Příloha č. 6
Bezpečnostní pravidla pro dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva Jihočeského kraje a Krajského úřadu Jihočeského kraje (dále jen „**Objednatel**“), ke kterým mají přístup Dodavatelé.

A.1 Základní odpovědnosti Dodavatele (Poskytovatel ve smyslu této smlouvy) Dodavatel řešení:

1. Je povinen postupovat v souladu s platnými právními předpisy ČR, zejména pak v souladu s požadavky vyplývajícími pro Objednatele, jakožto správce a provozovatele Významných informačních systémů, ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále též „Zákon“), vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále též „Vyhláška“) a dále z bezpečnostních doporučení NCKB pro administrátory v aktuálně platné verzi a reflektovat případné novely uvedených právních předpisů či novou právní úpravu.
2. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost Objednatele, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
3. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
4. Je povinen zajistit, aby předmět plnění nebyl nevyhovující z hlediska kybernetické a informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se Zákonem, a která dle analýzy rizik představují vysoké riziko.
5. Je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik.
6. Je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro Objednatele.
7. Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s Objednatelem.
8. Je povinen poskytovat cloudové služby v souladu s platnou legislativou ČR, zejm. zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů v platném znění, a vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.

A.2 Ochrana Aktiv

Dodavatel se před vlastním přístupem k datům a informacím Objednatele musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků Objednatele zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

A.3 Přístup k ICT/IS

Přihlášení dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

A.4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

1. Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí Zákonem a zejména Vyhláškou a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
2. Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury dodavatele.
3. Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.

4. Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

A.5 Řízení změn

1. Dodavatel se zavazuje určovat významné změny, za které se považují změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a představují vysoké riziko. Dodavatel je povinen o těchto významných změnách předem informovat Objednatele.
2. U významných změn se Dodavatel zavazuje zejména:
3. provádět analýzu rizik,
4. přijímat opatření za účelem snížení negativních dopadů těchto změn, včetně případného penetračního testování a testování zranitelnosti,
5. dokumentovat jejich řízení,
6. aktualizovat specifickou bezpečnostní politiku pro danou v oblast,
7. zajistit možnost navrácení do původního stavu,
8. v případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Dodavatel Objednateli veškerou potřebnou součinnost. Dodavatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

A.6 Řízení bezpečnostních rizik

1. Dodavatel je povinen alespoň 1x ročně provádět vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. O výsledku hodnocení rizik Dodavatel Objednateli předloží Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
2. vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok, včetně vyhodnocení souladu s těmito Bezpečnostními pravidly,
3. identifikaci a hodnocení rizik s vazbou na předmět plnění,
4. realizovaná bezpečnostní opatření,
5. nepokrytá bezpečnostní rizika a návrh opatření,
6. vyhodnocení bezpečnostních událostí a incidentů.

A.7 Monitorování činností

1. Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačních systémech, může být Objednatelem průběžně a pravidelně monitorována.
2. Předmět plnění musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, v rozsahu stanoveném Vyhláškou, které umožní jednoznačně určit uživatele, čas a provedenu činnost.
3. Dodavatel se zavazuje, že umožní přístup k auditním údajům (systémové a aplikační logy) v takové podobě a formátu, který je možné dále zpracovávat v rámci systému nástrojů SIEM (Security Information Event Management) a tyto bude pravidelně předávat Objednateli.

A.8 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Dodavatel se zavazuje, že bude hlásit všechny nestandardní situace, bezpečnostní slabiny, kybernetické bezpečnostní události (KBU) a kybernetické bezpečnostní incidenty (KBI) včetně případů porušení zabezpečení osobních údajů bez zbytečného odkladu po jejich detekci Objednateli.
2. Hlášení KBÚ a KBI provádí Dodavatel telefonicky nebo e-mailem na kontakty uvedené ve smlouvě. Součástí oznámení musí být popis povahy konkrétního případu (KBU nebo KBI).
3. Dodavatel se zavazuje stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání KBU a KBI.
4. Dodavatel se zavazuje v případě vzniku KBU a následného zvládání a vyhodnocování KBI a/nebo v případě podezření na KBI poskytnout Objednateli součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.
5. Pokud dojde ke KBU nebo ke KBI a následnému zvládání a vyhodnocování KBU nebo KBI poskytne Dodavatel požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem).
6. Dodavatel má povinnost provést analýzu příčin KBU nebo KBI a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel KBU nebo KBI zapříčinil nebo se na jeho vzniku podílel.
7. Dodavatel má povinnost uchovávat informace o všech KBU a KBI pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
8. Dodavatel bere na vědomí, že postup zvládání KBU nebo KBI či jiný důsledek porušení těchto Bezpečnostních pravidel, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Dodavatele.

Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.

A.9 Řízení kontinuity činností

1. Dodavatel se zavazuje zejména (podléhá schválení ze strany Objednatele):
a. určit minimální úroveň poskytovaných služeb přijatelnou z hlediska zajištění kontinutity poskytovaných činností,
b. určit dobu obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb dle písm. a.,
c. určit časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
d. vypracovat, aktualizovat a pravidelně testovat plány kontinuity činnosti a havarijní plány související s poskytováním předmětu plnění.
2. Dodavatel předloží Objednateli metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována.

A.10 Akvizice, vývoj a údržba

1. Dodavatel se zavazuje zejména:
a. zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění smlouvy,
b. předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
c. dokumentace skutečného provedení,
d. dokumentace všech bezpečnostních nastavení, funkcí a mechanismů,
e. dokumentace obsahující popis autorizačního konceptu a oprávnění,
f. dokumentace obsahující zálohovací a archivační postupy,
g. dokumentace obsahující instalační a konfigurační postupy,
h. dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

A.11 Kontrola a audit dodavatele

1. Dodavatel se zavazuje zejména:
a. umožnit Objednateli provést na straně Dodavatele minimálně jedenkrát (1x) za rok pravidelné vyhodnocení rizik souvisejících s předmětem plnění a poskytnout potřebnou součinnost,
b. umožnit Objednateli nebo Národnímu úřadu pro kybernetickou a informační bezpečnost provést kontrolu v souladu zavedených bezpečnostních opatření vyžadovaných na Dodavateli těmito Bezpečnostními pravidly a poskytnout potřebnou součinnost. Tento odstavec se neaplikuje, pokud je Dodavatel v rozsahu předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. c), d), f) nebo g) Zákona,
c. umožnit Objednateli provést po vzájemné dohodě v rozsahu předmětu plnění testy dostupnosti, důvěrnosti a integrity dat, informací a jiných zdrojů Dodavatele, které jsou využívány k poskytování předmětu plnění, a poskytnout potřebnou součinnost,
d. zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu s těmito Bezpečnostními pravidly.

A.12 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

A.13 Výměna informací

1. Dodavatel se zavazuje, že:
a. veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů,
b. on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty, použitý SSL certifikát, resp. jeho kvalita podléhá schválení ze strany Objednatele.

A.14 Informační povinnost Dodavatele

Dodavatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.

A.15 Likvidace dat

Pokud v rámci plnění předmětu Smlouvy má Dodavatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií na základě tabulky č.1. Přičemž, pokud není určena klasifikace informace, bude použit způsob likvidace pro důležitost aktiva kritickou.

A.16 Povinnosti při ukončení smlouvy

1. Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, podporou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů Objednatele (dále jen „Ukončení smlouvy“).
2. Dodavatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat Objednateli dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „Plán exitu“). Dodavatel se zavazuje Plán exitu po dobu trvání této Smlouvy průběžně aktualizovat a Objednateli vždy při změně jakékoliv skutečnosti uvedené v Plánu exitu předat aktualizovanou verzi Plánu exitu zohledňující tuto změnu. Dodavatel se zavazuje min. 1 x ročně provést export dat v Objednatelem odsouhlasené struktuře, současně předá Objednateli popis struktury dat v podobě, která bude pro Objednatele čitelná a pochopitelná a umožní Objednateli import dat do jiného Objednatelem vybraného systému/řešení.
3. Dodavatel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu exitu za přiměřeného použití vhodných ustanovení této Smlouvy. Závazek dle tohoto ustanovení platí i po ukončení této Smlouvy.
4. Strany se dohodly, že cena za vypracování Plánu exitu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle této Smlouvy.

A.17 Závěrečná ustanovení

Tato Bezpečnostní pravidla jsou v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení těchto Bezpečnostních pravidel stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení těchto Bezpečnostních pravidel a rovněž Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a těchto Bezpečnostních pravidel jako celkem.

A.18 Informace o verzi

Schváleno: Ing. Luboš Průcha, 3. zástupce ředitele Krajského úřadu Jihočeského kraje, Manažer kybernetické bezpečnosti

Datum: 14.04.2025

Tabulka č. 1

<table>
<tr><th></th><th colspan="4">Přípustný způsob likvidace podle úrovně důležitosti aktiva</th></tr>
<tr><th>Nosič informace</th><th>1. Nízká</th><th>2. Střední</th><th>3. Vysoká</th><th>4. Kritická</th></tr>
<tr><td>Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)</td><td>Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.

Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.</td><td colspan="2">Fyzická likvidace:

Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety)</td><td>Odstranění: Vymazání informací, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.</td><td colspan="2" rowspan="3">Fyzická likvidace:
Rozebrání zařízení a zničení nosiče informací.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a podobně)

Kancelářské vybavení (scanery, tiskárny, fax)</td><td>Odstranění: Vymazání informací, reset do továrního nastavení.</td><td>Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).</td></tr>
<tr><td>Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])

Optická média (CD, DVD, HD-DVD, BLU-RAY)

Elektronická média (flash paměti)</td><td>Odstranění: Smazání dat na úrovni souborového systému.</td><td>Přepsání: Přepsání dat.
V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů

Fyzická likvidace.</td><td colspan="2">Fyzická likvidace: Zničení nosiče informací.</td></tr>
<tr><td rowspan="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.

Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
</table>