



Jihočeská univerzita v Českých Budějovicích

<i>Označení dokumentu:</i>	ISMS-004
<i>Název dokumentu:</i>	Politika řízení dodavatelů
<i>Typ dokumentu:</i>	Interní dokument – TLP:GREEN
<i>Rozsah:</i>	Tato politika se vztahuje na veškeré dodavatele, kteří mají přístup k aktivům objednatele. Dle typu a významu aktiva je určen rozsah smluvních ujednání.
<i>Prvek legislativy:</i>	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 8, 9, 14
<i>Datum vydání:</i>	07. 07. 2026
<i>Datum účinnosti:</i>	07. 07. 2026
<i>Platnost do:</i>	odvolání
<i>Počet stran + příloh:</i>	5 + 7
<i>Verze:</i>	1.1
<i>Význam a benefity:</i>	Dodavatelé, jako významná kategorie podpůrných aktiv, musí být velmi pečlivě řízeni a kontrolováni. Veškeré parametry vztahu je nutné uvést ve smlouvě.
<i>Uložení:</i>	Sekce kyberbezpečnosti na Wiki JU
<i>Ruší dokumenty:</i>	-
<i>Zpracovatel:</i>	Manažer KB JU
<i>Přezkoumal:</i>	Výbor pro kybernetickou bezpečnost JU
<i>Schválil:</i>	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

V rámci daného oddílu je konkrétně vymezen obsah bezpečnostní politiky.

NÚKIB vydal podpůrný materiál **Metodika řízení dodavatelů**¹.

Institut Orgánu veřejné moci (OVM), který provozuje Významný informační systém je také zpracován v materiálu NÚKIBu².

a) Pravidla a principy pro výběr dodavatelů

Musí existovat dokumentovaný postup: Směrnice o realizaci výběrových řízení a veřejných zakázek. Směrnice (její příloha) obsahuje hlediska zpracovaná v materiálu NÚKIBu³.

Od r. 2022: Prověření dodavatele na vztahující se sankce:

- https://sankce.datlab.eu/?utm_medium=blog&utm_source=blog_sankce

V politice dodavatelů je akceptován proces Životní cyklus dodavatelského vztahu⁴.

Politika plynoucí z podpůrného materiálu NÚKIB:

- Existují 2 stupně pravidel pro dodavatelský smluvní vztah (VIS a ostatní IS)
- Existují 2 stupně kategorií dodavatelů (významný dodavatel pro VIS a běžný dodavatel pro ostatní IS)
- Pro každou kategorii existují vzory dodavatelských ujednání – viz příloha.
- Pro každého dodavatele je určen zaměstnanec odpovědný za smluvní vztah.
- Pro každou potřebu dodavatele proběhne zjištění rizik souvisejících s výběrem dodavatele, která jsou přetransformována do “bezpečnostních potřeb”.
- Bezpečnostní potřeby jsou zahrnuty do výběrových podmínek, které musí odpovídat zákonu o zadávání veřejných zakázek (ZZVZ), ale nesmí být navázány na osobu dodavatele, tedy diskriminační. Je potřeba je zohlednit jinak.

Existuje Procesní plán Postupu před uzavřením smlouvy⁵.

¹ Příloha č.1: Metodika řízení dodavatelů

² Příloha č.2: Provozovatel informačního nebo komunikačního systému, verze 3.2.

³ Příloha č.3: Zadávání veřejných zakázek v oblasti ICT a KB, verze 1.5.

⁴ Příloha č.4: VZOR: Životní cyklus dodavatelského vztahu.

⁵ Příloha č.5: VZOR: Postup před uzavřením smlouvy

b) Pravidla pro hodnocení rizik souvisejících s dodavateli

Existuje přehled dodavatelů a jejich parametrů. Přehled významných dodavatelů a dodavatelů je dostupný ve správě aktiv JU.

Existuje registr možných rizik spojených s dodavateli a způsoby jejich ošetření, s předmětem dodávky, případně dalších hledisek, která jsou posuzována. Registr rizik je dostupný ve správě aktiv JU.

Rizika související s dodavatelem

- Riziko ekonomické a finanční nezpůsobilosti.
- Riziko řízení dodavatelského řetězce (subdodavatelé).
- Riziko nedostatečné součinnosti dodavatele po realizaci dodávky, tj. v reálném provozu.
- Riziko nedostatečné součinnosti dodavatele při řízení incidentů.
- ...atp.

Rizika související s předmětem dodávky

- Riziko nevhodné technické kvalifikace.
- Riziko náhlého ukončení dodavatelských služeb.
- Riziko nesplnění aktuálních opatření vydaných legislativou.
- Atp.

Za stanovení rizik a jejich prosazení do zadávací dokumentace je zodpovědný zaměstnanec odpovídající za smluvní vztah.

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

A. Pro nevýznamné aktivum

1. Poskytovatel bere na vědomí, že objednatel je správcem významných informačních systémů dle § 3 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a dalších informačních systémů nutných pro zajištění řádného chodu objednatele coby veřejné vysoké školy zřízení zákonem, a to jak na úseku samosprávy, tak i na úseku státní správy.
2. Poskytovatel se zavazuje zavádět nezbytná technická a organizační opatření pro zajištění bezpečnosti služeb včetně informačních systémů a dat objednatele, s cílem zajistit důvěrnost, dostupnost a integritu informačních systémů a informací a s cílem chránit veškeré informace, data a údaje před vyzrazením, pozměňováním, zničením, ztrátou, zkreslením, neoprávněným zpřístupněním a zpracováním, a to ať již by šlo o činnosti náhodné, neoprávněné či nezákonné.
3. Poskytovateli není bez výslovného oprávnění ze strany objednatele povoleno jakékoliv používání, sdělování, šíření či přenášení důvěrných informací a dat objednatele mimo informační systém objednatele.
4. Poskytovatel bude v rozsahu předmětu plnění respektovat povinnosti objednatele uvedené zejména v § 18 až § 27 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

5. Poskytovatel se především zavazuje:

- používat jen takové zdroje a prostředky pro připojení k informačnímu systému objednatele, které mu objednatel poskytne, a to výhradně pro účely předmětu plnění dohodnutého v rámci této smlouvy a v přísném souladu s bezpečnostními politikami informačního systému objednatele, jejichž převzetí podpisem této smlouvy poskytovatel potvrzuje (jsou poskytovateli poskytnuty se smlouvou);
 - pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran;
 - na aktiva objednatele neinstalovat a nepoužívat v prostředí objednatele nástroje a programy, které nejsou nezbytnou součástí předmětu plnění v rámci této smlouvy.
6. Poskytovatel se zavazuje informovat objednatele o všech skutečnostech, které mohou mít vliv na zabezpečení kterékoliv poskytované služby a software, zejména o všech kybernetických bezpečnostních incidentech. Poskytovatel uvedené povinnosti splní bez zbytečného odkladu po zjištění skutečnosti, která byla rozhodná pro vznik dané povinnosti.
7. V případě bezpečnostního incidentu na straně poskytovatele, který měl dopad na data či systémy objednatele, se poskytovatel zavazuje nahradit objednateli vzniklou škodu v souladu s příslušnými ustanoveními občanského zákoníku. Poskytovatel je povinen učinit veškerá opatření potřebná k odvrácení škody nebo k jejímu zmírnění. Poskytovatel přebírá zodpovědnost i za své případné poddodavatele.
8. Poskytovatel bere na vědomí, že v případě, kdy technické spojení objednatele s poskytovatelem narušuje chod služeb objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato smlouva nestanoví jinak.

Poznámky

- Je potřeba zkontrolovat správné termíny: **poskytovatel, objednatel, předmět plnění, služby a software.**
- V případě, že by plnění mělo být prováděno přímo na aktivech významného informačního systému a/nebo významným dodavatelem, je nutné celý článek týkající se řízení bezpečnosti **rozpracovat** v souladu s přílohou č. 7 vyhlášky o kybernetické bezpečnosti. Lze předpokládat, že v takovém případě **smlouvu předloží prvotně dodavatel.**
- Při úpravě smlouvy v ní vždy zůstanou body, které budou souviset se zamýšleným účelem a stupněm spolupráce/smlouvy, a budou splnitelné a oprávněné.

B. Pro významný informační systém

Parametry smlouvy jsou uvedeny v materiálu NÚKIBu⁶, kde je více než 10 oblastí, které mají být co nejvíce konkrétně smluvně zachyceny.

⁶ Příloha č.6: Požadavky na smlouvy s dodavateli, verze 1.4.

Politika (podpůrný materiál) obsahuje všechna zákonem požadovaná hlediska, v praxi se na konkrétního dodavatele aplikují jen ta relevantní, přiměřenou měrou.

Existuje seznam potřebných ustanovení ve Vyhlášce⁷.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření

Politika je rovněž součástí podpůrného výše uvedeného materiálu NÚKIBu – Metodika řízení dodavatelů.

- Právo na případný zákaznický audit je zakotveno ve smlouvě.
- Je pravidelně prováděna kontrola bezpečnostních opatření prostřednictvím přezkoumávání plnění smluv v rozsahu dodržování požadavků na bezpečnostní opatření, a to:
 - u významného dodavatele alespoň jednou za rok,
 - u ostatních dodavatelů alespoň jednou za 2 roky.

e) Pravidla pro hodnocení dodavatelů

Politika je rovněž součástí podpůrného výše uvedeného materiálu NÚKIBu – Metodika řízení dodavatelů.

Inspirativní příklad. Hodnocení dodavatelů je zde vyhodnoceno výhradně s ohledem na možné dopady. Nejsou zahrnuty vlivy: cena, splatnost, dodací podmínky apod.

Hodnocení se provádí 1x ročně podle kritérií, které mají následující **váhu**:

- **Kvalita** – dodavatel má ISO: **váha 1,0**
- **Odbornost** – zkušenost dodavatele s obdobným plněním, rutina, potřeba subdodavatelů: **váha 0,8**
- **Stabilita** – dlouhodobá vzájemná finanční a tržní historie, reference: **váha 0,6**

Hodnocení kvality dle ISO:

Dodavatel musí mít zavedený systém managementu podle ČSN ISO řady 9000x27001 (kopie akreditovaného certifikátu musí být doložena). V případě, že systém managementu nemá zavedený, musí vyplnit dotazník a způsobilost musí být ověřena externím auditem. Výsledky a hodnocení externího auditu:

- dodavatel má ISO: **4 body**
- dodavatel nemá ISO, externí audit v pořádku: **3 body**
- dodavatel nemá ISO, externí audit shledal drobné nedostatky, nápravná opatření po externím auditu jsou v pořádku: **2 body**

⁷ <https://www.zakonyprolidi.cz/cs/2018-82#f6229237>

- dodavatel nemá ISO, nápravná opatření nebyla po externím auditu realizována: **1 bod.**

Hodnocení odbornosti

Dodavatel musí uvést seznam subdodavatelů, je posuzována jeho míra závislosti na nich:

- Předmět dodávek je jedna z hlavních specializací dodavatele. Ve výběrovém řízení doložil odbornou způsobilost konkrétních osob. Je schopen samostatně řešit stávající i budoucí architekturu i audit našeho řešení. Disponuje nepřetržitou pohotovostí (2 a více osob) pro případné servisní zásahy: **4 body**
- Dodavatel je odborně způsobilý samostatně na místě zprovoznit veškeré závady, převzít kontrolu nad provozem. Má veškerou dokumentaci: **3 body**.
- Dodavatel předává servisní požadavek třetí osobě, která není smluvně zajištěna, jako přímý kontakt uvedený ve smlouvě. Dodavatel samostatně zprovozní jen část, která byla předmětem dodávky, není schopen bez součinnosti s odběratelem zajistit provoz navazujících služeb: **2 body**
- Dodavatel je plně závislý na řízení/součinnosti s odběratelem: **1 bod.**

Hodnocení stability

Dodavatel má dobrou reputaci a stabilitu pro dodržení svých závazků:

- stávající dodavatel, který (nám) již v minulých 3 letech nezpозdil dodávku, ani na něj nebyly uplatňovány sankce: **4 body**
- stávající dodavatel, který (nám) již v minulých 3 letech dodával: **3 body**
- nový dodavatel, který zvítězil, včetně doložení realizací obdobného plnění v minulých 3 letech: **2 body**
- nový dodavatel: **1 bod.**

Výsledek hodnocení

1. skupina: Zcela vyhovující: **9,6 – 8,0 bodů**,
2. skupina: Vyhovující: **méně než 8,0 – 4,5 bodů**,
3. skupina: Nevhovující: **méně než 4,5 bodů**.

Viz vzor přílohy č. 9⁸.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.

⁸ Příloha č.7: VZOR: Hodnocení dodavatelů