

**Pokyn ředitele Krajského úřadu Středočeského kraje**

**č.**

***o informační a kybernetické bezpečnosti KÚSK***

**Příloha č. 4 - Politika řízení dodavatelů**

**Závazné pro:** zaměstnance Středočeského kraje zařazené do Krajského úřadu Středočeského kraje a třetí strany se smluvním závazkem ke Krajskému úřadu Středočeského kraje

**Navrhovatel:** Odbor bezpečnosti a krizového řízení

**Datum vyhlášení:**

**Přílohy:** Dokument neobsahuje přílohy

**Obsah:**

[Článek 1 Významní dodavatelů 3](#_Toc85572965)

[Článek 2 Pravidla pro výběr dodavatelů 3](#_Toc85572966)

[Článek 3 Identifikace bezpečnostních požadavků a kontrola jejich plnění 4](#_Toc85572967)

[Článek 4 Bezpečnostní požadavky stanovené ve smlouvách s dodavateli 4](#_Toc85572968)

[Článek 5 Bezpečnostní požadavky na smlouvy „cloud computing“ 5](#_Toc85572969)

[Článek 6 Bezpečnostní pravidla při realizaci a po ukončení dodávek 6](#_Toc85572970)

**Středočeský kraj**

***Politika řízení dodavatelů***

Tato směrnice definuje politiku řízení dodavatelů Krajského úřadu Středočeského kraje (dále jen KÚSK), která definuje práva a povinnosti v oblasti systému řízení bezpečnosti informací (dále jen ISMS).

# Článek 1 Významní dodavatelů

Významný dodavatel je 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.

Pokud KÚSK stanoví některého z dodavatelů služeb jako „významného dodavatele“ určitých služeb, musí následně, nad rámec stanovených standardních a specifických bezpečnostních požadavků, provést následující kroky:

1. prokazatelně vyrozumí dodavatele o jeho postavení „významného dodavatele“ (buď přímo ve smluvním ustanovení, nebo jinou písemnou prokazatelnou formou) s nezbytnými následujícími mandatorními náležitostmi:
   1. identifikace správce nebo provozovatele,
   2. identifikace informačního a komunikačního systému,
   3. identifikace významného dodavatele,
   4. vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem,
   5. vlastní obsah bezpečnostních požadavků,
2. smluvně zajistí pokrytí relevantních požadavků bezpečnostních opatření podle přílohy č. 7 VKB,
3. pravidelně 1x ročně provádí přezkum plnění smlouvy z hlediska řízení bezpečnosti informací,
4. vede evidenci svých „významných dodavatelů“,
5. následně ověří, zda vyrozuměný dodavatel – provozovatel VIS, nahlásil své kontaktní údaje NÚKIB.

# Článek Pravidla pro výběr dodavatelů

Výběr dodavatelů se řídí platným zákonem o zadávání veřejných zakázek a doprovodnými právními normami. Při zadávání veřejných zakázek malého rozsahu je postupováno dle základních zásad zákona o zadávání veřejných zakázek, tj. transparentnost, rovné zacházení a zákaz diskriminace. V rámci KÚSK jsou všechny postupy při zadávání veřejných zakázek upraveny interními akty řízení. Bezpečnostní požadavky na výrobky a/nebo služby dodavatele je nutno následně specifikovat v zadávací dokumentaci, a to zejména cestou stanovení vhodných kvalifikačních podmínek a vlastních bezpečnostních požadavků na poptávané produkty/služby a jejich dodávku, implementaci a údržbu.

S odkazem na ZKB, ust. § 4 odst. 4, je prosazování bezpečnostních požadavků na dodavatele povinné a zohlednění těchto požadavků, vyplývajících z bezpečnostních opatření nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Při výběrovém řízení musí být minimalizována případná rizika, která by mohla nastat při nevhodném výběru dodavatele, a to zejména při poptávkách s vyšší předpokládanou cenou zakázky a dlouhodobější spolupráci s dodavateli. Jedná se zejména o následující rizika:

1. riziko bezpečnostní nespolehlivosti (lze redukovat základními kvalifikačními předpoklady a dalšími požadavky stanovenými platným zněním zákona o zadávání veřejných zakázek),
2. riziko ekonomické a finanční nezpůsobilosti (lze redukovat čestným prohlášením dodavatele o jeho způsobilosti),
3. riziko nevhodné profesní kvalifikace (lze redukovat profesními kvalifikačními předpoklady na dodavatele, subdodavatele a jejich pracovníky v rámci zakázky),
4. riziko nevhodné technické kvalifikace (lze redukovat technickými kvalifikačními předpoklady na dodavatele, subdodavatele a jejich pracovníky v rámci zakázky).

Redukce výše uvedených základních rizik se provádí v souladu se zákonem o zadávání veřejných zakázek, ve znění pozdějších předpisů.

# Článek 3 Identifikace bezpečnostních požadavků a kontrola jejich plnění

Základním krokem před zahájením dodávek a služeb poskytovaných dodavatelsky je provedení analýzy všech aspektů a z nich plynoucích konkrétních požadavků, včetně bezpečnostních. Analýza se provádí v úvodní fázi projektové přípravy dodávek a služeb, nebo, v případě jednorázových nákupů a dodávek zboží, při specifikování požadovaných vlastností tohoto zboží a způsobu jeho dodání. Analýzu provádí zadavatel zakázky.

Pro kontrolu a případné doplnění těchto bezpečnostních požadavků je povinností zadavatelů těchto typů zakázek (tj. zadavatelským útvarem – viz platná Směrnice o zadávání veřejných zakázek) poskytovat návrhy zadávací dokumentace a smluv OBŘ, a to v dostatečném časovém předstihu (minimálně 5 pracovních dní před uzavřením zadávací dokumentace), před finalizací zadávací dokumentace a vypsáním výběrového řízení.

# Článek 4 Bezpečnostní požadavky stanovené ve smlouvách s dodavateli

V souvislosti s výše uvedenými pravidly a požadavky na minimalizaci rizik musí být tyto bezpečnostní požadavky promítnuty do konečné smlouvy s dodavateli. Další bezpečnostní požadavky, které je nezbytné smluvně zakotvit, jsou specifické požadavky (podle druhu poptávané technologie a/nebo služeb) na:

1. vlastní technologické bezpečnostní požadavky,
2. bezpečnostní požadavky na dodávku a implementaci (včetně bezpečné migrace dat, pokud je součástí implementace) a nezbytnou součinnost KÚSK jako zadavatele,
3. bezpečnost provozu v podmínkách KÚSK,
4. nezbytnou provozní (systémovou, uživatelskou a bezpečnostní) dokumentaci k dodávce,
5. specifikace případné výměny dat a způsobu jejího bezpečného provádění,
6. vhodné školení zaměstnanců KÚSK k obsluze a využití technologie (pokud bylo součástí dodávky).

Součástí smluv musí být též sankční ujednání za nedodržení smluvních podmínek dodávek, včetně bezpečnostních, a dále ustanovení o ochraně veškerých informačních aktiv KÚSK, jenž byla dodavateli poskytnuta, které bude zakomponováno jako samostatné ustanovení smlouvy, nebo jako nedílná příloha smlouvy. Jedná se zejména o zachování důvěrnosti a mlčenlivosti ve vztahu k poskytnutým interním informacím KÚSK, jejichž zveřejnění nebo poskytnutí jiným osobám by bylo v rozporu s účelem jejich poskytnutí, a mohlo by způsobit KÚSK nebo třetím stranám škodu.

# Článek 5 Bezpečnostní požadavky na smlouvy „cloud computing“

Při použití služeb typu „cloud computing“, k zajištění bezpečnosti poskytovaných informačních služeb a dat KÚSK a ve shodě se ZKB, § 4, odst. 5, musí být smluvně zajištěno, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená NÚKIB, a že KÚSK bude mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro něj poskytovatel služeb cloud computingu uchovává, včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Dalšími nezbytnými náležitostmi smlouvy jsou:

1. zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,
2. stanovení úrovně poskytovaných služeb,
3. systém schvalování subdodavatelů služby cloud computingu,
4. podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
5. řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
6. určení vlastníka uchovávaných dat,
7. dohoda o důvěrnosti smluvního vztahu,
8. stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
9. pravidla zákaznického auditu,
10. stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.

Některé výše uvedené vybrané náležitosti smlouvy lze vhodným způsobem uplatnit i u dalších nakupovaných ICT služeb.

# Článek 6 Bezpečnostní pravidla při realizaci a po ukončení dodávek

Při vlastní realizaci dodávky informačních aktiv musí být uplatněna následující obecná bezpečnostní pravidla:

1. Prokazatelné seznámení dodavatelů s relevantními požadavky ISMS

Pokud nejsou některé relevantní požadavky ISMS přímou součásti smluvních ujednání, je před vlastní dodávkou nezbytné zajistit seznámení dodavatelů s těmito požadavky a zajistit zadokumentování tohoto seznámení (např. formou zápisu z úvodní projektové schůzky při startu daného projektu). Za to odpovídá vedoucí daného projektu/dodávky ze strany KÚSK, který může požádat o součinnost OBŘ.

1. Kontrola dodavatelských činností

Kontrolu dodavatelských činností z pohledu ISMS zajišťuje Manažer ISMS v rámci standardních kontrol dodavatelských činností. K těmto kontrolám je s dostatečným předstihem přizván příslušným vedoucím daného projektu/dodávky za KÚSK.

1. Hodnocení činnosti dodavatelů

Po ukončení činnosti dodavatelů (ukončení projektu), nebo při pravidelných vyhodnocení činnosti dodavatelů u dlouhodobých služeb, provádí Manažer ISMS na výzvu vedoucího daného projektu/dodávky vyhodnocení, zda byly v daném období dodržovány bezpečnostní požadavky na zajištění dodávky informačních aktiv.