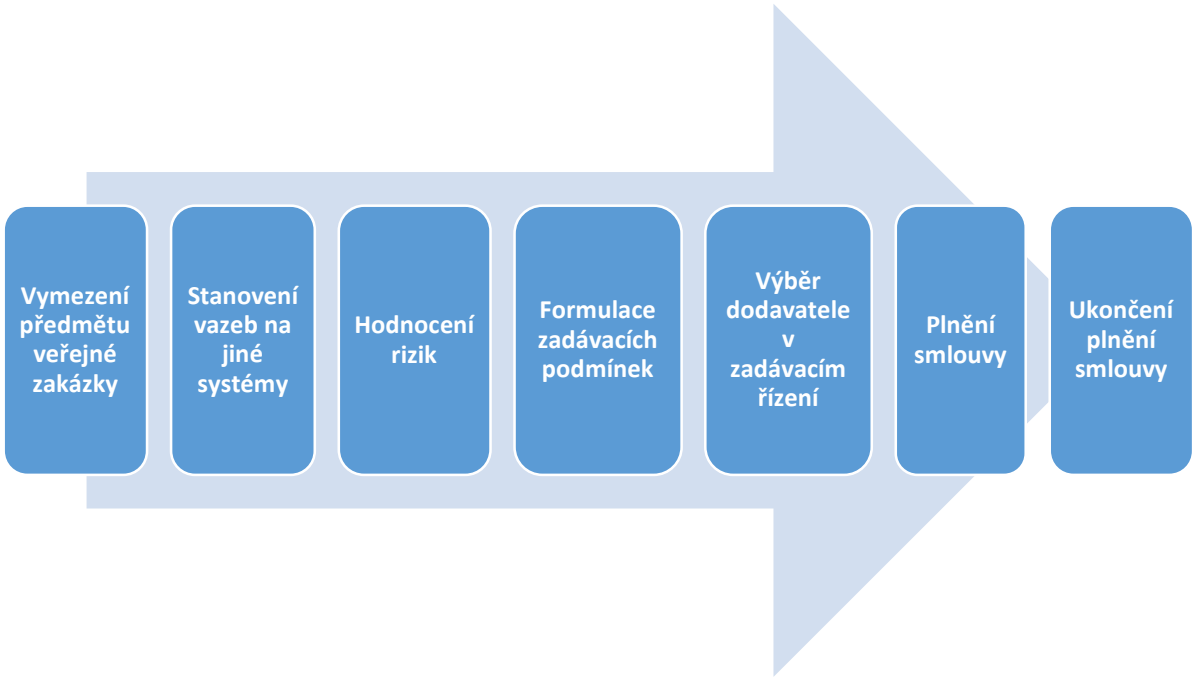
Fáze 3: Hodnocení rizik

Fáze 4: Formulace zadávacích podmínek

Fáze 5: Výběr dodavatele v zadávacím řízení k veřejné zakázce

Fáze 6: Plnění smlouvy

Fáze 7: Ukončení plnění smlouvy



Obrázek 3: Schéma životního cyklu dodavatelského vztahu v zadávacím řízení

Co se týče specifik hodnocení rizik v průběhu smluvního vztahu, blíže se mu věnuje podpůrný materiál Průvodce řízením dodavatelů ve vztahu k hodnocení rizik KB[6].

[6] Materiál je dostupný zde: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

5 Obsahová doporučení pro politiku řízení dodavatelů

Ačkoli se konkrétní podoba jednotlivých politik řízení dodavatelů bude napříč odvětvími a organizacemi lišit, lze v návaznosti na požadavky ZKB a VKB za současného zohlednění zkušeností z praxe stanovit základní pravidla pro stanovení obsahu jednotlivých podkapitol, které mají být v politice řízení dodavatelů obsaženy.

Doporučení vycházejí primárně z požadavků na zajištění kybernetické bezpečnosti, nicméně tam, kde je to relevantní, jsou výslovně uvedena a zohledněna též specifika a požadavky ZZVZ. Vlivy dalších právních předpisů nebo interních aktů jednotlivých spoluautorů nebyly pro účely tohoto materiálu zvažovány.

Níže uvedená doporučení jsou založena na zkušenostech spoluautorů tohoto dokumentu zejména s tvorbou politik ve vlastních strukturách, resp. na zkušenostech z kontrolní činnosti NÚKIB ve vztahu k povinným osobám a dozorové činnosti Ministerstva vnitra a Ministerstva financí ve vztahu k jejich podřízeným organizacím.

Struktura následujících podkapitol kopíruje strukturu bodu 1.4 přílohy č. 5 k VKB, která stanovuje obsahové náležitosti politiky řízení dodavatelů, tzn. pokryty jsou následující oblasti:

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik souvisejících s dodavateli.

c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

e) Pravidla pro hodnocení dodavatelů.

5.1 Pravidla a principy pro výběr dodavatelů

V rámci výběru dodavatelů poptávaného plnění jsou zohledňovány identifikované bezpečnostní potřeby v souladu s interními a právními předpisy.

Pravidla pro výběr dodavatele by měla zohledňovat základní bezpečnostní požadavky, resp. způsob jejich určení, hodnocení rizik souvisejících s dodavatelem a stanovenou úroveň zabezpečení. Významnými faktory pro určení konkrétní úrovně požadavků na dodavatele musí být především:

- charakter informačního nebo komunikačního systému, do nějž bude dodavatel svým plněním zasahovat (tedy zda jde o kritickou informační infrastrukturu, informační systém základní služby nebo významný informační systém),
- charakter dodavatele, tedy zda jde o „běžného“ dodavatele, významného dodavatele nebo provozovatele systému, příp. specifika vztahu dodavatele k systému, do kterého bude svým plněním zasahovat.

Při tvorbě pravidel budou zohledněny i relevantní vnitřní předpisy organizace nebo závazné pokyny nadřízených subjektů.

Výběr dodavatelů by měl být založen na výsledcích hodnocení rizik spojených s předmětem výběrového řízení a rizik souvisejících s významnými dodavateli (tzv. předsmluvní hodnocení rizik podle § 8 odst. 2 písm. a) VKB).

U zadavatelů **v zadávacím řízení** budou pravidla pro výběr dodavatele determinována rozsahem oprávnění a povinností vyvěrajících ze ZZVZ. Zadavatel při postupu podle ZZVZ nesmí vznést jiné kvalifikační požadavky na osobu dodavatele (příp. poddodavatele), než které mu ZZVZ výslovně umožňuje. Případné zbylé požadavky je třeba přetransformovat na požadavky na předmět plnění a nevázat je na osobu dodavatele. Zadáváním veřejných zakázek v oblasti ICT se zabývá další podpůrný materiál NÚKIB[7].

Identifikované bezpečnostní potřeby jsou formou jednotlivých požadavků zahrnuty do smluv, resp. do zadávacích podmínek, pokud je dodavatel vybírán v zadávacím řízení. Míra podrobnosti iniciačních zadávacích podmínek bude v takovém případě závislá na zvoleném druhu zadávacího řízení).

V rámci spolupráce s dodavatelem je vhodné, aby byl určen odpovědný zaměstnanec pro každého jednotlivého dodavatele, tzv. **zaměstnanec odpovědný za smluvní vztah**. Tento zaměstnanec musí určit a řídit všechny odborné záležitosti související s předmětnými dodávkami nebo službami, měl by tedy disponovat odborným povědomím o věcném plnění a zároveň i případnou právní podporou. Nedílnou součástí těchto aktivit je i zajištění úrovně bezpečnosti informací. Prakticky by tento zaměstnance měl působit i jako koordinátor spolupráce jednotlivých oddělení při tvorbě zadávací dokumentace.

5.2 Pravidla pro hodnocení rizik souvisejících s dodavateli

Hodnocení rizik souvisejících s dodavateli je součástí specifikace předmětu plnění a přípravy zadávací dokumentace v zadávacím řízení. Toto hodnocení rizik musí být zpracováno jednotnou metodikou, příp. metodikou k tomu určenou a standardně používanou. Pro ilustraci slouží vzor registru rizik v Příloze č. 3.

Předmětem hodnocení rizik souvisejících s dodavateli jsou i vydaná opatření NÚKIB.

Za provedení hodnocení rizik souvisejících s dodavateli odpovídá obvykle zaměstnanec odpovědný za smluvní vztah v součinnosti s garantem primárního aktiva a garantem podpůrného aktiva. Pokud se na hodnocení rizik nepodílí přímo i manažer kybernetické bezpečnosti, měl by o něm být informován.

[7] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Zadavani_verejnych_zakazek_v_oblasti_ICT_a_kyberneticka_bezpecnost_v1.3.pdf.

Podrobněji se hodnocení rizik ve vztahu k veřejným zakázkám věnuje podpůrný materiál Průvodce řízením dodavatelů ve vztahu k hodnocení rizik KB[8].

5.2.1 Pravidla pro hodnocení rizik souvisejících s předmětem plnění

Riziky souvisejícími s plněním předmětu výběrového řízení ve smyslu § 8 odst. 2 písm. a) VKB je třeba rozumět nejen rizika spojená se samotným předmětem plnění, nýbrž i rizika spojená s dodavatelem poptávaného plnění. Povinnost provádět toto tzv. předsmluvní hodnocení rizik se uplatní ve vztahu k významným dodavatelům (tedy i provozovatelům), nicméně je samozřejmě možné aplikovat tento postup i ve vztahu ke všem ostatním dodavatelům, pokud to odůvodňují potřeby povinné osoby.

U každého poptávaného plnění musí být určena jeho významnost, tedy zda bude jeho dodavatel označen jako provozovatel, významný dodavatel nebo běžný dodavatel. Toto určení by měla provést osoba odpovědná za konkrétní smluvní vztah.

Pravidla pro hodnocení rizik souvisejících s předmětem plnění (tj. i s dodavateli poptávaného plnění) by měla korespondovat se standardními postupy pro hodnocení rizik spojených s již implementovaným plněním. Lze však akceptovat i situaci, kdy jsou pravidla pro tzv. předsmluvní hodnocení rizik uzpůsobena specifikům dané situace, kdy povinná osoba mnohdy nemusí disponovat kompletními informacemi o předmětu plnění nebo o jeho dodavateli (zvláště v situacích, kdy je dodavatel vybírán v zadávacím řízení, u něhož je třeba stanovit zadávací podmínky předem a v němž již není možné reagovat na vývoj situace, tedy zejm. v otevřeném a užším řízení). V každém případě je třeba, aby byla pravidla nastavena předem, transparentně, smysluplně a pokud možno univerzálně, tedy aby nebyla neodůvodněně přizpůsobována jednotlivým výběrovým řízením.

Dále je potřeba, aby pravidla pro hodnocení rizik souvisejících s předmětem plnění a dodavateli odpovídala požadavkům VKB, aby bylo hodnocení rizik prováděno přiměřeně podle přílohy č. 2 k VKB.

V rámci hodnocení rizik je možné využít přílohu č. 3 k VKB, která obsahuje vybrané kategorie hrozeb a zranitelností. Výsledný a konkrétní organizaci uzpůsobený katalog hrozeb a zranitelností (potažmo kompletních rizik) má představovat znalostní bázi, která je na základě zkušeností pravidelně doplňována a slouží jako pomůcka pro osobu zodpovědnou za hodnocení rizik. Za údržbu katalogu hrozeb, zranitelností a rizik je zpravidla odpovědný manažer kybernetické bezpečnosti, na obsahu se podílejí všechny osoby, které musí provádět hodnocení rizik související s řízením dodavatelů. Výsledný katalog rizik by měl obsahovat konkrétní rizika využitelná v organizaci povinné osoby, stejně jako rizika specifická právě pro oblast, v níž organizace působí.

5.2.2 Postup hodnocení rizik před uzavřením smlouvy u významných dodavatelů

Ustanovení § 8 odst. 2 písm. a) VKB požaduje, aby bylo v rámci výběrového řízení a před uzavřením smlouvy provedeno hodnocení rizik souvisejících s plněním předmětu výběrového

[8] Materiál je dostupný zde: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

řízení. Jde o pravidlo obecně aplikovatelné na všechny povinné osoby, ať už jde o zadavatele podle ZZVZ, či nikoli. Konkrétní postup je tedy třeba přizpůsobit specifickým skutkovým okolnostem. Pokud jde o osobu nespadající do působnosti ZZVZ, je možné hodnocení rizik provést skutečně až před podpisem smlouvy, pokud to konkrétní okolnosti uzavírání smluvního vztahu nevylučují. Pokud jde o osobu spadající do působnosti ZZVZ, která nepostupuje na základě některé ze zákonných výjimek, je potřeba konkrétní postup přizpůsobit druhu zadávacího řízení, který byl pro výběr dodavatele zvolen. U transparentních druhů zadávacího řízení bude nutné provést kompletní předsmluvní hodnocení rizik již ve fázi tvorby zadávacích podmínek, neboť ty již nemohou být po uplynutí lhůty pro podání nabídek měněny. U méně transparentních druhů řízení (např. jednacího řízení) je možné provést hodnocení rizik až v pozdějších fázích zadávacího řízení.

Před uzavřením smlouvy musí být provedeno hodnocení rizik s ohledem na konkrétní předmět plnění smlouvy. Hodnocení rizik je prováděno podle k tomu určené metodiky pro identifikaci a hodnocení aktiv a rizik, vytvořené podle § 4 VKB a § 5 VKB, s ohledem na důležitost dodávky.

V případě, že není k dispozici dostatek informací o předmětu veřejné zakázky nebo o jejích potenciálních dodavatelích, je hodnocení rizik provedeno alespoň na obecné úrovni (VKB nedává na výběr, zda bude hodnocení provedeno, či nikoli). Výstupem může být identifikace potenciálně rizikových míst, na která je potřeba se zaměřit, aby nevznikl problém. V rámci hodnocení rizik spojených s dodavateli je možné využít jednak informace univerzálně platné pro jakékoli dodavatele, jednak informace vztahující se ke konkrétním dodavatelům. Informace o potenciálních dodavatelích poptávaného plnění je možné získat zejména v rámci průzkumu trhu realizovaného před zahájením výběrového řízení (případně v průběhu výběrového řízení, pokud to situace umožňuje, v případě zadávacího řízení půjde především o jednací řízení, příp. zadání veřejné zakázky mimo zadávací řízení). Otevřenost výběrového řízení a šíře okruhu potenciálních dodavatelů povinnou osobu nezbavuje povinnosti hodnotit rizika spojená s potenciálními dodavateli ještě před uzavřením smlouvy.

Při hodnocení rizik jsou hodnocena inherentní rizika, resp. v případě již zavedených bezpečnostních opatření i tato opatření, a následně jsou zohledněna bezpečnostní opatření, která vyplývají z bezpečnostních pravidel pro dodavatele, zohledněna relevantní ustanovení uvedená v příloze č. 7 k VKB a doplněna bezpečnostní opatření, která se vztahují ke konkrétnímu plnění tak, aby výsledné hodnoty identifikovaných rizik byly z pohledu zavedených politik akceptovatelné. **Zvolená bezpečnostní opatření musí být zohledněna v uzavírané smlouvě.**

V závislosti na způsobu výběru dodavatele je nutné zvolená bezpečnostní opatření buďto zahrnout již do podmínek výběrového řízení, nebo je zohlednit či upravit až v průběhu řízení (při zohlednění dalších informací, které povinná osoba v průběhu jednání s dodavateli získala). V takovém případě dojde následně po výběru dodavatele k porovnání hodnocení dodavatele v jednotlivých oblastech podle kapitoly 4.1 s hodnocením rizik dodávaného plnění. Na základě výsledku tohoto porovnání mohou být přijata dodatečná bezpečnostní opatření, která musí být zohledněna ve smlouvě.

Za hodnocení rizik a výběr relevantních bezpečnostních opatření zpravidla odpovídá zaměstnanec odpovědný za smluvní vztah a architekt kybernetické bezpečnosti. V případě, že organizace nemá obsazenou roli architekta kybernetické bezpečnosti, mělo by se jednat o zaměstnance, který má v náplni práce navrhování a implementaci bezpečnostních opatření.

5.2.3 Minimální skutečnosti posuzované při hodnocení rizik souvisejících s předmětem plnění

Při posuzování hodnocení rizik je nutné zohlednit minimálně následující oblasti:

- rozsah prostředků a informací, ke kterým bude umožněn přístup,
- hodnota, citlivost a kritičnost primárních aktiv, ke kterým bude umožněn přístup,
- typ požadovaného přístupu:
  - fyzický – budovy, kanceláře, místnosti s počítači, spisovny,
  - logický – data, informační systémy, aplikace,
- rozsah přidělených privilegovaných oprávnění,
- realizovaná opatření bezpečnosti informací a jejich stav,
- formy výběru a určení osob, které se budou podílet na plnění závazků, a způsoby jejich seznámení s bezpečnostními politikami a pravidly,
- postupy pro řešení bezpečnostních incidentů,
- zákonné, smluvní a jiné požadavky, které ovlivňují vztah s dodavatelem,
- použití poddodavatele dodavatelem pro zajištění dodávky služby,
- vliv rizik na zájmy povinné osoby,
- riziko související s upozorněními vládního CERT, varováními, ochrannými a reaktivními opatřeními či jinými instrumenty využívanými NÚKIB pro zvýšení bezpečnosti informací,
- další relevantní rizika související s předmětem výběrového řízení.

5.2.4 Postup podle ZZVZ

Při výběru dodavatele v otevřeném řízení podle ZZVZ je v zásadě možné postupovat dvěma způsoby:

a) hodnotit rizika spojená s předmětem plnění (a tedy i s jeho potenciálními dodavateli) před zahájením samotného řízení, ve fázi tvorby zadávacích podmínek, a zvolená bezpečnostní opatření zahrnout do zadávacích podmínek a případného návrhu smlouvy, nebo

b) hodnotit rizika spojená s předmětem plnění (a tedy i s jeho potenciálními dodavateli) ve fázi hodnocení nabídek (např. pokud je bezpečnost jedním z kritérií kvality).

Možná je i kombinace výše uvedených postupů, pro inspiraci lze využít podpůrný materiál Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost[9].

[9] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Zadavani_verejnych_zakazek_v_oblasti_ICT_a_kyberneticka_bezpecnost_v1.3.pdf.

Konkrétní podoba předsmluvního hodnocení rizik je odpovědností povinné osoby. Pokud bude toto hodnocení provedeno příliš obecně, bez vynaložení přiměřeného úsilí pro získání dostatku relevantních informací o rizicích souvisejících s předmětem plnění a potenciálními dodavateli, výsledkem bude uzavření smlouvy neodpovídající požadavkům ZKB a VKB. Uvedení smlouvy do souladu s požadavky ZKB bude následně odpovědností povinné osoby.

5.2.5 Postup pravidelného hodnocení rizik souvisejících s předmětem plnění během smluvního vztahu

Po uzavření smluvního vztahu, resp. po implementaci dodaného plnění, je hodnocení rizik dodávky zapracováno do standardního procesu hodnocení aktiv a rizik, který musí zohledňovat mj. případné vydání varování, reaktivních a ochranných opatření a výsledky kontrol zavedených bezpečnostních opatření. Tento proces probíhá podle interní metodiky organizace. Dodávka je včleněna do informačního nebo komunikačního systému, u kterého standardně probíhá hodnocení aktiv a rizik podle § 4 a § 5 VKB.

Za promítnutí rizik spojených s dodávkou do standardního hodnocení aktiv a rizik v rámci organizace odpovídá obvykle manažer kybernetické bezpečnosti.

5.2.6 Výsledek hodnocení rizik souvisejících s předmětem plnění

Výsledky hodnocení rizik souvisejících s předmětem plnění a dodavateli jsou součástí specifikace plnění, příp. zadávací dokumentace, kde jsou uvedena příslušná bezpečnostní opatření, a to ještě před uzavřením smlouvy.

Výsledky hodnocení rizik dodavatelů a příslušná opatření u již uzavřených smluvních vztahů a které ovlivní primární nebo podpůrná aktiva nesmí být v rozporu s uzavřenou smlouvou či veřejnou zakázkou, na jejímž základě byla tato smlouva uzavřena. Pokud jsou identifikovány rozpory, přichází v úvahu:

a) prověřit, zda jsou všechny smluvní strany ochotné uzavřít příslušný dodatek smlouvy,

b) znovu projednat smluvní vztah v režimu změn podle § 222 ZZVZ, neboť se jedná o změnu smlouvy, jejíž potřeba vznikla v důsledku okolností, které zadavatel jednající s náležitou péčí nemohl předvídat, ve smyslu § 222 odst. 6 písm. a) ZZVZ; nemožnost předvídat takovou změnu je dána nemožností předvídat vývoj v oblasti legislativního procesu,

c) pokud nebude nalezena shoda na uzavření dodatku smlouvy, prostřednictvím čerpání kapacit dodavatele zajistit všechny povinnosti dodavatele, u nichž je to možné (např. povinnost poskytovat zadavateli součinnost při plnění jeho povinností podle ZKB a jeho prováděcích předpisů, povinnost vypracovat a předložit havarijní plány apod.), pokud tato možnost není v uzavřené smlouvě dána nebo je již vyčerpána jinými potřebami, zohlednit všechny chybějící povinnosti v hodnocení rizik, příp. přijmout náhradní opatření.

5.2.7 Ukončení smluvního vztahu u významných dodavatelů

Při ukončení smluvního vztahu významného dodavatele se zpravidla jedná o významnou změnu a následuje odpovídající postup, který zahrnuje také aktualizaci hodnocení rizik.

Postup v případě, že nastane významná změna, popisuje interní dokument organizace podle § 11 VKB a její přílohy č. 5: 1.21. Politika řízení změn.

5.3 Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti

Předně, obsahem smlouvy (příp. jiného závazného dokumentu smluvních stran) musí být informace o tom, že smlouva se týká informačního nebo komunikačního systému spadajícího do působnosti ZKB. Současně je vhodné, aby již v těle smlouvy byla obsažena informace o tom, zda je dodavatel významným dodavatelem, příp. provozovatelem systému.

Ve smlouvě by měla být v co největších podrobnostech popsána jednotlivá práva a povinnosti smluvních stran co do způsobů realizace relevantních bezpečnostních opatření podle § 5 ZKB a určena odpovědnost za řádné plnění jednotlivých bezpečnostních opatření. Obecné deklarace v tom smyslu, že dodavatel je odpovědný za dodržování ZKB a VKB bez další konkretizace, jsou nedostatečné.

V otázce rozložení odpovědnosti za plnění zákonných povinností mezi správce systému a provozovatele lze odkázat na podpůrný materiál NÚKIB k provozovateli informačního nebo komunikačního systému[10].

Smlouva s dodavatelem dále obsahuje popis úrovně služeb (tzv. SLA). Pro konkrétní případ se stanovují takové parametry úrovně služeb, které zohlední povahu plnění smlouvy.

Smlouva by měla dále obsahovat:

- vymezení úrovně poskytovaných služeb,
- způsob komunikace pro řízení kybernetických bezpečnostních událostí a incidentů,
- způsob a úroveň realizace jednotlivých bezpečnostních opatření,
- podmínky výkonu kontrolní činnosti ze strany organizace zaměřené na dodržování stanovených bezpečnostních opatření dodavatelem,
- povinnost dodavatele realizovat nápravná opatření z kontrolní činnosti organizace,
- určení vzájemné smluvní odpovědnosti v oblasti kybernetické bezpečnosti,
- výši sankcí za porušení povinností v oblasti kybernetické bezpečnosti,
- pravidla náhrady škody,
- pravidla pro řízení dokumentace,
- pravidla při ukončení smluvního vztahu (tzv. exit plan).

[10] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf.

Požadavky na obsah smluv s významnými dodavateli jsou uvedeny v příloze č. 7 VKB, pro ostatní dodavatele se jedná o doporučená ustanovení. Tyto požadavky jsou detailněji vyloženy v podpůrném materiálu Požadavky na smlouvy s dodavateli[11].

Následující výčet uvádí hlavní oblasti, které mohou být pro objednatele při identifikaci jeho požadavků na smlouvy ICT klíčové. Oblasti zvýrazněné podtržením je do smlouvy potřeba zahrnout vždy, pokud jde o **významného dodavatele a provozovatele** podle VKB a pokud je to relevantní u dané zakázky. Ostatní uvedené oblasti je doporučeno vzít s ohledem na snahu posílit pozici objednatele alespoň v úvahu.

Předmět zakázky:

- detailní specifikace rozsahu a úrovně požadovaného předmětu plnění,
- určení místa a času požadovaného plnění,
- stanovení časového rámce, ve kterém bude plnění poskytováno,
- specifikace funkcionality předmětu plnění,
- stanovení počtu uživatelů požadujících předmět plnění,
- specifikace předmětného hardwaru a softwaru,
- specifikace vývoje a procesů řízení změn,
- nastavení úrovně dostupnosti systémů a aplikací,
- nastavení integrity zpracování,
- nastavení rozhraní s ostatními systémy.

Service Level Agreement (SLA):

- popis provozu služby, včetně údržby a servisních služeb,
- dostupnost systémů (včetně vyhodnocovacího období),
- úrovně údržby, doplňovací cyklus,
- reakční časy (do kdy je nutné zahájit řešení problému),
- čas řešení problémů (RTO – doba, do které je nutné obnovit provoz),
- garantovaná doba dostupnosti,
- nejdelší doba výpadku,
- termíny a časy fungování systémů a podpory,
- klíčové rizikové ukazatele týkající se důvěrnosti, dostupnosti a integrity informací,
- klíčové rizikové ukazatele týkající se činností dodavatele, jež mají nebo mohou mít dopad na organizaci,
- frekvence monitoringu a hlášení,
- postup v případě porušení výše uvedeného (eskalační proces), pokuty a sankce.

[11] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Vyklad_pozadavku_na_smlouvy_s_dodavateli_v1.2.pdf.

Bezpečnost:

- stanovení úrovně bezpečnosti informací z pohledu důvěrnosti, dostupnosti a integrity,
- určení způsobu a výše úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel,
- stanovení ochrany systémů a informačních aktiv prostřednictvím obnovy záloh, plánování pro případy nepředvídatelných událostí nebo propouštění,
- ustanovení o povinnosti dodavatele informovat objednatele o incidentech souvisejících s plněním smlouvy,
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky objednatele nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele objednatelem,
- monitoring aktiv a souvisejících dat, odezva (objednatele i dodavatele) a postupy oznamování (rutinního i incidentů),
- ekonomické spolehlivosti dodavatele,
- přístupu dodavatele k informacím objednatele, které jsou přenášeny prostřednictvím jejich komunikačních systémů a aplikací,
- definování a úpravy systému schvalování pro případy poddodávek prováděných třetími stranami,
- ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,
- povinnost dodavatele informovat povinnou osobu a způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy.

Komunikace:

- rozvržení systému komunikace mezi objednatelem a dodavatelem,
- implementace ustanovení o součinnosti, i s případnými sankcemi při neposkytnutí součinnosti.

Data:

- určení vlastnictví dat a oprávnění užívat data,
- specifikace vlastnictví informačních aktiv, včetně dat a doménových jmen,
- doba uchování zálohovaných dat organizace,
- ochrana přístupu uživatele k úložišti dat (popisuje mechanismy používané k ochraně pověření uživatele pro přístup k službám),
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat.

Záruky a odpovědnost:

- zavedení záruk dodavatele za kvalitu jím nebo třetí stranou poskytované služby,

- odpovědnosti za design, implementaci, výkonnost a monitoring kontroly,
- odpovědnosti za data, ochranu osobních údajů a soukromí,
- odpovědnosti za systém, komunikaci, operační systém, pomocný software, data a kontrolu přístupů do aplikačního softwaru a jejich správu,
- ustanovení o způsobu převzetí smluv s třetími stranami.

Právo na audit:

- kdo může vykonávat audit (zda např. zaměstnanec objednatele, kdokoliv, kdo je zmocněn objednatelem, nebo případně jiný subjekt),
- jak často se může audit opakovat a délka jeho trvání,
- náklady na audit a jejich hrazení,
- možnost setkat se s pracovníky interního auditu dodavatele a přezkoumat jejich auditní práci a výstupy auditu,
- oznámení doby provedení auditu a způsob tohoto oznámení,
- požadavky na dokumentaci.

Přezkoumávání smlouvy:

- ustanovení o pravidelném přezkoumávání předmětu smlouvy v souladu s aktuálními požadavky a z toho vyplývajících změn smlouvy.

Řízení změn:

- ustanovení o pravidlech schvalování změn obsahu smlouvy,
- stanovení přezkumu možných dopadů změn (např. prostřednictvím hodnocení rizik), akceptačního procesu (jakým způsobem je změna přijata), testování před nasazením do provozu, promítnutí do bezpečnostních politik, dokumentování změny, možnost navrácení do původního stavu apod.,
- povinnost dodavatele informovat objednatele o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, případě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem.

Právo duševního vlastnictví:

- ustanovení o autorství programového (zdrojového) kódu, popřípadě o programových licencích.

Mlčenlivost (NDA):

- ustanovení o zachování mlčenlivosti (důvěrnosti) informací souvisejících se smlouvou.

Soulad s právními předpisy:

- ustanovení o souladu smluv s obecně závaznými právními předpisy,

- postup v případě významných legislativních změn a způsob, jakým bude těmto požadavkům smlouva přizpůsobena.

Ukončení smlouvy a řešení sporů:

- okolnosti, za kterých může být smlouva ukončena,
- smluvní pokuty v případě ukončení za jiných než stanovených okolností,
- lhůty, ve kterých je potřeba takové ukončení smlouvy provést,
- podmínky pro obnovení smlouvy, včetně vyjednávacích procesů,
- prověření a odsouhlasení změn smlouvy a souvisejících dokumentů (např. SLA),
- specifikaci podmínek ukončení smlouvy z pohledu bezpečnosti (např. přechodné období při ukončení spolupráce, migrace dat, pravidla předání dat a informací, formát předávaných dat, likvidace předaných dat nebo finanční aspekty předání dat),
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (např. zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,
- ustanovení o sankcích za porušení povinností.

5.4 Pravidla pro provádění kontroly zavedení bezpečnostních opatření

Kontrola zavedení a dodržování bezpečnostních opatření dodavatelem je součástí hodnocení rizik dodavatelů.

Mezi kontrolní mechanismy patří:

- bezpečnostní audit u dodavatele před uzavřením smluvního vztahu,
- bezpečnostní audit u dodavatele po implementaci požadovaných bezpečnostních opatření,
- výkon plánovaných nebo nahodilých kontrol,
- následné kontroly k ověření realizace nápravných opatření,
- sledování dodržovaní smluvně stanovené úrovně služeb.

5.4.1 Kontrola v průběhu smlouvy

U uzavřených smluv musí být pravidelně prováděna kontrola bezpečnostních opatření prostřednictvím přezkoumávání plnění smluv v rozsahu dodržování požadavků na bezpečnostní opatření, a to:

- u významného dodavatele alespoň jednou za půl roku (dobrá praxe),
- u dodavatele alespoň jednou za rok (dobrá praxe).

V průběhu trvání smluvního vztahu je průběžně kontrolováno a monitorováno jeho plnění přiměřeně s ohledem na důležitost dodávky. Za přezkoumávání je odpovědný obvykle zaměstnanec odpovědný za smluvní vztah a auditor kybernetické bezpečnosti.

Předmětem kontroly bude zejména:

- zajištění důvěrnosti, dostupnosti a integrity informací,
- postupy předávání informací třetím stranám,
- dodržování podmínek SLA,
- vyhodnocování dodržování SLA z pohledu dodavatele,
- aktuálnosti jmenného seznamu zaměstnanců dodavatele, kteří budou přistupovat k datům nebo službám odběratele, včetně způsobu seznámení těchto zaměstnanců s bezpečnostními pravidly,
- výsledky spojené s monitorováním výkonnosti, kvality a bezpečnosti služeb ICT a řídicích systémů a míry plnění dohody o bezpečnosti služby,
- přezkoumání zpráv o službách poskytovaných dodavatelem a výsledky pravidelných setkání s dodavatelem,
- výsledky auditů, které se k danému dodavateli vztahují a přístup dodavatele k řešení nálezů,
- výsledky řešení kybernetických bezpečnostních incidentů, přístup dodavatele k řízení kybernetických bezpečnostních incidentů a stav opatření k zamezení opakování kybernetických bezpečnostních incidentů,
- záznamy, které se vztahují k bezpečnosti informací souvisejících s dodavatelem, jako jsou události bezpečnosti informací, provozní problémy, selhání nebo výpadky vztahující se ke službám poskytovaným dodavatelem,
- výsledky činností spojených s aktivací nebo testováním plánů kontinuity a schopnosti dodavatele naplnit cíle kontinuity a související ujednání,
- aktualizace hodnocení rizik souvisejících s dodavatelem v souhrnném hodnocení rizik,
- řízení poddodavatelů dodavatele,
- kontrola shody se smlouvou,
- evidence, řízení a řešení všech identifikovaných problémů,
- evidence, řízení a řešení změn, včetně provedení analýzy k provedení změny.

O reportech a závěrech by měl být informován manažer kybernetické bezpečnosti. Na základě zjištěných nedostatků musí být přijímána efektivní bezpečnostní opatření pro jejich řešení. Zároveň je smluvně upraven postup pro řešení změn na straně dodavatele, resp. pro zavádění bezpečnostních opatření pro napravení nedostatků.

5.4.2 Pravidla pro provádění zákaznického auditu u dodavatele

V případě, že dojde k potřebě provést zákaznický audit, je proveden přiměřeně podle vnitřního předpisu pro audit kybernetické bezpečnosti podle § 16 VKB a její přílohy č. 5: 1.1. Pravidla

a postupy pro provádění auditů kybernetické bezpečnosti, anebo prostřednictvím externí společnosti. Rozsah auditu je dán požadavky na daného dodavatele podle struktury dodávek či poskytovaných služeb.

Má-li dodavatel zavedený, a nezávislým certifikačním orgánem certifikovaný systém bezpečnosti informací podle normy ČSN ISO/IEC 27001 (minimálně pro rozsah poskytovaných služeb), je možné k tomuto při provádění zákaznického auditu přihlédnout, nikoliv však touto certifikací nahradit provedení celého zákaznického auditu.

Periodicita, způsob a rozsah provádění auditů u dodavatele je upraven ve smlouvě s dodavatelem.

Součástí provádění zákaznického auditu musí být umožnění otestování:

- procesu zvládání kybernetických bezpečnostních incidentů,
- havarijních plánů a plánů kontinuity služeb dodavatele,
- bezpečnostních parametrů služby.

5.5 Pravidla pro hodnocení dodavatelů

Informace o dodavatelích sloužící k jejich hodnocení jsou zaznamenávány do formuláře (jako vzor může sloužit Příloha č. 4).

Za aktuálnost a věcnou správnost evidence dodavatelů zpravidla zodpovídá manažer kybernetické bezpečnosti, za jednotlivá hodnocení dodavatelů odpovídají příslušní zaměstnanci odpovědní za smluvní vztah. Všechny dokumenty musí být pravidelně aktualizovány odpovědnými osobami.

Informace o dodavateli jsou získávány z veřejně dostupných zdrojů, zkušenostmi s dodavatelem před, během a po ukončení smluvního vztahu, z informací příslušných orgánů a z dalších relevantních zdrojů. Mělo by jít o ověřené a legálně získané informace.

Na základě všech dostupných informací je dodavatel ohodnocen, čímž dojde ke stanovení kategorie dodavatele.

5.5.1 Postup při hodnocení dodavatelů

Dodavatel může být hodnocen především v následujících oblastech:

- historie/pověst dodavatele,
- certifikace,
  - v oblasti bezpečnosti informací,
  - v oblasti řízení jakosti,
- reference ze spolehlivých zdrojů,
- transparentnost vlastnické struktury,
- kvalita a dostupnost informací z veřejných zdrojů,
- předchozí zkušenosti:
  - kvalita spolupráce,

- kvalita technické podpory,
- dodržení termínů dodávky,
- včasné informace o změnách a jejich zdůvodnění,
- reklamace a případné problémy s jejich uplatněním,
- výsledky zákaznických auditů u dodavatele nebo kontrol příslušných státních orgánů,
- dodržovaní smluvně stanovené úrovně poskytování služeb.

V každé z těchto oblastí může dodavatel získat body např. podle následující tabulky.

Tabulka 1: Bodové hodnocení

Počet bodů	Popis	Vodítko
2	Bylo zjištěno velké množství pozitivních informací.	S dodavatelem je dlouhodobě spolupracováno bez komplikací, anebo je dodavatel spolehlivou organizací s dlouhodobou historií a množstvím kladných referencí ze spolehlivých zdrojů.
1	Bylo zjištěno menší množství pozitivních informací.	O dodavateli jsou k dispozici kladné recenze, ale nejsou dostupné žádné přímé zkušenosti nebo informace ze spolehlivých zdrojů.
0	Nebyly zjištěny žádné informace.	Dodavatel je na trhu teprve krátce, anebo nebylo možné zjistit dostatek relevantních informací, aby mohl být objektivně posouzen.
-1	Byly zjištěny drobné nedostatky.	Na dodavatele existují stížnosti, které nejsou závažného charakteru.
-2	Byly zjištěny zásadní negativní informace.	Vážné negativní zkušenosti z minulé spolupráce s dodavatelem, anebo jejich detailní popis ze spolehlivého zdroje.

Sloupec „Vodítko“ má pouze demonstrativní charakter a uvádí příklady možných zkušeností s dodavatelem. Neobsahuje kompletní výčet. V ideálním případě si hodnotitel pro každou oblast hodnocení vytvoří vlastní vodítko.

Každá organizace by si měla zvolit kritéria a parametry hodnocení dodavatelů, která jí budou nejvíce vyhovovat a budou odpovídat jejím potřebám a specifikům. Hodnocení se může zakládat na kombinaci objektivně a subjektivně hodnotitelných veličin, pokud to dává organizaci smysl.

Na základě bodového hodnocení dodavatele v jednotlivých oblastech je zařazen do jedné z kategorií např. podle následující tabulky:

Tabulka 2: Kategorie dodavatelů

Počet bodů	Kategorie	Popis
12 až 22	**A**	Pro řízení dodavatele stačí standardní pravidla[12] řízení dodavatelů, která jsou shodná pro všechny.
0 až 11	**B**	K řízení dodavatele jsou doporučena méně náročná bezpečnostní opatření nad rámec standardních pravidel. V případě vyšší náročnosti opatření lze dodavatele řídit s využitím pouze standardních pravidel.
-11 až -1	**C**	K řízení dodavatele je potřeba zavést další bezpečnostní opatření nad rámec standardních pravidel.
-22 až -12	**D**	Dodavatel je považován za nevhodného a není doporučen ke spolupráci.

Hodnocení může být sestaveno i např. na základě dotazníku, ve kterém je stanovena sada požadavků v oblasti ISMS vycházející ze ZKB, příp. z normy ČSN ISO/IEC 27001 (lze doplnit např. i požadavky normy ČSN ISO/IEC 27036). Dodavatel následně dotazník vyplní a výsledek může být podkladem pro hodnocení dodavatele např. ve formě bodového ohodnocení. Alternativně může být využito i předložení auditorské zprávy nezávislé externí auditorské společnosti za účelem ověření souladu implementovaného kontrolního rámce, dodržování bezpečnostních kontrol, opatření, procesů a systému řízení bezpečnosti informací podle požadavků a opatření vyplývajících z ČSN ISO/IEC 27001 (ISO 27002) a ZKB, v oblasti řízení informační bezpečnosti a ochrany informací.

Další možností je dodání nezávislého reportu externího hodnotitele jako např. ISAE 3402, SSAE 18, který provedl posouzení prostředí dodavatele obsahující přehled přijatelných bezpečnostních kontrol, opatření a postupů pro řízení bezpečnosti informací a řízení a zvládání rizik a incidentů.

Výše uvedené skutečnosti mohou být předmětem následných kontrol ze strany organizace.

Hodnocení dodavatelů je prováděno **před uzavřením smlouvy a po ukončení smlouvy**, protože může sloužit jako podklad pro budoucí smluvní vztahy, příp. jako podklad jiné části organizace, která by chtěla s dodavatelem spolupracovat. **V průběhu smluvního vztahu jsou prováděna průběžná hodnocení,** která slouží jako podklad pro hodnocení dodavatele po ukončení

[12] Netýká se specifických rizik dodávky, na která je potřeba přijímat dodatečná bezpečnostní opatření.

smluvního vztahu. Průběžná hodnocení se nemusí pokaždé týkat všech oblastí hodnocení dodavatele, ale musí obsahovat všechny relevantní skutečnosti z průběhu smluvního vztahu. Průběžná hodnocení, jako např. poznámky o zpoždění dodávky, jsou prováděna ideálně jednou za půl roku (dobrá praxe za účelem snížení rizika opomenutí některých skutečností z důvodu časové prodlevy). Za provedení hodnocení odpovídá zaměstnanec odpovědný za smluvní vztah.

Zaměstnanci odpovědní za smluvní vztah se podílejí na zlepšování procesu hodnocení dodavatelů obvykle společně s manažerem kybernetické bezpečnosti.

5.5.2 Využití výstupů hodnocení dodavatelů

O výsledku hodnocení dodavatele je zpravidla informován manažer kybernetické bezpečnosti. Negativní hodnocení dodavatele v oblasti kybernetické bezpečnosti by mělo být projednáno výborem pro řízení kybernetické bezpečnosti (dobrá praxe).

Na základě zjištěné míry rizika přijímá osoba odpovědná za řízení rizik a akceptaci v organizaci příslušná bezpečnostní opatření před uzavřením smlouvy nebo v rámci již uzavřených smluvních vztahů.

Hodnocení může být prakticky využito při výběru dodavatelů do nových smluvních vztahů. V rámci smluvního vztahu mimo zadávací řízení může být pozitivně hodnocený dodavatel na základě hodnocení upřednostněn, naopak negativní hodnocení může být důvodem vyřazení dodavatele. **V zadávacím řízení** mohou být získané poznatky využity při formulaci zadávacích podmínek a hodnotících kritérií, a případně pro úpravy budoucích smluvních vztahů, např. pokud je dodavatel problematický v oblasti, která byla doposud ve smluvních ujednáních řešena nedostatečně. Nadto lze tyto informace promítnout i do hodnocení rizik, byť jen v obecné rovině.

6 Kontrola účinnosti řízení dodavatelů

Za účelem neustálého zlepšování musí být prováděna kontrola účinnosti procesu řízení dodavatelů alespoň jednou za rok. Za kontrolu účinnosti řízení dodavatelů obvykle odpovídá manažer kybernetické bezpečnosti, který spolupracuje s jednotlivými zaměstnanci odpovědnými za smluvní vztahy např. za účelem zlepšení procesů.

Kontrola účinnosti je zaměřena na:

- provádění identifikace a hodnocení rizik souvisejících s dodávaným plněním,
- provádění identifikace a hodnocení rizik souvisejících s dodavateli,
- vedení a aktualizování Evidence dodavatelů,
- promítnutí bezpečnostních požadavků do smluv s dodavateli,
- zohledňování hodnocení dodavatelů do výběru dodavatele,
- seznamování a kontrolu dodržování bezpečnostních opatření dodavateli (např. zákaznický audit).

Výsledkem kontroly účinnosti procesu řízení dodavatelů je zpráva o účinnosti, která obsahuje zjištění a doporučení pro zlepšení celého procesu (dobrá praxe).

Zpráva o účinnosti je jedním ze vstupních zdrojů informací pro celkové vyhodnocení účinnosti systému řízení bezpečnosti informací a její výsledky musí být zohledněny v plánu zvládání rizik.

7 Další aspekty řízení dodavatelů

7.1 Rozhodnutí o předání dat

Jak již bylo zmíněno v úvodu, tento dokument obecně shrnuje problematiku řízení dodavatelů z pozice povinných osob. Do této soukromoprávní problematiky může v průběhu celého dodavatelského životního cyklu vstoupit NÚKIB rozhodnutím podle § 15a ZKB.

V souladu s tímto ustanovením může NÚKIB v případě hrozícího kybernetického bezpečnostního incidentu na návrh správce uložit provozovateli povinnost předat správci data, provozní údaje a informace, které má provozovatel k dispozici v souvislosti s provozováním regulovaného systému. Návrh musí mj. obsahovat podrobný popis předchozího jednání mezi správcem a provozovatelem zejména s ohledem na nesplnění smluvní povinnosti provozovatele.

Tento veřejnoprávní zásah do soukromoprávních vztahů je tedy podmíněn nutností ošetřit si dodavatelské vztahy již ve smlouvě uzavřené s provozovatelem a nejedná se tak o náhradu nedostatečně smluvně upravených povinností provozovatele.

7.2 Cloud computing

Nad rámec obecných požadavků podle VKB na řízení dodavatelů mají povinné osoby, které jsou orgány veřejné moci, povinnost řídit dodavatele služeb cloud computingu v souladu s § 4 odst. 5 ZKB. Jedná se o povinnost před uzavřením smlouvy zařadit poptávaný cloud computing do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému podle prováděcího právního předpisu a zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená NÚKIB. Blíže se touto problematikou zabývá podpůrný materiál Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně[13].

Povinné osoby musí také zajistit, že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává, včetně možnosti kontroly uchovávaných informací a dat v reálném čase.

[13] Materiál je dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/2021-11-30_Pruvodce-zarazenm-do-bezpecnostni-urovne_final.pdf.

8 Použité pojmy a zkratky

Architekt kybernetické bezpečnosti – § 7 odst. 2 VKB „bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního nebo komunikačního systému“. Tato role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.

Auditor kybernetické bezpečnosti – § 7 odst. 4 VKB „bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti“. Tato role není slučitelná s ostatními bezpečnostními rolemi podle VKB.

Dodavatel – je každý, kdo poskytuje dodávky, služby nebo stavební práce a vstupuje do právního vztahu s povinnou osobou. Dodavatelem je provozovatel informačního nebo komunikačního systému, významný dodavatel a každý dodavatel, který nesplní definici provozovatele informačního nebo komunikačního systému či významného dodavatele.

Garant aktiva – § 7 odst. 3 VKB „bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva“.

ISMS – systém řízení bezpečnosti informací.

Manažer kybernetické bezpečnosti – § 7 odst. 1 VKB „bezpečnostní role odpovědná za systém řízení bezpečnosti informací“. Tato role není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi.

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost.

Provozovatel informačního nebo komunikačního systému – § 2 písm. g) ZKB „orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“. Provozovatel je vždy významným dodavatelem.

VKB – vyhláška č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Výbor pro řízení kybernetické bezpečnosti – § 6 odst. 7 VKB „je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností, jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti“.

Významný dodavatel – § 2 písm. g) VKB „provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému“.

Zadavatel – § 4 odst. 2 ZZVZ „osoba, která k úhradě nadlimitní nebo podlimitní veřejné zakázky použije více než 200 000 000 Kč, nebo více než 50 procent peněžních prostředků, poskytnutých

a) z rozpočtu veřejného zadavatele,

b) z rozpočtu Evropské unie nebo veřejného rozpočtu cizího státu s výjimkou případů, kdy je veřejná zakázka plněna mimo území Evropské unie.“

Zadávací řízení – procesní postup zadavatelů při zadávání veřejných zakázek a výběru dodavatele podle ZZVZ.

Zaměstnanec odpovědný za smluvní vztah – zaměstnanec, který určuje a řídí všechny odborné záležitosti související s předmětnými dodávkami nebo službami, měl by tedy disponovat odborným povědomím o věcném plnění.

ZKB – zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

ZZVZ – zákon č. 134/2016 Sb., o zadávání veřejných zakázek (zákon o zadávání veřejných zakázek).

9 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP: AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP: AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
21. prosince 2022	1.0	Odbor regulace, Odbor kontroly	Vytvoření dokumentu
6. září 2023	2.0	Odbor regulace, Odbor kontroly	Zapracování připomínek, finalizace