Ministerstvo zdravotníctva Slovenskej republiky (ďalej len „MZ SR“) v zmysle ustanovenia § 3 písm. m) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB“) stojí v postavení prevádzkovateľa základnej služby a v zmysle ustanovenia § 4 písm. b) ZoKB je zároveň ústredným orgánom v oblasti kybernetickej bezpečnosti (ďalej len „ústredný orgán“), ktorý zodpovedá za zabezpečenie kybernetickej bezpečnosti v sektore zdravotníctva. MZ SR v zmysle ustanovenia § 5 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoITVS“) vykonáva ako orgán riadenia správu informačných technológií verejnej správy. Z uvedeného postavenia MZ SR vyplýva povinnosť implementovať požiadavky ZoKB a ZoITVS.

Cieľom obstarávaného predmetu zákazky je zabezpečiť súlad bezpečnostných opatrení s vyššie vymedzenou legislatívou a zároveň odstrániť nedostatky zistené auditom kybernetickej bezpečnosti[1], vykonaného v zmysle ustanovenia § 29 ZoKB, ako aj plnenie úloh v rozsahu pôsobnosti MZ SR ako ústredného orgánu a orgánu riadenia, a to:

a) Realizáciou inventarizácie, klasifikácie a kategorizácie informačných aktív[2], analýzou rizík (ďalej len „AR“) a analýzou dopadov (ďalej len „BIA“). Ich spísanie do ucelenej formy v 3 úrovniach, a to:
   a. MZ SR ako prevádzkovateľ základnej služby,
   b. MZ SR v postavení ústredného orgánu sektoru Zdravotníctvo,
   c. pre časť 79 organizácií v zakladateľskej, zriaďovateľskej a akcionárskej pôsobnosti MZ SR.
b) Vypracovaním bezpečnostnej dokumentácie pre oblasti vymedzené ustanovením § 20 ods. 3 ZoKB a ustanovením § 14 až § 23 ods. 1 a 2 ZoITVS pre MZ SR.
c) Vypracovaním návrhu stratégie kybernetickej bezpečnosti v zmysle vykonanej AR/BIA podľa bodu a) a akčného plánu pre implementáciu prioritných opatrení predmetnej stratégie v zmysle členenia 3 úrovní.

Poskytnutím služieb tvoriacich predmet tejto zákazky MZ SR zabezpečí vykonanie rozboru stavu informačnej a kybernetickej bezpečnosti prostredníctvom analýzy rizík, vrátane syntézy v návrhu stratégie kybernetickej bezpečnosti spolu s akčným plánom pre implementáciu jej prioritných opatrení.[3]

Predmet zákazky bude realizovaný s cieľom zabezpečenia komplexnej kybernetickej bezpečnosti, riadenia bezpečnostných rizík, rozvoja úrovne informačnej a kybernetickej bezpečnosti MZ SR i sektora zdravotníctva a zabezpečenia jeho súladu s legislatívou ZoITVS a ZoKB so zreteľom na governance informačnej a kybernetickej bezpečnosti. Predmet zákazky je spolufinancovaný z Európskeho fondu regionálneho rozvoja, prioritná os 7 - Informačná spoločnosť, výzvy “*č. OPII-2021/7/16-DOP Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS*”, kód projektu v ITMS+ 311071BNT5.[4]

Súčasťou predmetu zákazky je využitie nástroja na monitorovanie a riadenie bezpečnostných incidentov poskytnutého Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“) z projektu „*Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy*“[5] (ďalej len “CMRKB”) pre evidenciu informačných aktív, ich klasifikácie, kategorizácie IS a sietí a riadenie identifikovaných rizík a incidentov. Požadované informácie z vykonanej analýzy je potrebné doplniť do samostatného offline klientskeho modulu alebo online klientskeho web portálu. Offline klientsky modul slúži na spracovanie informácií v prostredí organizácie a umožňuje

[1] V rámci súčinnosti poskytne MZ SR zhotoviteľovi po podpise Zmluvy o dielo informácie potrebné na plnenie predmetu zákazky.
[2] Výklad pojmu „aktíva“. Hmotné, alebo nehmotné statky, ktoré pre organizáciu priamo, alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu. (Aktívami sú všeobecne najmä: procesy, know-how, dáta, informácie, software, služby, objekty, technologické komponenty a priestory organizácie).
[3] V zmysle metodiky a inštitucionálneho rámca tvorby verejných stratégií https://www.mirri.gov.sk/sekcie/investicie/narodny-investicny-plan/vladne-materialy/metodika-a-institucionalny-ramec-tvorby-verejnych-strategii/index.html
[4] https://www.itms2014.sk/schvalena-zonfp?id=5fa03177-267b-4ea9-866c-218c5b219e85
[5] https://www.uvo.gov.sk/vyhladavanie-zakaziek/detail/434214

export vybraných údajov na portál Vládneho informačného systému kybernetickej bezpečnosti (ďalej len „VISKB“) buď automaticky prostredníctvom „Application Programming Interface“ (API) alebo formou exportu do zašifrovaného súboru, ktorý je následne možné importovať na portál VISKB prostredníctvom jeho webového rozhrania. Jeho úlohou je správa údajov v nižšie uvedenom rozsahu a export vybraných údajov (uvedených v centrálnom module VISKB) v zašifrovanej forme prostredníctvom webového rozhrania portálu do centrálneho modulu. Modul umožňuje evidenciu aktív organizácie a ich manažment, vrátane ich klasifikácie a kategorizácie, manažment rizík, poskytovanie reportov a štatistických prehľadov. Modul má podobu samostatne spustiteľnej (portable) aplikácie bez potreby inštalácie v operačnom systéme Windows.

Miestom realizácie predmetu zákazky je sídlo MZ SR a jeho detašované pracovisko na Bárdošovej ulici č. 2 v Bratislave.

Hlavnými aktivitami predmetu zákazky v zmysle vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov sú:

- Analýza a Dizajn,
- Implementácia a Testovanie,
- Nasadenie.

Popis východiskovej situácie

V zozname základných služieb má MZ SR zaradené systémy vymedzené v tabuľke 1.

Tabuľka 1 Základné služby MZ SR

Názov informačného systému	Kód MetaIS	Typ ISVS
Centrálny Informačný Systém Inšpektorátu kúpeľov a žriediel Ministerstva zdravotníctva Slovenskej republiky	isvs_4853	agendový
CSM	isvs_7752	ekonomický a administratívny chod inštitúcie
DALI - Informačný systém pre kategorizáciu	isvs_4851	agendový
Human	isvs_4849	ekonomický a administratívny chod inštitúcie
Informačný systém pre databázu referenčných cien pre potreby Ministerstva zdravotníctva Slovenskej republiky	isvs_4852	ekonomický a administratívny chod inštitúcie
Informačný systém SPIN	isvs_9321	ekonomický a administratívny chod inštitúcie
Informačný systém STATA	isvs_4850	ekonomický a administratívny chod inštitúcie

Názov informačného systému	Kód MetaIS	Typ ISVS
Intranet Ministerstva zdravotníctva Slovenskej republiky	isvs_4848	ekonomický a administratívny chod inštitúcie
Portál Kategorizácia	isvs_4845	prezentačný
Webové sídlo Ministerstva zdravotníctva Slovenskej republiky	isvs_4826	prezentačný

Okrem vyššie vymedzených systémov prevádzkuje MZ SR aj ostatné informačné systémy, ktoré sú dostupné v Centrálnom metainfromačnom systéme verejnej správy (MetaIS[6]), vrátane bežných podporných systémov (ako napr.: doménový radič „Windows Active Directory“, mailový systém a vnútorná infraštruktúra IKT), ktoré majú v prípade ich narušenia negatívny vplyv na fungovanie MZ SR. Pre aktíva nie je spracovaná analýza rizík a analýza dopadov.

Bezpečnostná dokumentácia

V súčasnosti má MZ SR vypracované a účinné interné riadiace akty (ďalej len „IRA“) pre oblasť informačnej a kybernetickej bezpečnosti z roku 2014, ktoré nereflektujú aktuálne požiadavky v zmysle vecne príslušnej legislatívy. Konkrétny zoznam IRA:

- Bezpečnostný projekt MZ SR
- Evidencia informačných systémov
- Bezpečnostná politika
- Personálna bezpečnosť
- Riadenie aktív
- Riadenie rizík
- Riadenie fyzickej a objektovej bezpečnosti
- Riadenie logických prístupov
- Riadenie komunikácie a prevádzky
- Riadenie aktualizácie IKT a tretie strany
- Riadenie incidentov
- Riadenie kontinuity
- Terminologický slovník informačnej bezpečnosti

Ďalšia úprava IRA po roku 2014:

- Služobný predpis č. 1/2015 MZ SR - Základné pravidlá bezpečného spracúvania údajov a používania prostriedkov IT používateľmi aktív zo dňa 1.6.2015
- Opatrenie vedúcej služobného úradu č. 1/2015 zo dňa 20.8.2015 (povinnosť oboznámiť sa s služobného predpisu +/2015)
- Služobný predpis Ministerstva zdravotníctva Slovenskej republiky č. 1/2016 (Základné pravidlá správy informačných systémov a služieb administrátormi systému) zo dňa 5.1.2016
- Opatrenie generálneho tajomníka služobného úradu č. 1/2022 na zabezpečenie kontinuálneho riadenia úrovne informačnej a kybernetickej bezpečnosti v prostredí Ministerstva zdravotníctva SR zo dňa 15.5.2022

[6] https://metais.vicepremier.gov.sk/cilist/ISVS?page=1&count=20&filter%5BglobalSearch%5D=%257B%257D

- Smernica Ministerstva zdravotníctva Slovenskej republiky o postupe pri tvorbe, pripomienkovaní, uzatváraní a evidovaní zmlúv zo dňa 15.7.2022
- Smernica Ministerstva zdravotníctva Slovenskej republiky o stanovení pravidiel a podmienok prideľovania a používania zariadení informačno-komunikačnej techniky zo dňa 18.7.2022.

Organizačný poriadok

MZ SR v súlade so všeobecne záväznými právnymi predpismi a Štatútom MZ SR ustanovuje vnútorné organizačné členenie organizačných útvarov, v ktorom je začlenený aj Odbor informačnej bezpečnosti.[7] Tento je v súčasnosti obsadený a pozostáva z riaditeľa a 3 referentov. Projekt môže poukázať na potrebu zabezpečenia ďalších bezpečnostných rolí napr. pre účely bezpečnostného monitoringu, riadenia bezpečnostných incidentov, posudzovania technických zraniteľností alebo výkon interných bezpečnostných auditov a pod. formou rozšírenia odboru.

Do plnenia opisu predmetu zákazky budú zapojení biznis garanti MZ SR. MZ SR pre riadenie a prevádzku projektu disponuje s nasledovnými zdrojmi.

RIS RR

Rozpočtový informačný systém riadenia rizík (kód MetaIS „isvs_9015“), ktorý je implementovaný v prostredí MZ SR a naprieč organizáciami v zakladateľskej, zriaďovateľskej a akcionárskej pôsobnosti MZ SR.

Pracovná skupina na podporu pri zvyšovaní úrovne kybernetickej bezpečnosti v sektore zdravotníctva

Pracovnú skupinu zriaďuje Bezpečnostný výbor MZ SR[8] pre oblasť informačnej a kybernetickej bezpečnosti. Členmi pracovnej skupiny sú zástupcovia útvarov organizačných jednotiek MZ SR a nasledujúcich organizácií: Univerzitná nemocnica Bratislava, Národné centrum zdravotníckych informácií a Asociácia nemocníc. Pracovná skupina na základe zásady odbornosti najmä:

a) plní úlohy uložené predsedom Výboru. podpredsedom Výboru alebo vedúcim pracovnej skupiny;
b) poskytuje súčinnosť, usmernenia a odbornú/kvalifikovanú podporu pri zvyšovaní úrovne kybernetickej bezpečnosti v sektore zdravotníctva;
c) napomáha identifikovať, rozvíjať a realizovať projekty s cieľom zvyšovať kybernetickú bezpečnosť v sektore zdravotníctva.

Spôsob realizácie aktivít projektu

Obstarávaný predmet zákazky je v súlade s horizontálnym projektom č. OPII-2021/7/16-DOP “Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS”, pričom predmetom zákazky je:

1. Analyzovať aktuálny stav v oblasti riadenia informačnej a kybernetickej bezpečnosti a jeho zosúladenie s požiadavkami vecne príslušnej legislatívy.
2. Vykonať analýzu relevantných rizík v zmysle metodiky[9] Národného bezpečnostného úradu (ďalej len „NBÚ“) a analýzu dopadov (AR/BIA) zameranú na 3 úrovne:
   a) MZ SR v postavení prevádzkovateľa základnej služby a orgánu riadenia v oblasti informačných technológií verejnej správy,
   b) MZ SR v postavení ústredného orgánu sektoru Zdravotníctvo,

[7] https://health.gov.sk/?organizacna-struktura
[8] Vestník MZ SR 2021, čiastka 11-14 z dňa 11. júna 2021, 69 ročník.
https://www.health.gov.sk/Zdroje?/Sources/dokumenty/vestniky_mz_sr/2021/vestnik-2021-11-14.pdf
[9] https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf

c) pre množinu 79 organizácií v zakladateľskej, zriaďovateľskej a akcionárskej pôsobnosti MZ SR ako celok, ktoré sú prevádzkovateľom základnej služby (zo 79 organizácií je 28 v sektore zdravotníctvo, 56 v sektore verejná správa a z toho 5 je prienikom zaradenia v oboch sektoroch, pozn. aktuálny stav).

Požadovaným výstupom realizácie predmetu zákazky bude prehľad identifikovaných rizík s návrhom možných opatrení na ich minimalizáciu na všetkých úrovniach, vrátane

a) identifikácie aktív a ohodnotenia ich kritickosti,
b) klasifikácie aktív a kategorizácie informačných systémov (ďalej len "IS") a sietí,
c) identifikácie hrozieb a vektorov útokov,
d) analýzy potenciálnych dopadov,
e) identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
f) identifikácie existujúcich opatrení a reziduálnych rizík,
g) návrhu bezpečnostných opatrení na mitigáciu identifikovaných rizík.

3. Na základe AR/BIA v bode 2. spracovať stratégiu informačnej a kybernetickej bezpečnosti pre MZ SR v postavení prevádzkovateľa základnej služby a sektor Zdravotníctvo vrátane roadmapy (akčného plánu) na implementáciu navrhnutých opatrení v zmysle metodiky a inštitucionálneho rámca tvorby verejných stratégií[10]. Vypracovať podklad pre formálne rozhodnutia vedenia MZ SR v oblasti riadenia rizík (o ich akceptácii alebo prijatí adekvátnych opatrení na ich zníženie alebo úplnú elimináciu).
4. Vypracovať požadované IRA a interné dokumenty v slovenskom jazyku elektronicky spracovávané na dátovom nosiči (CD/DVD, USB kľúč, externý prenosný pevný disk s primeranou kapacitou a rozhraním nim. USB 3.0 alebo vyšším a pod.) pre relevantné oblasti riadenia informačnej a kybernetickej bezpečnosti v zmysle IRA – „*Smernica upravujúca tvorbu, vydávanie, publikovanie a evidenciu interných riadiacich aktov Ministerstva zdravotníctva Slovenskej republiky*" platná od dňa 1.10.2018, ktorá tvorí prílohu č. 2 Špecifikácie zákazky.
5. Zaviesť do prostredia MZ SR klientský nástroj (modul) poskytnutý MIRRI z projektu CMRKB pre evidenciu informačných aktív, ich klasifikácie, kategorizácie IS a sietí a riadenie identifikovaných rizík a incidentov.

Implementácia predmetu zákazky bude pozostávať z nasledovných aktivít

Hlavné aktivity:
Aktivita **Analýza a dizajn** bude pozostávať z nasledovných častí:

- analýza aktuálneho stavu informačnej a kybernetickej bezpečnosti a súladu s legislatívnymi požiadavkami,
- inventarizácia a klasifikácia informačných aktív a kategorizácia IS a sietí,
- analýza rizík a analýza dopadov,
- zavedenie procesu riadenia rizík a procesu governance informačnej a kybernetickej bezpečnosti,
- dodávka produktov definovaných v tabuľke 2 na základe dostupných metodík[11] MIRRI,
- analýza zavedenia offline klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.

Aktivita **Implementácia a Testovanie** pozostáva z customizácie klientskeho modulu VISKB, nástroja (Portable App[12]), ktorý umožňuje evidenciu potrebných údajov v oblasti informačnej a kybernetickej bezpečnosti, najmä evidenciu kontaktných údajov a základných údajov o MZ SR, evidenciu aktív, klasifikáciu a kategorizáciu, dáta z AR/BIA, katalóg

[10] https://www.mirri.gov.sk/sekcie/investicie/narodny-investicny-plan/vladne-materialy/metodika-a-institucionalny-ramec-tvorby-verejnych-strategii/index.html
[11] https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostna-dokumentacia-metodiky/index.html
[12] (prenosná aplikácia) softvérový produkt navrhnutý tak, aby sa dal jednoducho presúvať z jedného výpočtového prostredia do druhého

rizík a pod. Jedná sa open source modul VISKB poskytnutý MIRRI[13]. Tento sa v aktivite Implementácia a Testovanie prispôsobí na potreby MZ SR.

Aktivita **Nasadenie** pozostáva z nasadenia vyššie spomínaného klientskeho nástroja evidencie informačných aktív, rizík a incidentov. Základné údaje o organizácii, ako názov organizácie, adresa organizácie, typ organizácie (podľa číselníka typov), poznámka. Kontaktné údaje, ako meno, e-mail, telefón na pracovisko, mobilný telefón, roly osoby (roly podľa číselníka rolí a možnosť textového popisu iných rolí), dostupnosť kontaktu (8x5, 24x7, ...). IPv4 adresy, ako IPv4 adresa alebo rozsah IPv4 adries (adresa siete/dĺžka masky), účel použitia danej adresy (adries).

Zoznam produktov, ktoré sú predmetom zákazky je nasledovný:

Tabuľka 2 Zoznam produktov

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
1.1	Posúdenie súladu s bezpečnostnými požiadavkami podľa ZoKB (vyhlášky NBÚ č. 362/2018 Z. z.) ako aj ZoITVS (vyhlášky č. 179/2020 Z. z.) a návrh strategického akčného plánu úloh na zabezpečenie súladu	Nakoľko bol audit v zmysle ZoKB vykonaný, ide o "pred-audit", resp. posúdenie stavu kybernetickej bezpečnosti aj voči požiadavkám ZoITVS. Výstupom aktivity bude: - Úplný kontrolný zoznam legislatívnych požiadaviek za obe legislatívy a ich súladu s aktuálnym stavom, - Návrh akčného plánu strategických úloh.
1.2	Vypracovanie IRA a prevádzkovej dokumentácie riadenia informačnej a kybernetickej bezpečnosti:	Výstupom aktivity bude interná dokumentácia a IRA uvedené nižšie.
1.2.1	Stratégia kybernetickej bezpečnosti	V štruktúre a v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky NBÚ č. 362/2018 Z. z.
1.2.2	Bezpečnostná politika	V štruktúre a v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky NBÚ č. 362/2018 Z. z.
1.2.3	Smernica pre riadenie informačnej bezpečnosti	IRA ohľadom organizačnej štruktúry (roly) riadenia informačnej a kybernetickej bezpečnosti a základných úloh, povinností a zodpovedností v tejto oblasti.
1.2.4	Klasifikácia informácií a kategorizácia sietí a informačných systémov	IRA pre výkon identifikácie a inventarizácie aktív a následne spôsobu ich klasifikácie a kategorizácie IS a sietí.
1.2.5	Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA)	IRA pre výkon AR/BIA, vrátane definovania základných parametrov (hrozby, dopadové kritéria, spôsob identifikácie a klasifikácie rizík, spôsob definovania RTO a RPO a pod.).

[13] Špecifikácia klientskeho modulu VISKB https://www.uvo.gov.sk/vyhladavanie-dokumentov/detail/3165611

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
1.2.6	Smernica o bezpečnej prevádzke IS a sietí	Bude pokrývať najmä oblasti: - bezpečná správa a prevádzka IS a sietí, - riadenie zmien, - riadenie kapacít, - riadenie záplat a aktualizácii, - zálohovanie dát, - posudzovanie technických zraniteľností, - správa používateľských účtov a riadenie prístupov, - bezpečnostné požiadavky pre prístupové práva a účty privilegovaných používateľov.
1.2.7	Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov	Bude pokrývať procesy bezpečnostného monitoringu a identifikácie bezpečnostných incidentov a kompletný proces ich riadenia.
1.2.8	Politika BCM vrátane stratégie obnovy a BCP a DRP min. pre kritické systémy organizácie	Obsahom bude najmä: Politika BCM, stratégia obnovy, BCP a DRP plány pre kritické systémy.
1.2.9	Bezpečnostný projekt kritických informačných systémov MZ SR	Bezpečnostný projekt kritických (kľúčových) informačných systémov podľa ZoITVS
1.3	Inventarizácia, klasifikácia a kategorizácia	Výstupom aktivity bude realizácia inventarizácie a klasifikácie informačných aktív (vytvorenie zoznamu aktív a ich klasifikácie z pohľadu dôvernosti, integrity a dostupnosti) a kategorizácie IS a sietí na základe klasifikácie. Na aktivite sa budú podieľať aj interní zamestnanci, cieľom predmetu zákazky je aj transfer know-how, aby si bola organizácia schopná klasifikáciu a kategorizáciu následne aktualizovať aj vlastnými silami.
1.4	Vykonanie analýzy rizík a analýzy dopadov	Výstupom bude vykonaná AR/BIA podľa jednotnej smernice (metodiky) pre dátovo-procesné aktíva (biznis agendy) a IKT zdroje, ktoré tieto agendy podporujú. Na AR/BIA sa budú podieľať aj interní zamestnanci, cieľom predmetu zákazky je aj transfer know-how, aby si bola organizácia schopná tieto analýzy opakovane realizovať a aktualizovať aj vlastnými silami.
1.5	Návrh katalógu rizík a spôsobov ich riadenia	Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), ktorý bude obsahovať identifikované riziká z AR/BIA a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík a ich schválenia vedením MZ SR alebo Bezpečnostným výborom ak tento bude zriadený.

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
1.6	Klientsky modul evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov	Implementácia a prispôsobenie klientského modulu poskytnutého MIRRI z projektu CMRKB pre evidenciu informačných aktív, ich klasifikácie, kategorizácie IS a sietí a riadenie identifikovaných rizík a incidentov.
2.1	Analýza kybernetických rizík v sektore zdravotníctvo	Analýza rizík sa bude týkať v členení celý sektor zdravotníctvo[14] s podmnožinami: • Organizácie v pôsobnosti MZ SR (NCZI, ÚVZ a RÚVZ, ďalšie rozpočtové a príspevkové organizácie MZ SR v členení poskytovatelia ústavnej zdravotnej starostlivosti, poskytovatelia ambulantnej ústavnej starostlivosti • Ďalšie organizácie, neštátni poskytovatelia ústavnej zdravotnej starostlivosti, neštátni poskytovatelia ambulantnej zdravotnej starostlivosti • Iné entity (napr. zaoberajúce sa laboratórnymi službami). Oblasti analýzy rizík, • Dôvernosť, integrita a dostupnosť spracúvaných informácií s osobitným dôrazom na osobitnú kategóriu osobných údajov v (zdravotné záznamy)[15] • Dostupnosť poskytovaných služieb / kontinuita činností • Personálne zabezpečenie kybernetickej bezpečnosti • Fyzická a objektová bezpečnosť • Zabezpečovanie súladu s predmetnou legislatívou • Riziká dodávateľských služieb, vývoja a údržby informačných systémov • Riziká riadenia kybernetickej bezpečnosti • Reakcia na bezpečnostné incidenty.
2.2	Návrh stratégie kybernetickej bezpečnosti v sektore zdravotníctvo	Na základe analýzy kybernetických rizík v rezorte Zdravotníctvo (v zmysle ID 2.1 tejto tabuľky) navrhnúť stratégiu kybernetickej bezpečnosti v sektore v súlade s Národnou stratégiou kybernetickej bezpečnosti na roky 2021 až 2025, Akčným plánom realizácie národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 a inými strategickými dokumentmi v príslušnej oblasti, ktoré sú verejne dostupné. Pokryje oblasti najmä:

[14] V zmysle Prílohy č. 1 k ZoKB

[15] Osobitnú kategóriu osobných údajov vymedzuje Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) a *per analogiam* zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
		• Východiská stratégie • Bezpečnostné princípy a zásady • Hlavné hrozby a zraniteľnosti • Strategické ciele v rezorte • Organizačné zabezpečenie kybernetickej bezpečnosti • Budovanie bezpečnostného povedomia • Spôsob implementácie kybernetickej bezpečnosti • Prioritné opatrenia.
2.3	Návrh akčného plánu pre implementáciu prioritných opatrení stratégie	Akčný plán vychádza zo stratégie kybernetickej bezpečnosti v zdravotníctve (v zmysle ID 2.2 tejto tabuľky). Detailnejšie rozpracúva prioritné opatrenia. Zahŕňa v sebe: • konkrétne úlohy a aktivity rozdelené podľa strategických cieľov a priorít, • spôsob realizácie jednotlivých úloh a aktivít • časový horizont plnenia úloh, • zodpovedné subjekty v roli gestorov a participujúcich subjektov, • dopady, resp. náklady vyvolané jednotlivými úlohami.

Z časového hľadiska budú všetky aktivity realizované nasledovným spôsobom:

- Od začiatku až do konca plnenia predmetu zákazky budú všetky aktivity realizované v predpokladanom horizonte 6 mesiacov od nadobudnutia účinnosti Zmluvy o dielo uzatvorenej ako výsledok verejného obstarávania,
- Analýza a Dizajn budú realizované od nadobudnutia účinnosti Zmluvy o dielo uzatvorenej ako výsledok verejného obstarávania až do konca plnenia predmetu zákazky,
- Implementácia a Testovanie ako aj Nasadenie budú realizované v posledných troch mesiacoch plnenia predmetu zákazky, pričom sa ako vstup pre „customizáciu“ použijú práve výstupy z aktivity/etapy Analýza a Dizajn (počas posledných 3 mesiacov).

Počas plnenia predmetu zákazky sa vyžaduje vo všetkých aktivitách využitie odborne spôsobilého kľúčového experta, ktorý disponuje v oblasti informačnej a kybernetickej bezpečnosti niektorým z certifikátov vydaných autoritami „*ISACA, (ISC)², GIAC, alebo CompTIA*“[16] prípadne ich ekvivalent.

[16] Podľa „Prílohy č. 2 Zoznamu odborných certifikátov“ v dokumente Výber dodávateľa služieb kybernetickej bezpečnosti“ dostupný na adrese https://www.mirri.gov.sk/wp-content/uploads/2022/03/KB-K1_2_3-vyber-dodavatela-sluzieb-kybernetickej-bezpecnosti.pdf

Ministerstvo zdravotníctva Slovenskej republiky
Limbová ul. 2, P.O.BOX 52, 837 52 Bratislava 37

Bratislava, 21. 09. 2018
Číslo: S11256-2018-ONAPP-1

Smernica
upravujúca
tvorbu, vydávanie, publikovanie a evidenciu interných riadiacich aktov Ministerstva zdravotníctva Slovenskej republiky

Vypracovala:
JUDr. Niki Vrbová
vedúca Oddelenia nesporovej agendy a právnej podpory

Zodpovední:
Mgr. Marianna Kozmannová
riaditeľka Odboru právneho (poverená zastupovaním)

Mgr. Katarína Hermann
riaditeľka Osobného úradu

Predkladá:
JUDr. Ing. Jozef Ráž
generálny tajomník služobného úradu

Článok 1
Úvodné ustanovenie

Ministerstvo zdravotníctva Slovenskej republiky (ďalej aj ako „ministerstvo“ alebo „MZ SR“) podľa Čl. 11 ods. 2 písm. a) bodu 2. Organizačného poriadku Ministerstva zdravotníctva Slovenskej republiky v platnom znení (ďalej len „Organizačný poriadok MZ SR“) vydáva na zabezpečenie jednotného postupu pri tvorbe, vydávaní, publikovaní a evidencii interných riadiacich aktov ministerstva túto smernicu.

Článok 2
Predmet úpravy

1) Smernica ustanovuje zásady a jednotný postup vecne príslušných organizačných útvarov ministerstva v zmysle Organizačného poriadku MZ SR pri tvorbe, vydávaní, publikovaní a evidencii interných riadiacich aktov ministerstva s cieľom vytvoriť funkčný a efektívny systém ich tvorby a evidencie.

2) Smernica sa nevzťahuje na legislatívne právne akty (zákony, nariadenia vlády Slovenskej republiky, vyhlášky, výnosy a opatrenia ministerstva) a opatrenia ministerstva, ktoré sú zverejňované vo Vestníku Ministerstva zdravotníctva Slovenskej republiky.

Článok 3
Vymedzenie niektorých pojmov

1) Interné riadiace akty v súlade so zákonmi a ostatnými všeobecne záväznými právnymi predpismi bližšie upravujú proces riadenia na ministerstve.

2) Internými riadiacimi aktami ministerstva sú:

a) v kompetencii ministra
   1. príkaz ministra;
   2. smernica ministerstva;

b) v kompetencii generálneho tajomníka služobného úradu
   1. služobný predpis;
   2. opatrenie generálneho tajomníka služobného úradu;

c) v kompetencii štátnych tajomníkov a generálnych riaditeľov
   1. metodické usmernenie;
   2. iné riadiace akty (napr. pokyn a pod.).

3) Register interných riadiacich aktov ministerstva je register vedený v elektronickej a v písomnej forme, v ktorom sú zaevidované všetky vydané interné riadiace akty ministerstva. Register interných riadiacich aktov vedie Odbor právny.

Článok 4
Pravidlá tvorby interných riadiacich aktov

1) Interné riadiace akty sa vypracúvajú v súlade s právnymi predpismi, Organizačným poriadkom MZ SR a inými internými riadiacimi aktami.

2) Na tvorbu interných riadiacich aktov sa primerane použijú legislatívno-technické pokyny uvedené v prílohe č. 1 Legislatívnych pravidiel vlády Slovenskej republiky.

3) Interný riadiaci akt možno zmeniť alebo doplniť len interným riadiacim aktom rovnakého druhu. Zmeny alebo doplnenia sa vykonávajú dodatkami, alebo vydaním nového interného riadiaceho aktu, ktorý zruší predošlý.

4) Interné riadiace akty sa označujú vzostupne. Evidenčné číslo má tvar „N/RRRR“, kde „N“ je poradové číslo interného riadiaceho aktu v danom roku a „RRRR“ je rok vydania.

5) Za prípravu a predkladanie návrhu interného riadiaceho aktu zodpovedá organizačný útvar ministerstva, ktorý má predmetnú upravovanú oblasť vo svojej vecnej pôsobnosti podľa Organizačného poriadku MZ SR (ďalej len „gestorský útvar“). Ak sa interný riadiaci akt týka pôsobnosti viacerých organizačných útvarov, zodpovedá za jeho prípravu ten organizačný útvar, ktorého sa interný riadiaci akt prevažne týka. Ak pôsobnosť nie je zrejmá a medzi organizačnými útvarmi nedôjde k dohode, o pôsobnosti rozhodne osoba oprávnená schváliť interný riadiaci akt. Ostatné organizačné útvary zodpovedné za prípravu interného riadiaceho aktu sa označujú ako spolugestorské útvary.

Článok 5
Schvaľovanie, evidencia a zverejňovanie interných riadiacich aktov

1) Gestorský útvar predloží návrh interného riadiaceho aktu na schválenie príslušnému vedúcemu zamestnancovi ministerstva (minister zdravotníctva Slovenskej republiky, štátny tajomník ministerstva, generálny tajomník služobného úradu, generálny riaditeľ sekcie ministerstva a pod.).

2) Gestorský útvar predloží schválený a podpísaný interný riadiaci akt v jednej fotokópii a zároveň v elektronickej podobe Odboru právnemu na zaevidovanie do Registra interných riadiacich aktov.

3) Ak sa vykonáva zmena alebo doplnenie existujúceho (platného) interného riadiaceho aktu, gestorský útvar predloží v písomnej aj elektronickej podobe dodatok, príp. aj konsolidované znenie novelizovaného interného riadiaceho aktu so zapracovanými zmenami.

4) Za obsahové náležitosti interného riadiaceho aktu je zodpovedný gestorský útvar.

5) Odbor právny pridelí internému riadiacemu aktu evidenčné číslo podľa článku 4 ods. 4 tejto smernice.

6) Po pridelení evidenčného čísla gestorský útvar zabezpečí zverejnenie interného riadiaceho aktu na intranete ministerstva alebo na internetovej stránke ministerstva (podľa druhu interného riadiaceho aktu).

7) Gestorský útvar je zodpovedný za správne a aktuálne znenie zverejnených interných riadiacich aktov.

Článok 6
Spoločné ustanovenia

1) Gestorský útvar je povinný priebežne sledovať aktuálnosť interných riadiacich aktov vo svojej pôsobnosti a podľa potreby navrhovať ich zmenu, doplnenie alebo zrušenie.

2) Každý zamestnanec ministerstva je povinný v rozsahu potrebnom pre riadny výkon svojich služobných úloh alebo pracovných úloh oboznamovať sa s internými riadiacimi aktami evidovanými v Registri interných riadiacich aktov a zverejňovanými na intranete ministerstva, a dodržiavať ich.

Článok 7
Záverečné ustanovenie

Táto smernica nadobúda účinnosť dňom 1. októbra 2018.

Andrea Kalavská
ministerka