MĚSTSKÁ ČÁST PRAHA 14
ÚŘAD MĚSTSKÉ ČÁSTI
Odbor právních a kontrolních činností

Bratří Venclíků 1073, 198 21 Praha 9 | IČ: 00231312 | www.praha14.cz

[redacted]

Váš dopis značka: 66 BR 1913 MC14.DUB.RC /2025
Spisová značka: INFZ 65/2025
Číslo jednací: UMCP14/25/171653/OPKČ/MRV

Vyřizuje: Bc. Soňa Mrvová
E-mail: sona.mrvova@praha14.cz
Telefon: 281 005 247

Praha, 25. srpna 25

Sdělení o poskytnutí informace dle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Městská část Praha 14, Bratří Venclíků 1073, 198 21 Praha 9 (dále jen „povinný subjekt"), obdržela žádost ze dne 11. 8. 2025 podanou podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, ve které jste požádala o objasnění výrazu „Nesmím na Vás vstupovat" a „Kolegyně si Vás ztotožní" a dále jste požádala o informace ve věci „Kybernetická bezpečnost na Radnici".

Povinný subjekt poskytuje informace.

Obrat „Nesmím na Vás vstupovat" byl v dané situaci použit jako zjednodušené vyjádření skutečnosti, že bez zákonného důvodu nemůže úředník samostatně vyhledávat nebo čerpat údaje o občanovi z registrů a informačních systémů. Vstup je roven nahlížení na údaje o držiteli občanského průkazu.

K dalšímu obratu „Kolegyně si Vás ztotožní" uvádíme, že se jedná o úřední postup, jehož smyslem je ověření totožnosti občana. V praxi spočívá ve srovnání údajů uvedených v předloženém dokladu totožnosti (např. občanský průkaz, cestovní pas) s údaji vedenými ve státních registrech. Účelem je zajistit, aby úřad jednal skutečně s Vámi jako s jednoznačně identifikovanou osobou.

V oblasti kybernetické bezpečnosti se Úřad městské části Praha 14 řídí legislativou a standardy závaznými pro orgány územní samosprávy, inspirace informacemi poskytovanými Českou správou sociálního zabezpečení není pro úřad relevantní, neboť tato instituce vykonává zcela odlišnou agendu. Pro Vaši informaci přikládáme samostatný zpracovaný materiál k problematice kybernetické bezpečnosti úřadu, který podrobně uvádí povinnosti úřadu a používané standardy.

Bc. Soňa Mrvová
vedoucí úseku kontroly a stížností OPKČ

Soňa Mrvová
Digitálně podepsal Soňa Mrvová
Datum: 2025.08.25 11:17:21 +02'00'

Příloha
Dle textu

KYBERNETICKÁ BEZPEČNOST NA NAŠÍ RADNICI

(informační rámec a závazky)

Naše zásada

Kybernetická bezpečnost je pro Úřad městské části Praha 14 absolutní prioritou. Chráníme dostupnost, důvěrnost a integritu informací ve všech provozovaných informačních systémech (IS) a službách, a to jak interních, tak poskytovaných občanům. Tato informace shrnuje právní rámec, normy a praktické požadavky, jimiž se řídíme.

1) Český právní rámec (aktuální a připravovaná úprava)

• Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) – hlavní právní předpis v oblasti kybernetické bezpečnosti do 31. 10. 2025. Ukládá povinnosti vybraným subjektům (např. správcům významných IS, prvků kritické informační infrastruktury) včetně bezpečnostních opatření, hlášení incidentů a vedení bezpečnostní dokumentace.

• Zákon č. 264/2025 Sb., o kybernetické bezpečnosti – nový ZKB účinný od 1. 11. 2025 (transpozice směrnice NIS2). Rozšiřuje okruh povinných osob, zavádí nové role a procesy (řízení rizik, řízení dodavatelů), a navazuje na prováděcí předpisy NÚKIB. Na jejich základě upravíme interní předpisy, smlouvy a technická opatření.

• Prováděcí předpisy NÚKIB a navazující úpravy:

– Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (do 31. 10. 2025). Definuje bezpečnostní opatření, kategorii incidentů, reaktivní opatření a náležitosti podání.

– Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

– Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (ve znění č. 315/2014 Sb.).

– „Cloudové" předpisy NÚKIB pro orgány veřejné moci (OVM):

▪ Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu OVM (zařazení poptávaného cloudu podle dopadů).

▪ Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro OVM využívající služby poskytovatelů cloud computingu (minimální pravidla řízení rizik, smluv a provozu v cloudu).

• Související české předpisy pro digitalizaci a IS VS:

– Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS).

– Zákon č. 12/2020 Sb., o právu na digitální služby.

– Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (datové schránky).

– Zákon č. 111/2009 Sb., o základních registrech.

– Zákon č. 499/2004 Sb., o archivnictví a spisové službě + vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby (včetně novel).

– Zákon č. 127/2005 Sb., o elektronických komunikacích (provoz sítí a služby, incidenty, spolupráce s ČTÚ).

– Zákon č. 106/1999 Sb., o svobodném přístupu k informacím (bezpečné zveřejňování, anonymizace).

– Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (je-li relevantní).

2) Rámec EU a mezinárodní závazky
• GDPR – Nařízení (EU) 2016/679, obecné nařízení o ochraně osobních údajů. Vyžaduje minimalizaci, zákonnost, integritu a důvěrnost zpracování a zavádí oznamování porušení zabezpečení osobních údajů (data breaches).
• eIDAS – Nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru (podpisy, pečetě, časová razítka, kvalifikované služby); eIDAS 2 – Nařízení (EU) 2024/1183 (evropská digitální identita/peněženka).
• NIS2 – Směrnice (EU) 2022/2555 o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v Unii. V ČR implementována novým ZKB (od 1. 11. 2025).
• Akt o kybernetické bezpečnosti – Nařízení (EU) 2019/881 (ENISA, rámec pro evropské kyberbezpečnostní certifikace).
• CER – Směrnice (EU) 2022/2557 o odolnosti kritických subjektů (relevantní pro infrastrukturu a krizové řízení).

3) Normy a standardy (doporučený referenční rámec)
Pro řízení kybernetické a informační bezpečnosti budeme systematicky vycházet z osvědčených norem a rámců:
• ISO/IEC 27001:2022 – systém řízení bezpečnosti informací (ISMS) a ISO/IEC 27002:2022 – soubor bezpečnostních kontrol.
• ISO/IEC 27005:2022 – řízení rizik bezpečnosti informací.
• ISO/IEC 27701:2019 – rozšíření ISMS o systém řízení ochrany osobních údajů (PIMS) navázaný na GDPR.
• ISO 22301:2019 – systém řízení kontinuity činností (BCMS).
• NIST Cybersecurity Framework 2.0 (2024) – doplňkový praktický rámec (Identify–Protect–Detect–Respond–Recover + Governance).
• ETSI EN 319 401 a ETSI EN 319 411-1/-2 – rámec a požadavky na důvěryhodné služby (relevantní pro kvalifikované poskytovatele a certifikáty podle eIDAS).

4) Praktické požadavky pro náš úřad (shrnutí dopadů)
• Zavedený ISMS: politika bezpečnosti, definované role (Statutární orgán, Garant KB, CISO, vlastníci aktiv/procesů), řízení rizik a kontrol.
• Klasifikace aktiv a informací; inventarizace IS/assetů (včetně cloudových) a datových toků; stanovení „přiměřených" opatření dle rizik.
• Technická a organizační opatření: řízení přístupů (IAM, MFA), segmentace sítí, aktualizace a zranitelnosti, zálohování a obnova, šifrování, logování a detekce (SIEM), hardening, bezpečné vývojové a provozní praktiky.
• Incident management: definice incidentu, oznamování (NÚKIB / ÚOOÚ, pokud se jedná o osobní údaje), evidence a post-incidentní analýzy.
• Kontinuita a odolnost: analýza dopadů (BIA), plány kontinuity/obnovy (BCP/DRP), testování a cvičení (včetně kybercvičení).
• Bezpečnost v cloudu: zařazení dle vyhl. 315/2021 Sb., uplatnění pravidel dle vyhl. 190/2023 Sb.,

smluvní a technické zajištění (šifrování, rezidence dat, dohledatelnost, auditovatelnost).
• Dodavatelský řetězec: prověřování a smluvní záruky, bezpečnostní požadavky ve veřejných zakázkách, pravidelný dohled a reporting.
• Ochrana osobních údajů: DPIA, minimalizace, pseudonymizace/šifrování, řízení souhlasů a práv subjektů údajů, oznamování porušení.
• Školení a povědomí: role-based školení, pravidelné testy (phishing), interní kampaně.
• Audit, testování a zlepšování: interní audity, penetrační testy a zátěžové testy, management nálezů, metriky a přezkum vedením.
• Dokumentace: bezpečnostní politika, směrnice přístupů, klasifikace informací, pravidla správy záznamů a spisové služby, provozní dokumentace IS, plán reakce na incidenty apod.

5) Jak budeme postupovat v roce 2025
• Do 31. 10. 2025 udržujeme plnou shodu s „dosavadním" ZKB (181/2014 Sb.) a vyhl. 82/2018 Sb.
• Paralelně dokončíme analýzu dopadů nového ZKB (264/2025 Sb.) a prováděcích vyhlášek; připravíme aktualizace interních předpisů, smluvních vzorů a technických kontrol.
• Pro systémy v cloudu platí průběžně vyhlášky 315/2021 Sb. a 190/2023 Sb. – provádíme opakované posouzení úrovně a souladu.

Závěr
Kybernetická bezpečnost je kontinuální proces řízený riziky a odpovědností vedení. Všechna oddělení, odbory a úseky úřadu spolupracují na naplnění právních povinností i interních standardů – s cílem poskytovat spolehlivé digitální služby občanům a chránit jejich data. Tento rámec pravidelně aktualizujeme dle legislativních změn a vývoje hrozeb.