HLAVNÍ MĚSTO PRAHA
MAGISTRÁT HLAVNÍHO MĚSTA PRAHY
Odbor právní podpory
Oddělení svobodného přístupu k informacím

MHMPXPR16M62

[redacted]

Váš dopis zn./ze dne:
28. 11. 2025
Č. j.:
MHMP 1311446/2025
Sp. zn.:
S-MHMP 1264292/2025

Vyřizuje/tel.:
JUDr. Ivana Červová
236 002 174
Počet listů/příloh: **-/0**
Datum:
19.12.2025

Poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,

Vážená paní,

hlavní město Praha – Magistrát hlavního města Prahy (dále jen „MHMP“), jako povinný subjekt ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“), obdržel Vaši žádost ze dne 28. 11. 2025 o poskytnutí informace (dále jen „žádost“). Z důvodu vyhledávání a sběru informací v jiných úřadovnách povinného subjektu (MHMP) odlišných od odboru vyřizujícího Vaši žádost, byla prodloužena lhůta pro poskytnutí informace, a to přípisem ze dne 3. 12. 2025 pod č. j. MHMP 1277940/2025.

Ve Vaší žádosti uvádíte:

„…v souvislosti s realizovaným šetřením i na dalších krajských úřadech v České republice, si dovoluji požádat o poskytnutí níže uvedených informací.
…
V textu této žádosti je dále pro označení krajského úřadu používán souhrnný pojem „úřad“, a dále pro označení Odboru informatiky nebo Oddělení informatiky souhrnný pojem „IT útvar“.

1. ***Strategie ICT a digitalizace krizového řízení.***

• Jakou formou je ve Vaší Strategii ICT zahrnuta problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncepci Smart Cities?
• Pokud je tato problematika ve Vaší Strategii ICT obsažena, jakým způsobem dochází k plnění těchto cílů?
• Lze plnění těchto cílů dohledat veřejně např. na webových stránkách nebo specializovaném portále Vašeho úřadu?

Sídlo: Mariánské nám. 2/2, 110 00 Praha 1
Pracoviště: Jungmannova 36/31, 110 00 Praha 1
Kontaktní centrum: 800 100 000, fax: 236 007 157
E-mail: posta@praha.eu, ID DS: 48ia97h

• Jaké moderní technologie nebo koncepty Smart Cities považuje Váš úřad za klíčové pro rozvoj krizového řízení např. prostřednictvím IoT senzorů, umělé inteligence nebo cloudových služeb?
• Obsahuje Strategie ICT Vašeho úřadu také cíle v oblasti síťové bezpečnosti a kybernetické odolnosti, a to v kontextu podpory digitalizace krizového řízení?
• Má Váš úřad zpracovaný plán rozvoje infrastruktury např. modernizace aktivních prvků, segmentace sítě, modernizace síťové páteře?
• Jakou formou jsou tyto cíle financovány a vyhodnocovány z hlediska investiční efektivity a udržitelnosti?

2. Koncepce Smart Cities a rozvoj ICT v oblasti krizového řízení.

Koncepční testování inovativních bezpečnostních technologií

• Jaké nové technologie v oblasti bezpečnosti ICT infrastruktury Váš úřad testuje nebo jaké jsou na Vašem úřadu implementovány přístupy např. Zero Trust, behaviorální monitoring, endpoint detection?
• Využívá Váš úřad testovací prostředí (sandbox) pro ověřování nových řešení před nasazením do provozu?
• Mají tyto technologie i souvislost s krizovým řízením?
• Spolupracuje Váš úřad s NÚKIB, univerzitami či komerčními partnery v oblasti testování bezpečnostních inovativních technologií, pokud ano s jakými ve Vašem kraji?
• Jakým způsobem IT útvar Vašeho úřadu stanovuje priority a finanční plánování pro testování nových bezpečnostních technologií?

Komplexní rozvoj metropolitních dispečinků jako center situačního a krizového řízení

• Jakým způsobem IT útvar Vašeho úřadu technicky nebo bezpečnostně podporuje městské či regionální dispečerské systémy např. formou metodické podpory, sdílení infrastruktury, zajištění konektivity, šifrovaného přenosu dat nebo zálohovacích služeb?
• Má Váš úřad zpracovaný plán modernizace síťové infrastruktury např. aktivních prvků, serverů, datových linek, které jsou využívány také pro datové propojení a komunikaci s dispečerskými systémy měst a složek Integrovaného záchranného systému (IZS)?
• Má Váš úřad zřízen centrální bezpečnostní dohled např. SOC nebo SIEM, a pokud ano, zahrnuje tento dohled i monitoring nebo koordinaci bezpečnostních událostí z informačních systémů, které využívají města nebo dispečinky v rámci krizového řízení?
• V rámci zajištění technologické infrastruktury a informačních toků pro krizové řízení krajské úřady spravují také účelové informační systémy pro krizové řízení, včetně systémů v režimu utajovaných informací. Krajské úřady tedy zajišťují provoz, bezpečnost a správu informačního systému krizového řízení, včetně částí fungujících v režimu utajovaných informací podle zákona č. 412/2005 Sb. Je tento systém součástí technického zázemí krajského dispečinku nebo krizového štábu? Zajišťuje provoz tohoto systému přímo Váš úřad IT útvarem nebo prostřednictvím externího dodavatele např. na základě servisní smlouvy?

Zajištění kompatibility technologických řešení v rámci krizového řízení
• Jakým způsobem IT útvar Vašeho úřadu zajišťuje interoperabilitu systémů mezi úřadem, městy, složkami IZS a státní správou?
• Jakým způsobem IT útvar Vašeho úřadu vyhodnocuje bezpečnostní rizika a zajišťuje kompatibilitu síťové architektury s národními systémy?

Zavádění vzdálených přístupů pro PČR do MKDS obcí

• Koordinuje Váš úřad podporu pro zavádění vzdálených přístupů PČR do městských kamerových systémů, pokud ano, jaký odbor a jakým způsobem?
• Kdo na Vašem úřadu schvaluje technické parametry a finanční rámec těchto propojení na Vašem úřadu a jaký odbor má za tyto činnosti odpovědnost?

Bezpečné regionální privátní datové sítě

• Podílí se Váš úřad na rozvoji a rozšiřování bezpečných regionálních datových sítí pro sdílení citlivých dat?
• Jakým způsobem (formou) IT útvar řeší správu a upgrade aktivních síťových prvků (firewally, switche, routery)?
• Jakou formou zabezpečení jsou řešena přístupová práva, audit a šifrování datových přenosů?
• Využívá Váš úřad SIEM pro centralizovanou správu logů a bezpečnostních událostí?
• Jak jsou tyto sítě financovány a udržovány (interní rozpočet / dotační programy)?
• Jakým způsobem Váš IT útvar vyhodnocuje návratnost a efektivitu těchto investic?
• Je součástí těchto procesů také finanční a investiční plánování modernizace sítě na Vašem úřadu?

Metodika zahrnutí bezpečnostního kritéria do činností úřadu

• Má Váš úřad implementovanou interní metodiku pro hodnocení bezpečnostních dopadů IT projektů v souladu s platnou legislativou v oblasti kybernetické bezpečnosti v ČR a EU?
• Jakou formou je na Vašem úřadu zajištěno projektové řízení IT zahrnující síťovou bezpečnost, řízení rizik a rozpočtové dopady?
• Jakým způsobem Váš úřad školí pracovníky ICT a vedoucí odborů v oblasti síťové bezpečnosti a krizové komunikace?

Kompatibilita inovativních technologických řešení

• Jakým způsobem IT útvar Vašeho úřadu zajišťuje technickou a bezpečnostní kompatibilitu nových řešení vycházejících z koncepce Smart Cities a digitalizace krizového řízení se stávající síťovou infrastrukturou úřadu?
• Jakým způsobem IT útvar plánuje modernizaci a financování síťové infrastruktury v souvislosti s digitální transformací?“

V souladu s ustanovením § 14 odst. 5 písm. d) InfZ Vám v součinnosti odborem informatických činností MHMP a odborem bezpečnosti MHMP poskytujeme požadované informace, a to následovně.
K jednotlivým otázkám Vaší žádosti uvádíme:

• Jakou formou je ve Vaší Strategii ICT zahrnuta problematika zaměřená na digitalizaci krizového řízení v návaznosti na moderní technologie a koncepci Smart Cities?
Problematika digitalizace krizového řízení je ve Strategii ICT hl. m. Prahy zahrnuta koncepčně a průřezově, zejména v oblasti rozvoje ICT architektury, integrace informačních systémů, práce s daty a zajištění kybernetické bezpečnosti. Tyto oblasti vytvářejí technologické a organizační předpoklady pro podporu agend krizového řízení v návaznosti na moderní technologie a principy Smart Cities.

• Pokud je tato problematika ve Vaší Strategii ICT obsažena, jakým způsobem dochází k plnění těchto cílů?
Plnění cílů probíhá prostřednictvím systematické realizace opatření a projektů vyplývajících z informační koncepce. Jedná se hlavně o rozvoj infrastruktury, integraci systémů, digitalizaci služeb a posilování

bezpečnosti ICT, přičemž jednotlivé aktivity jsou realizovány v návaznosti na průběžně identifikované potřeby úřadu.

• Lze plnění těchto cílů dohledat veřejně např. na webových stránkách nebo specializovaném portále Vašeho úřadu?
Ano, plnění těchto cílů lze v omezeném rozsahu dohledat prostřednictvím veřejně dostupných strategických dokumentů a informací o jejich naplňování, zejména v rámci projednávání hodnotících zpráv orgány hl. m. Prahy. Vybrané informace o projektech v oblasti Smart Cities jsou rovněž zveřejňovány na specializovaných webových stránkách hl. m. Prahy. Detailní technické a provozní informace nejsou z důvodu bezpečnosti a charakteru řešení veřejně publikovány.

• Jaké moderní technologie nebo koncepty Smart Cities považuje Váš úřad za klíčové pro rozvoj krizového řízení např. prostřednictvím IoT senzorů, umělé inteligence nebo cloudových služeb?
Veškeré technologie využívané v rámci hl. m. Prahy pro krizové řízení jsou v souladu s možnostmi úřadu a jeho materiálně technologickým vybavením. Odbor bezpečnosti MHMP sleduje trendy technologického rozvoje a v součinnosti s příslušnými odbory MHMP a zainteresovanými subjekty reaguje na jejich případné možné implementace do procesů HMP pro krizové řízení.

• Obsahuje Strategie ICT Vašeho úřadu také cíle v oblasti síťové bezpečnosti a kybernetické odolnosti, a to v kontextu podpory digitalizace krizového řízení?
Ano obsahuje.

• Má Váš úřad zpracovaný plán rozvoje infrastruktury např. modernizace aktivních prvků, segmentace sítě, modernizace síťové páteře?
Ano má, a to v rámci informační koncepce.

• Jakou formou jsou tyto cíle financovány a vyhodnocovány z hlediska investiční efektivity a udržitelnosti?
Financování probíhá z rozpočtu MHMP a následně je periodicky vyhodnocováno cyklicky v souvislosti s obměnami končících podpor výrobce konkrétní technologie.

• Jaké nové technologie v oblasti bezpečnosti ICT infrastruktury Váš úřad testuje nebo jaké jsou na Vašem úřadu implementovány přístupy např. Zero Trust, behaviorální monitoring, endpoint detection?
S ohledem na skutečnost, jejich zveřejnění by mohlo vést k narušení bezpečnostních opatření a zvýšení rizika neoprávněného zásahu do chráněných systémů, sdělujeme, že je implementována většina bezpečnostních technologií.

• Využívá Váš úřad testovací prostředí (sandbox) pro ověřování nových řešení před nasazením do provozu?
Ano, využívá.

• Spolupracuje Váš úřad s NÚKIB, univerzitami či komerčními partnery v oblasti testování bezpečnostních inovativních technologií, pokud ano s jakými ve Vašem kraji?
Ne, v oblasti testování bezpečnostních inovativních technologií nespolupracuje.

• Jakým způsobem IT útvar Vašeho úřadu stanovuje priority a finanční plánování pro testování nových bezpečnostních technologií?
Stanovování priorit a plánování financí probíhají strategicky v rámci plnění informační koncepce a současně v konkrétních případech dle aktuálních mimořádných bezpečnostních hrozeb.

• *Jakým způsobem IT útvar Vašeho úřadu technicky nebo bezpečnostně podporuje městské či regionální dispečerské systémy např. formou metodické podpory, sdílení infrastruktury, zajištění konektivity, šifrovaného přenosu dat nebo zálohovacích služeb?*
V případě MČ a zřizovaných organizací všemi dotazovanými způsoby, vždy dle konkrétního projektu, systému a příslušné organizace.

• *Má Váš úřad zpracovaný plán modernizace síťové infrastruktury např. aktivních prvků, serverů, datových linek, které jsou využívány také pro datové propojení a komunikaci s dispečerskými systémy měst a složek Integrovaného záchranného systému (IZS)?*
Plán pro tyto konkrétní prvky zpracovaný není, řeší se operativně v návaznosti na aktualizace infrastruktury u zájmových subjektů. Tím je zajištěna kontinuita.

• *Má Váš úřad zřízen centrální bezpečnostní dohled např. SOC nebo SIEM, a pokud ano, zahrnuje tento dohled i monitoring nebo koordinaci bezpečnostních událostí z informačních systémů, které využívají města nebo dispečinky v rámci krizového řízení?*
S ohledem na případná bezpečnostní rizika sdělujeme pouze, že má SOC i SIEM.

• *V rámci zajištění technologické infrastruktury a informačních toků pro krizové řízení krajské úřady spravují také účelové informační systémy pro krizové řízení, včetně systémů v režimu utajovaných informací. Krajské úřady tedy zajišťují provoz, bezpečnost a správu informačního systému krizového řízení, včetně částí fungujících v režimu utajovaných informací podle zákona č. 412/2005 Sb. Je tento systém součástí technického zázemí krajského dispečinku nebo krizového štábu? Zajišťuje provoz tohoto systému přímo Váš úřad IT útvarem nebo prostřednictvím externího dodavatele např. na základě servisní smlouvy?*
Je zajištěno prostřednictvím externích dodavatelů, na základě servisních a rozvojových smluv.

• *Jakým způsobem IT útvar Vašeho úřadu zajišťuje interoperabilitu systémů mezi úřadem, městy, složkami IZS a státní správou?*
Interoperabilita zajištěna na základě součinnosti s příslušnými subjekty.

• *Jakým způsobem IT útvar Vašeho úřadu vyhodnocuje bezpečnostní rizika a zajišťuje kompatibilitu síťové architektury s národními systémy?*
Vyhodnocení rizik probíhá na základě pravidelných interních jednání s podklady získanými z monitorovacích a bezpečnostních systémů. Zajištění kompatibility probíhá na základě plnění legislativních a technických požadavků provozovatelů národních systémů.

• *Koordinuje Váš úřad podporu pro zavádění vzdálených přístupů PČR do městských kamerových systémů, pokud ano, jaký odbor a jakým způsobem?*
Ano. Kompetence je rozdělena mezi odbor bezpečnosti MHMP a odbor informatických činností MHMP. Odbor informatických činností MHMP má v kompetenci přidělování práv přístupu do MKS dle stanovených pravidel.

• *Kdo na Vašem úřadu schvaluje technické parametry a finanční rámec těchto propojení na Vašem úřadu a jaký odbor má za tyto činnosti odpovědnost?*
Odbor informatických činností MHMP ve spolupráci s odborem bezpečnosti MHMP.

• *Podílí se Váš úřad na rozvoji a rozšiřování bezpečných regionálních datových sítí pro sdílení citlivých dat?*
Nepodílí.

• *Jakým způsobem (formou) IT útvar řeší správu a upgrade aktivních síťových prvků (firewally, switche, routery)?*
Jedná se o neveřejnou a strategickou informaci.

• *Jakou formou zabezpečení jsou řešena přístupová práva, audit a šifrování datových přenosů?*
Jedná se o neveřejnou a strategickou informaci.

• *Využívá Váš úřad SIEM pro centralizovanou správu logů a bezpečnostních událostí?*
Ano, využívá.

• *Jak jsou tyto sítě financovány a udržovány (interní rozpočet / dotační programy)?*
Financování probíhá z rozpočtu MHMP a z dostupných dotačních programů, následně je vše periodicky vyhodnocováno.

• *Jakým způsobem Váš IT útvar vyhodnocuje návratnost a efektivitu těchto investic?*
Je periodicky vyhodnocováno cyklicky v souvislosti s obměnami končících podpor výrobce konkrétní technologie.

• *Je součástí těchto procesů také finanční a investiční plánování modernizace sítě na Vašem úřadu?*
Ano, je.

• *Má Váš úřad implementovanou interní metodiku pro hodnocení bezpečnostních dopadů IT projektů v souladu s platnou legislativou v oblasti kybernetické bezpečnosti v ČR a EU?*
v současné době je zahájen proces úpravy interních dokumentů v souvislosti s nabytím účinnosti nového zákona o KB č. 264/2025 Sb**.**

• *Jakou formou je na Vašem úřadu zajištěno projektové řízení IT zahrnující síťovou bezpečnost, řízení rizik a rozpočtové dopady?*
Projektové řízení je realizováno systémově prostřednictvím standardizovaných pracovních postupů, které zajišťují jednotný přístup k implementaci a správě informačních technologií. Tato činnost je realizována jako kontinuální služba, přičemž jednotlivé projekty vycházejí z průběžné identifikace potřeb úřadu a aktuálního kontextu projektového okolí. Specifika síťové bezpečnosti jsou řešena v součinnosti s odpovědnými rolemi dle zákona o kybernetické bezpečnosti, jejichž úkolem je zajistit integraci bezpečnostních opatření a metodiku řízení rizik do celého životního cyklu IT projektů. Rozpočtové dopady jsou řízeny v rámci standardních finančních mechanismů MHMP s důrazem na provozní udržitelnost a efektivitu vynaložených prostředků.

• *Jakým způsobem Váš úřad školí pracovníky ICT a vedoucí odborů v oblasti síťové bezpečnosti a krizové komunikace?*
Tato školení zajišťuje odbor personální MHMP, a to cestou interních a externích vzdělávacích kurzů.

• *Jakým způsobem IT útvar Vašeho úřadu zajišťuje technickou a bezpečnostní kompatibilitu nových řešení vycházejících z koncepce Smart Cities a digitalizace krizového řízení se stávající síťovou infrastrukturou úřadu?*
IT útvar zajišťuje technickou a bezpečnostní kompatibilitu nových řešení prostřednictvím uplatňování architektonických, technických a bezpečnostních standardů MHMP. Nová řešení jsou posuzována z hlediska souladu se stávající síťovou a technologickou infrastrukturou a s požadavky vyplývajícími z platné legislativy v oblasti kybernetické bezpečnosti.

• *Jakým způsobem IT útvar plánuje modernizaci a financování síťové infrastruktury v souvislosti s digitální transformací?*
Toto je plánováno v rámci informační koncepce.

S pozdravem

Mgr. Rudolf Kramář, Ph.D.
ředitel odboru právní podpory
podepsáno elektronicky