

Politika řízení dodavatelů

I. Úvodní ustanovení

- 1) Politika řízení dodavatelů stanovuje pravidla pro dodavatele ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále také „zákon o kybernetické bezpečnosti“) a vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále také „vyhláška o kybernetické bezpečnosti“) v podmínkách Univerzity Hradec králové (dále také „UHK“).
- 2) Účelem této politiky je specifikovat zadávací podmínky veřejných zakázek včetně zakázek malého rozsahu pro potenciální významné dodavatele, kterými se rozumí každý provozovatel informačního nebo komunikačního systému a každý, kdo s UHK vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému (dále také „dodavatele“) v podmínkách UHK.
- 3) Tato politika se vztahuje na všechny dodavatele, kteří se podílejí na rozvoji, provozu nebo zajištění bezpečnosti významných informačních systémů (dále také „VIS“) na UHK a mají přístup k aktivům UHK. Dle typu a významu aktiva je určen rozsah smluvních ujednání jednotlivých veřejných zakázek.

II. Pravidla a principy pro výběr dodavatelů

- 1) UHK stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací (dále také „SŘBI“) UHK, seznamuje své dodavatele s těmito pravidly a vyžaduje jejich plnění.
- 2) UHK řídí rizika spojená s dodavateli a vede evidenci svých dodavatelů.
- 3) UHK prokazatelně písemně informuje své dodavatele o jejich evidenci, přičemž náležitosti prokazatelného informování jsou:
 - a) identifikace správce nebo provozovatele,
 - b) identifikace informačního a komunikačního systému,
 - c) identifikace dodavatele,
 - d) vyrozumění o tom, že dodavatel je pro správce významným dodavatelem, popřípadě že významný dodavatel je zároveň provozovatelem,
 - e) obsah bezpečnostních pravidel pro dodavatele zohledňující požadavky SŘBI.
- 4) UHK zajistí v souvislosti s řízením rizik spojených s dodavateli, aby smlouvy uzavírané s dodavateli obsahovaly relevantní opatření k zajištění bezpečnosti VIS.
- 5) UHK pravidelně přezkoumává plnění smluv s dodavateli z hlediska SŘBI.

III. Pravidla pro hodnocení rizik souvisejících s dodavateli

- 1) Výbor kybernetické bezpečnosti (dále také „Výbor KB“) v rámci všech uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření a ve spolupráci s útvary zajišťující právní agendu smluvních vztahů určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.
- 2) Výbor KB provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany, v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.
- 3) Pro hodnocení rizik dodavatelů byl vytvořen a je využíván chráněný dokument *Checklist pro audit a kontroly dodavatelů*.

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

- 1) Smlouvy uzavírané s dodavateli musí obsahovat následující či obdobný text:
Dodavatel bere na vědomí, že UHK je správcem významných informačních systémů dle § 3 písm. e) zákona o kybernetické bezpečnosti, a dalších informačních systémů nutných pro zajištění řádného chodu UHK coby veřejné vysoké školy podle zákona č. 111/1998 Sb. o vysokých školách.
- 2) Smlouvy uzavírané s dodavateli musí obsahovat dále tyto náležitosti, přičemž se vychází
z Bezpečnostních pravidel pro významné dodavatele, relevantně ke konkrétnímu dodavateli a konkrétnímu obsahu dodávky nebo služby:
 - a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
 - b) ustanovení o oprávnění užívat data,
 - c) ustanovení o autorství programového kódu, popřípadě o programových licencích,
 - d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
 - e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi UHK a dodavatelem a nebudou v rozporu s požadavky UHK na dodavatele,
 - f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky UHK nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
 - g) ustanovení o řízení změn,
 - h) ustanovení o souladu smluv s obecně závaznými právními předpisy,
 - i) ustanovení o povinnosti dodavatele informovat UHK o:
 - kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
 - způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,

- významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,
 - j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
 - k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
 - l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
 - m) pravidla pro likvidaci dat,
 - n) 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,
 - o) ustanovení o sankcích za porušení povinností.
- 3) V případě zpracování osobních údajů je nezbytné vyjasnění vztahů mezi smluvními partnery (samostatní správci, společní správci a vztah správce vs. zpracovatel). V případě společných správců je nezbytné určení prostředků a účelů zpracování.

V. Pravidla pro provádění kontroly zavedení bezpečnostních opatření

- 1) Právo na případný zákaznický audit musí být zakotveno ve smlouvě.
- 2) Zákaznickým auditem se rozumí pravidelně prováděná kontrola bezpečnostních opatření prostřednictvím přezkoumávání plnění smluv v rozsahu dodržování požadavků na bezpečnostní opatření, a to alespoň jednou za rok. Podrobnosti jsou uvedeny v *Metodice hodnocení dodavatelů*, která je chráněným dokumentem.

VI. Pravidla pro hodnocení dodavatelů

- 1) Hodnocení dodavatelů bude probíhat na základě pevně stanoveného postupu definovaného v *Metodice hodnocení dodavatelů*. Základem hodnocení dodavatelů bude posouzení míry naplnění požadavků definovaných ve smlouvě, směřujících především k zajištění bezpečnosti informací a kybernetické bezpečnosti UHK.
- 2) Výsledek hodnocení bude využit jak pro získávání zpětné vazby v rámci SRBI, tak pro případné posuzování dodavatele v dalších veřejných zakázkách.
- 3) Povinnost provést hodnocení dodavatelů má osoba odpovědná za věcné plnění smlouvy (žadatel o pořízení služby či zboží) ve spolupráci s Manažerem KB a s využitím konzultací se zaměstnanci Oddělení informačních technologií vždy nejpozději při ukončení smluvního vztahu s dodavatelem, u déle trvající spolupráce pak vždy ke konci každého kalendářního roku trvání smluvního vztahu s daným dodavatelem.

- 4) Výsledky provedených hodnocení dodavatelů jsou předávány Výboru KB a mají charakter chráněného dokumentu.

VII. Závěrečná ustanovení

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

V Hradci Králové dne 31. 5. 2024

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