Dodatek č. 1

k Rámcové dohodě o poskytování IT specialistů pro zajištění a zvyšování úrovně kybernetické bezpečnosti č. 2023/07185

Česká pošta, s.p.

se sídlem:	Politických vězňů 909/4, 225 99 Praha 1
IČO:	47114983
DIČ:	CZ47114983
zastoupen:	Ing. Miroslavem Štěpánem, zástupcem ředitele Ing. Jaroslavem Hlouškem, ředitelem úseku ICT a eGovernment
zapsán v obchodním rejstříku u:	Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení:	[redacted]

dále jako „**Objednatel**“ nebo „**ČP**“

a

T-SOFT a.s.

se sídlem:	Za Brumlovkou 1559/5, Praha 4, 140 00
IČO:	40766314
DIČ:	CZ40766314
zastoupen:	Ing. Michalem Vaněčkem, Ph.D., MBA, místopředsedou představenstva
zapsán v obchodním rejstříku u:	Městského soudu v Praze, oddíl B, vložka 15233
bankovní spojení:	[redacted]

dále jako „**Dodavatel**“

dále každý jednotlivě také jen „**Smluvní strana**“, nebo společně jen „**Smluvní strany**“ uzavírají ve smyslu § 1901 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“) a § 222 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), tento Dodatek č. 1 (dále jen „**Dodatek**“), kterým se doplňuje a mění text Rámcové dohody o poskytování IT specialistů pro zajištění a zvyšování úrovně kybernetické bezpečnosti č. 2023 / 07185 ze dne 27. 9. 2023 (dále jen „**Smlouva**“), a to následovně:

Preambule

Vzhledem k narůstajícímu množství požadavků, je nutné, aby Dodavatel mohl poskytnout současně více specialistů současně.

1 Předmět Dodatku

Smluvní strany se dohodly, že dosavadní text Přílohy č. 1 Smlouvy – Specifikace a jmenný seznam specialistů – se ruší a nahrazuje se v celém rozsahu novým zněním dle přílohy tohoto Dodatku.

2 Závěrečná ustanovení

2.1 Smluvní strany shodně prohlašují, že obsahem Dodatku není podstatná změna Smlouvy v tom smyslu, že Dodatkem nedochází k umožnění účast jiných dodavatelů nebo ovlivnění výběru dodavatele v původním zadávacím řízení, pokud by zadávací podmínky původního zadávacího řízení odpovídaly této změně, změna dále nemění ekonomickou rovnováhu závazku ze Smlouvy ve prospěch Dodavatele a nevede k významnému rozšíření rozsahu plnění veřejné zakázky.

2.2 Ustanovení v tomto Dodatku nabývají platnosti dnem podpisu Smluvními stranami a účinnosti dnem uveřejnění tohoto Dodatku v registru smluv. Plnění předmětu Smlouvy v rozsahu tohoto Dodatku v době od platnosti Dodatku do jeho účinnosti se považuje za plnění podle Smlouvy a práva a povinnosti z něj vzniklé se řídí Smlouvou.

2.3 Nedílnou součástí tohoto Dodatku je jeho příloha s názvem:

Příloha č. 1 Smlouvy: Specifikace a jmenný seznam specialistů

2.4 Je-li Dodatek vyhotoven v listinné podobě, je vyhotoven ve dvou stejnopisech s platností originálu a každá ze Smluvních stran obdrží po jednom (1) stejnopisu. Pokud je Dodatek vyhotoven v elektronické podobě, Smluvní strany obdrží elektronický originál opatřený elektronickými podpisy obou Smluvních stran, včetně časového razítka dle příslušných právních předpisů.

NA DŮKAZ TOHO, že Smluvní strany s obsahem Dodatku souhlasí, rozumí mu a zavazují se k jeho plnění, připojují své podpisy a prohlašují, že tento Dodatek byl uzavřen podle jejich svobodné a vážné vůle prosté tísně, zejména tísně finanční.

V Praze

_____

Ing. Jaroslav Hloušek
ředitel úseku ICT a eGovernment
Česká pošta, s.p.

V Praze

_____

Ing. Michal Vaněček, Ph.D., MBA
místopředseda představenstva
T-SOFT a.s.

V Praze

_____

Ing. Miroslav Štěpán
zástupce ředitele
Česká pošta, s.p.

Příloha č. 1 – Specifikace a jmenný seznam specialistů

Každý specialista musí mít minimálně středoškolské vzdělání s maturitou a účast na min. jedné zakázce dle požadavků v Zadávacím řízení.

1) Projektový manažer bezpečnosti
Praxe: Minimálně 3 roky praxe s řízením projektů v oblasti bezpečnosti informací
Dovednosti a znalosti: Prediktivní, agilní a hybridní přístupy k řízení projektů
Certifikace: Platné osvědčení pro oblast projektové metodologie PRINCE 2 (min. úroveň Foundation) nebo ekvivalent (PMI, IPMA)

2) Manažer kybernetické bezpečnosti
Praxe: Minimálně 5 let praxe s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací
Dovednosti a znalosti: Znalost ISO/IEC 27000, řízení rizik, řízení kontinuity činností, právních a regulatorních požadavků ZoKB, VoKB, zpracování osobních údajů a ochrany investic, hodnocení kybernetické bezpečnosti a znalost reportingování zákonných požadavků kybernetické bezpečnosti
Certifikace: Minimálně jedna z certifikací: CISM, CDPSE, CRISC od ISACA, CISSP, CCSP, SSCP od (ISC)², Manažer BI (akreditační schéma ČIA)

3) Bezpečnostní architekt
Praxe: Minimálně 5 let praxe s navrhováním a implementací bezpečnostních opatření a zajišťováním architektury bezpečnosti
Dovednosti a znalosti: Znalost ISO/IEC 27000, ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na KB, právních a regulatorních požadavků ZoKB, VoKB, zpracování osobních údajů, definicím rizik a rizikových scénářů, ochrany investic a znalost reportingování zákonných požadavků kybernetické bezpečnosti
Certifikace: Minimálně jedna z certifikací: CISM, CRISC od ISACA, CISSP od (ISC)², Security+, CySA+, CASP+ od CompTIA

4) Bezpečnostní specialista Aplikační architekt
Praxe: Minimálně 3 roky praxe s navrhováním a implementací bezpečnostních opatření a aplikační bezpečnosti
Dovednosti a znalosti: Znalost aplikační bezpečnosti s ohledem na návrh vhodných technických opatření v rámci infrastruktury ČP, a to především s ohledem na již využívané technologie

5) Bezpečnostní specialista na penetrační testování
Praxe: Minimálně 3 roky praxe s navrhováním a implementací bezpečnostních opatření a aplikační bezpečnosti
Dovednosti a znalosti: Znalost a praktické zkušenosti s oblastí penetračního testování webových aplikací, webových služeb mobilních aplikací dle: -OWASP Web Security Testing Guide, OWASP Application Security Verification Standard (www.owasp.org). -OSSTMM (Open-Source Security Testing Manual - www.isecom.org). -IS Auditing Procedure Security Assessment–Penetration Testing And Vulnerability Analysis (www.isaca.org). -ISO/IEC 27001 (BS 7799). -ISO/IEC 27002 (ISO/IEC 17799:2005). -BS 25999-1:2006.
Certifikace: Minimálně jedna z certifikací: CSWAE, OSWP od Offensive Security, CPT od IACRB, GPEN, GWAPT, GCPN od GIAC, CEH od ECCouncil, CompTIA pentest+

6) Bezpečnostní specialista na Operační systémy
Praxe: Minimálně 3 roky praxe v oboru ICT a hardeningu OS
Dovednosti a znalosti: Znalost OS MS Windows server/desktop, OS Linux a SunSolaris s ohledem na zajištění bezpečnosti
Certifikace: Minimálně jedna z certifikací: Microsoft Certified Security Engineer, Microsoft Certified Technology Specialist (MCTS)

7) Bezpečnostní specialista Cloud security
Praxe: Minimálně 3 roky praxe v oboru ICT a CLOUD prostředí OS
Dovednosti a znalosti: Obecný přehled na použití CLOUD prostředí mimo perimetr Objednatele s detailnější znalostí MS AZURE, bezpečnostní architektury a zajištění odolnosti tohoto prostředí. Principy a zkušenost s přípravou strategie použití externích CLOUD prostředí v rámci podniku s ohledem na zajištění KII.
Certifikace: Minimálně jedna z certifikací: Microsoft Certified Cybersecurity Expert, nebo Microsoft certified Azure security Engineer Associate

8) Bezpečnostní auditor
Praxe: Minimálně 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti
Dovednosti a znalosti: Znalost postupů auditu implementace zákona o kybernetické bezpečnosti a jeho vyhlášky, ČSN EN ISO/IEC 27001:2014.
Certifikace:

Minimálně jedna z certifikací: CISA od ISACA, CIA, CGAP od ČIA (IIA), ISO 27001 Lead Auditor, CopTia Security+, Certified in Risk and Information Systems Control (CRISC), Auditor BI (akreditační schéma ČIA)

9) Network architekt bezpečnosti
Praxe:
Minimálně 5 let praxe v ICT oboru síťové bezpečnosti
Dovednosti a znalosti:
Znalost bezpečnostních technologií, jejich implementace v praxy pro NGFW, Přístupová řešení 802.1X, Win Infrastructure Security, PAM, IDM, EMM …)

10) Bezpečnostní specialista SIEM
Praxe:
Minimálně 3 roky praxe v oblasti SIEM
Dovednosti a znalosti:
Vyhodnocování procesů v prostředí v reálném čase

11) Bezpečnostní analytik
Praxe:
Minimálně 2 roky praxe v oblasti zpracování analýz informační nebo kybernetické bezpečnosti
Dovednosti a znalosti:
Znalost metodologie a rámce auditu infomační bezpečnosti, akvizice, vývoj a nasazení ICT, řízení provozu, údržby a služeb ICT, ochrany aktiv, hodnocení kybernetické bezpečnosti, metody testování a vzorkování, analyzování výsledků analýz a znalost reportování stavu zákonných požadavků
Certifikace:
Platné osvědčení specialisty informační bezpečnosti, minimálně na úrovni Foundation ISO/ICE 27001, nebo adekvátní certifikace a platné osvědčení fyzické osoby pro přístup k utajovaným informacím minimálně stupně utajení důvěrné podle zákona č. 412/2005 Sb.

12) Specialista pro řízení kontinuity činnosti
Praxe:
Minimálně 2 roky praxe v oblasti provádění zátěžových testů, testování business kontinuity a zpracování souvisejících analýz
Dovednosti a znalosti:
Znalost podnikových procesů a jejich integrace v ICT, řízení bezpečnosti a rizik a znalost navrhování a implementace bezpečnostních opatření

13) Technický specialista bezpečnosti
Praxe:
Minimálně 2 roky praxe v oblasti bezpečnosti serverů, operačních systémů, síťových služeb a řízení zranitelnosti
Dovednosti a znalosti:
Znalost architektury informačních a komunikačních systémů, hardware komponent a nástrojů architektury, operačních systémů a SW, bezpečnost komunikací a sítí a znalost řízení identit a přístupů

Pozice	**Jméno a příjmení**
Projektový manažer bezpečnosti	[redacted]
Manažer kybernetické bezpečnosti	[redacted]
Bezpečnostní architekt	[redacted]
Bezpečnostní specialista Aplikační architekt	[redacted]
Bezpečnostní specialista na penetrační testování	[redacted]
Bezpečnostní specialista na Operační systémy	[redacted]
Bezpečnostní specialista Cloud security	[redacted]
Bezpečnostní auditor	[redacted]
Network architekt bezpečnosti	[redacted]
Bezpečnostní specialista SIEM	[redacted]
Bezpečnostní analytik	[redacted]
Specialista pro řízení kontinuity činnosti	[redacted]
Technický specialista bezpečnosti	[redacted]