Příloha č. 2

Doložka

o bezpečnostních požadavcích na provádění vývojových prací (služeb) na tvorbě softwaru pro SZIF

Smluvní strany se dohodly, že jejich vzájemný právní vztah z výše uvedené Smlouvy o poskytování služeb dále jen („Smlouva"), bude podléhat režimu dodržování níže uvedených bezpečnostních ujednání:

1. Účel

Účelem této dohody je definovat v souvislosti se Smlouvou a jejím plněním, postupy a základní principy zajištění bezpečnosti při provádění vývojových prací na tvorbě aplikací a softwaru (dále jen SW) pro SZIF.

2. Klasifikace informačního systému SZIF

Poskytovatel bere na vědomí, že informační systém SZIF je na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a návazných vyhlášek v platném znění (dále jen „zákon o kybernetické bezpečnosti) zařazen do kategorie „Významný informační systém".

3. Základní povinnosti Poskytovatele

Poskytovatel se zavazuje:

3.1. zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v rámci plnění předmětu smlouvy, zejména o interních procesech objednatele a dalších skutečnostech interního charakteru, ať už se týkají Objednatele nebo jeho klientů. Tato povinnost trvá i po skončení smluvního vztahu,

3.2. při vývoji, testování, úpravách a provozu SW, zohlednit bezpečnostní požadavky a principy vyplývající z normy ISO/IEC 27001:2013 a zákona o kybernetické bezpečnosti,

3.3. zachovávat princip oddělení prostředí vývoje, testování a provozu. Jsou-li k testování užita provozní data, je zhotovitel povinen zajistit jejich modifikaci tak, aby nemohla být zneužita,

3.4. dodržovat ochranu dat použitých pro testování, aby byla data pečlivě vybrána, kontrolována a chráněna proti zneužití,

3.5. zpracovat popis informací, které mu mají být poskytnuty nebo zpřístupněny a metody poskytování nebo zpřístupňování informací,

3.6. dodržovat požadavky na ochranu duševního vlastnictví a autorských práv,

3.7. zavést dohodnutý soubor opatření, včetně řízení přístupu, přezkoumávání výkonnosti, monitorování, podávání zpráv a provádění auditů,

3.8. dodržet požadavky na řízení bezpečnostních událostí a incidentů, zejména oznámení události / incidentu a spolupráce při nápravě v rámci řízení bezpečnostních událostí a incidentů SZIF,

3.9. provádět ochranu záznamů (logů, auditních logů), aby byly záznamy chráněny před ztrátou, zničením, falšováním, neoprávněným přístupem a neoprávněným vydáním v souladu s legislativními, předpisovými, smluvními požadavky a požadavky týkajícími se činnosti SZIF,

3.10. při změně programového vybavení v rámci vývoje či servisu SW vytvořit zálohu původního programového vybavení včetně jeho konfigurace na datovém médiu stanovené Objednatelem,

3.11. dodržovat ochranu osobních údajů, aby bylo soukromí a ochrana údajů zajištěna v souladu s požadavky příslušné legislativy a nařízení,

3.12. dodržovat regulaci kryptografických opatření, aby byla stanovená kryptografická opatření používána v souladu se všemi příslušnými dohodami, legislativou a předpisy,

3.13. při změně / úpravě SW v rámci životního cyklu vývoje SW byly změny řízeny a kontrolovány pomoci formálních postupů řízení změn,

3.14. u jím vyvíjeného/servisovaného SW provádět přezkoumání penetračním testováním a posouzení bezpečnostních zranitelností. Tyto testování doloží příslušným protokolem.

4. Závěrečná ustanovení

Poskytovatel je povinen prokazatelně seznámit s těmito Bezpečnostními požadavky své pracovníky a pracovníky subdodavatelských firem, které jsou ve smluvním vztahu s Poskytovatelem a podílí se na plnění této smlouvy. Poskytovatel odpovídá za kontrolu dodržování těchto Bezpečnostních požadavků.

Tato Doložka o Bezpečnostních požadavcích na provádění vývojových prací (služeb) na tvorbě SW pro SZIF je nedílnou součásti výše uvedené Smlouvy jako její Příloha č. 2, která je vyhotovena v elektronické podobě, každá ze smluvních stran obdrží elektronický originál. ~~, která je sepsána ve 2 vyhotoveních, z nichž každá ze smluvních stran obdrží po 1 vyhotovení~~.