Příloha č. 2

BEZPEČNOSTNÍ OPATŘENÍ

1. Úvod

Tato příloha smlouvy ji doplňuje a stanovuje bezpečnostní opatření zejména pro naplnění požadavků vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, (dále jen „ZoKB“), a prováděcích vyhlášek č. 408/2025 Sb. o regulovaných službách a č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „VyKB“).

2. Bezpečnostní požadavky

2.1. Účel

1. Tato příloha smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro poskytovatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi objednatelem a poskytovatelem. Požadavky na poskytovatele jsou definovány dle platné právní úpravy, především pak dle ZoKB a VyKB pro režim nižších povinností.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků dle ZoKB, VyKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, zahájí bez zbytečného odkladu po výzvě kterékoli smluvní strany jednání k uzavření písemného dodatku smlouvy zohledňující takové požadavky. Smluvní strany berou na vědomí, že poskytovatel plní smlouvu osobně jako fyzická osoba, a bezpečnostní požadavky se uplatní přiměřeně tomuto faktu.

2.2. Obecné bezpečnostně provozní požadavky

Poskytovatel se při plnění ze smlouvy pro objednatele zavazuje plnit následující povinnosti:

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro poskytovatele ze ZoKB a VyKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a dále v souladu s relevantními bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) objednatele;
2. působit jako zodpovědná kontaktní osoba pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze smlouvy a této přílohy a související komunikace mezi smluvními stranami;
3. provádět veškeré činnosti osobně; pokud by objednatel udělil písemné svolení se zapojením třetí osoby, je poskytovatel povinen tuto osobu smluvně zavázat k dodržení bezpečnostních povinností minimálně v rozsahu této přílohy a souvisejících ustanovení smlouvy, přičemž za jednání takové osoby odpovídá poskytovatel, jako by plnění poskytoval sám;
4. seznámit se s platnými předpisy a bezpečnostními požadavky stanovenými smlouvou a jejími přílohami a prokazatelně je dodržovat;
5. poskytnout objednateli součinnost při identifikaci a hodnocení rizik spravovaných aktiv v místě plnění a navrhovat opatření k minimalizaci nebo odstranění zjištěných rizik;
6. zaznamenávat a na vyžádání objednateli poskytnout veškeré podstatné okolnosti související s předmětem plnění dle smlouvy (technické záznamy, logy, konfigurace apod.);

7. přistupovat k aktivům objednatele pouze na základě bezpečnostní zásady tzv. „potřeba vědět“ (need-to-know principle), pouze v rozsahu nezbytném pro provádění servisu;
8. garantovat dostupnost, důvěrnost a integritu dat, se kterými při servisu pracuje;
9. průběžně detekovat technické zranitelnosti a konfigurační nesoulady; postup pro nasazování bezpečnostních aktualizací a minimalizaci rizik se řídí touto smlouvou a pokyny objednatele;
10. uchovávat provozní data v souladu s legislativou ČR;

2.3. Oprávnění užívat data

1. Poskytovatel zpracovává data objednatele pouze v rozsahu nezbytném pro plnění smlouvy. Zpracování na vlastních technických prostředcích poskytovatele (např. servisní notebook) je přípustné pouze za předpokladu, že poskytovatel tato zařízení prokazatelně chrání proti neoprávněnému přístupu třetích osob (např. silným přístupovým heslem, šifrováním pevného disku a aktualizovaným antivirem). Předávání dat třetím osobám nebo jejich ukládání do veřejných cloudových úložišť bez předchozího písemného souhlasu objednatele je zakázáno.
2. Poskytovatel se zavazuje nakládat s daty pouze v souladu se smlouvou a příslušnými právními předpisy.
3. Licenční podmínky k softwaru instalovanému na zařízeních objednatele se řídí autorskými právy výrobců.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Objednatel je oprávněn provádět hodnocení, kontroly a audity bezpečnostních opatření zavedených poskytovatelem v souvislosti s plněním této smlouvy. Poskytovatel je povinen poskytnout objednateli (nebo jím pověřeným osobám) plnou součinnost.
2. V případě zjištění nesouladů se smluvní strany bez zbytečného odkladu vzájemně informují a dohodnou se na nápravném plánu a termínech jeho realizace.

2.5. Povinnosti v řízení změn

1. Poskytovatel provádí veškeré změny v konfiguraci lokální sítě, uživatelských stanic či zálohování výhradně na základě požadavků nebo po předchozím prokazatelném odsouhlasení informatikem objednatele.
2. Významné změny (např. v topologii lokální sítě) je poskytovatel povinen předem písemně nebo e-mailem oznámit objednateli.

2.6. Zvládání bezpečnostních událostí a incidentů

Poskytovatel se při poskytování plnění pro objednatele zavazuje, že:

1. bez zbytečného odkladu informuje kontaktní osobu objednatele o všech bezpečnostních událostech a incidentech, které mají nebo by mohly mít dopad na bezpečnost lokální sítě, počítačů nebo dostupnost služeb; oznamování porušení zabezpečení osobních údajů se řídí článkem VI. smlouvy;
2. na případnou žádost objednatele poskytne technickou součinnost při detekci a zvládání událostí; ohlašování incidentů dozorovému orgánu provádí výhradně objednatel;
3. při technických zásazích postupuje tak, aby nedošlo k destrukci logů a dat, a bylo možné jejich případné využití pro forenzní účely (zajištění stop);

4. byl-li incident způsoben činností nebo zanedbáním povinností ze strany poskytovatele, navrhne poskytovatel bezodkladně nápravná opatření k zamezení jeho opakování.

2.7. Informační povinnost a povinnosti při výměně informací

1. Poskytovatel průběžně poskytuje informatikům objednatele informace a podklady nezbytné pro bezpečný provoz pobočky, včetně informací o relevantních hrozbách a zjištěných zranitelnostech; zjištěné zranitelnosti bez zbytečného odkladu oznámí a navrhne přiměřená technická nápravná opatření.
2. Veškerá komunikace a výměna citlivých provozních informací (předávání přístupových hesel, konfigurací sítě apod.) probíhá dohodnutými bezpečnými kanály (např. šifrované e-maily, osobní předání, bezpečné úložiště archivu) s přiměřeným zajištěním důvěrnosti, integrity a dostupnosti.
3. Poskytovatel je povinen informovat objednatele o významných změnách na své straně, které by mohly ovlivnit bezpečnost plnění smlouvy.

2.8. Specifikace podmínek pro řízení kontinuity činností, zálohování a obnovu dat

1. Požadavky na pravidelné lokální zálohování uživatelských dat, konfigurací síťových prvků a parametry tohoto zálohování jsou závazně upraveny v příloze č. 1 této smlouvy.
2. V případě narušení kontinuity poskytovatel bezodkladně spolupracuje na obnově systému z poslední funkční zálohy.

2.9. Bezpečnost lidských zdrojů

1. Poskytovatel se zavazuje dodržovat přísnou mlčenlivost o všech citlivých informacích a datech v souladu s článkem VI. smlouvy.
2. Přístupy do vnitřního IT prostředí objednatele přiděluje, spravuje a odebírá výhradně informatik objednatele.
3. Přístupové údaje (jména, hesla, certifikáty) smí poskytovatel používat jen v nezbytném rozsahu pro výkon servisní činnosti a nesmí je sdílet s žádnou třetí osobou.

2.10. Požadavky na systémovou a provozní bezpečnostní dokumentaci

1. Součástí plnění poskytovatele je přiměřená technická součinnost při dokumentování aktuálního stavu a bezpečnostního nastavení IT infrastruktury místa plnění. Na žádost objednatele poskytovatel předá v dohodnutém termínu a formátu zejména:
   a) aktuální přehled spravovaných koncových zařízení, síťových prvků a lokálního softwaru včetně verzí operačních systémů;
   b) technickou dokumentaci a schémata úprav realizovaných v zapojení lokální sítě v rozsahu nezbytném pro zajištění jejich další údržby;
   c) přehled lokálních integrací a přístupů, např. nastavení síťových tiskáren, přístupy na lokální úložiště apod.
2. Při ukončení platnosti smlouvy nebo na výzvu objednatele před jejím ukončením je poskytovatel povinen poskytnout plnou součinnost potřebnou k bezproblémovému převzetí správy lokální sítě objednatelem nebo novým poskytovatelem.
3. V rámci součinnosti při ukončení smlouvy poskytovatel předá nebo bezpečně zlikviduje veškeré autentizační a přístupové údaje k systémům a prvkům objednatele.

4. Součinnost podle této kapitoly poskytuje poskytovatel v rámci sjednané paušální ceny za služby.

2.11. Fyzická ochrana a bezpečnost prostředí

1. Poskytovatel se zavazuje v budovách objednatele dodržovat režim návštěv v neveřejných prostorách a bezpečnostní požadavky na řízený přístup do bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče.
2. Poskytovatel se zavazuje, že v budovách objednatele neponechá volně dostupná instalační, záložní nebo archivní média ani interní provozní dokumentaci k předmětu plnění této smlouvy.

2.12. Požadavky na řízení přístupu

1. Přidělení oprávnění k přístupu poskytovateli musí být řízeno zásadou tzv. „potřeba vědět“ a přístup nesmí být sdílen s jinými osobami.
2. Poskytovatel se zavazuje, že do informačních systémů objednatele neinstaluje ani v nich nebude užívat žádné komponenty třetích stran ani nástroje (např. pro vzdálenou správu), které nebyly předem písemně odsouhlaseny objednatelem nebo nejsou součástí dohodnutého plnění.
3. Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit programový kód mající za cíl narušení integrity, dostupnosti nebo důvěrnosti systémů objednatele.
4. Poskytovatel se zavazuje chránit autentizační prostředky, přístupové certifikáty a údaje k systémům objednatele před zneužitím či ztrátou.

2.13. Likvidace dat

Způsob bezpečné likvidace a vracení dat po ukončení smlouvy se řídí ustanovením článku V. odst. 2 smlouvy.

2.14. Sankce

Sankce za porušení povinností plynoucích z této přílohy se řídí článkem VI. odst. 11. smlouvy.

2.15. Způsob distribuce dokumentů poskytovateli

Poskytovatel má právo vyžádat si od objednatele bezpečnostní politiky a dokumenty ISMS relevantní k předmětu smlouvy. Tyto dokumenty představují důvěrné informace ve smyslu čl. VI smlouvy a poskytovatel je povinen je po ukončení smlouvy vrátit nebo prokazatelně zlikvidovat.

… ……
podpis poskytovatele

……
podpis objednatele