# Příloha č. 11

# Povinné role v týmu dodavatele, jejich kvalifikace a reference

## Vedoucí projektu (Project Manager)

Popis role: Vedoucí projektu je odpovědný za celkové řízení projektu, koordinaci týmu, komunikaci s KZ, plánování a sledování harmonogramu, rozpočtu a souladu s požadavky smlouvy. Dohlíží na implementaci bezpečnostních opatření dle PPK KZ, bezpečnostního standardu KZ a zajišťuje soulad s legislativními požadavky (zákon o kybernetické bezpečnosti, ISO 9001, ISO 27001).

Minimální kvalifikace:

Vysokoškolské vzdělání v oboru IT, managementu IT nebo příbuzném technickém směru (minimálně bakalářský titul) a nejméně 3 roky odborné praxe v řízení vývoje nebo ekvivalentní odborná praxe (min. 5 let v řízení vývoje).

Certifikace v oblasti projektového řízení (např. PMP, PRINCE2 Practitioner, IPMA Level C nebo obdobné).

Znalost problematiky kybernetické bezpečnosti na úrovni legislativních požadavků ČR (zákon č. 181/2014 Sb.
a vyhláška č. 82/2018 Sb.) a standardů ISO 27001.

Reference: úspěšně řídil minimálně 2 projekty v oblasti vývoje a implementace softwaru pro veřejný sektor nebo ideálně zdravotnictví v hodnotě nad 2 miliony Kč bez DPH v posledních 5 letech. Reference musí obsahovat jméno zadavatele, popis projektu, dobu trvání a okolnost úspěšné akceptace díla.

## Architekt softwarového řešení (Software Architect)

Popis role: Architekt softwarového řešení navrhuje technickou architekturu systému, zajišťuje jeho kompatibilitu s infrastrukturou KZ, soulad s bezpečnostními požadavky (např. kryptografická ochrana, řízení přístupů) a aplikaci zásad bezpečného vývoje dle standardů KZ. Podílí se na testování a ověření bezpečnosti řešení.

Minimální kvalifikace:

Vysokoškolské vzdělání v oboru IT nebo příbuzném technickém směru (minimálně bakalářský titul) a nejméně 3 roky odborné praxe při návrhu a vývoji software nebo ekvivalentní odborná praxe (min. 5 let v oblasti návrhu softwarových systémů).

Certifikace v oblasti softwarové architektury nebo kybernetické bezpečnosti (např. TOGAF, CISSP nebo obdobné).

Prokazatelná zkušenost s návrhem systémů splňujících standardy ISO 27001 a požadavky na kybernetickou bezpečnost dle české legislativy.

Reference: pracoval na minimálně 2 projektech vývoje softwaru pro veřejný sektor nebo zdravotnické IS
v posledních 5 letech, kde navrhl architekturu systému s důrazem na bezpečnost a dostupnost. Reference musí obsahovat popis technického řešení, jméno zadavatele a dobu realizace.

## Specialista kybernetické bezpečnosti (Cybersecurity Specialist)

Popis role: Specialista na kybernetickou bezpečnost zajišťuje implementaci bezpečnostních opatření dle bezpečnostních standardů KZ, provádí analýzu rizik, řídí penetrační testy, monitorování incidentů a koordinaci reakcí na bezpečnostní události. Garantuje soulad s požadavky zákona o kybernetické bezpečnosti a standardy ISO 27001. Komplexně řídí bezpečnost aktiv, užitých k zajištění a podpoře dodávky.

Minimální kvalifikace:

Vysokoškolské vzdělání v oboru IT bezpečnosti nebo příbuzném technickém směru (nejméně bakalářský titul)
a nejméně 3 roky odborné praxe při řízení kybernetické bezpečnosti nebo ekvivalentní odborná praxe (min. 5 let v oblasti kybernetické bezpečnosti).

Certifikace v oblasti kybernetické bezpečnosti (např. CISSP, CISM, CEH, OSCP nebo obdobné).

Zkušenost s řízením a audity kybernetické bezpečnosti a implementací opatření podle zákona o kybernetické bezpečnosti.

Reference: zajišťoval kybernetickou bezpečnost minimálně na 2 projektech vývoje nebo podpory softwaru pro veřejný sektor nebo zdravotnictví v posledních 5 letech, včetně řízení penetračních testů nebo řešení bezpečnostních incidentů. Reference musí zahrnovat jméno zadavatele, popis činností a výsledek.

## Vedoucí vývoje (Lead Developer)

Popis role: Vedoucí vývoje je odpovědný za technické vedení vývojového týmu, zajištění kvality kódu, implementaci softwarového řešení na určených platformách a soulad s technickými standardy KZ. Dohlíží na proces vývoje, peer-review kódu, integritu a testování řešení v souladu s částí „Vývoj, akvizice a údržba“ bezpečnostního standardu KZ. Koordinuje vývoj tak, aby byl kompatibilní s infrastrukturou KZ a použitými technologiemi.

Minimální kvalifikace:

Vysokoškolské vzdělání v oboru IT nebo příbuzném technickém směru (minimálně bakalářský titul) a 3 roky odborné praxe při vývoji software nebo ekvivalentní odborná praxe (min. 5 let v oblasti vývoje softwaru).

Prokazatelná odborná způsobilost v technologiích a platformách relevantních pro zakázku, doložená certifikátem.

Zkušenost s vývojem softwaru v regulovaném prostředí (např. zdravotnictví, veřejný sektor) a znalost zásad bezpečného vývoje (např. OWASP Top 10, Secure SDLC).

Reference: Dodavatel prokáže, že vedoucí vývoje vedl vývojový tým minimálně na 2 projektech v oblasti vývoje softwaru v posledních 5 letech, kde byly použity platformy shodné nebo obdobné těm, které jsou specifikovány
v technické příloze zadávací dokumentace. Reference musí zahrnovat jméno zadavatele, popis použité technologie, roli osoby v projektu a výsledek (např. úspěšné nasazení systému).