Opis predmetu zákazky

# **Názov zákazky**

Aktualizácia vrcholovej riadiacej dokumentácie v súlade s požiadavkami zaistenia kybernetickej bezpečnosti v zmysle európskej a národnej legislatívy.

# **Zadanie**

Predmetom zákazky je vypracovanie alebo aktualizácia riadiacej dokumentácie pre NCZI podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

1. Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).
2. Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a nadväzujúcich vyhlášok najmä vyhlášky Vyhláška č. 179/2020 Z. z. - vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

# **Riadiaca dokumentácia v oblasti riadenia informačnej bezpečnosti**

Minimálny rozsah požiadaviek zadávateľa zákazky je:

3.1Vypracovanie/aktualizácia bezpečnostnej dokumentácie

Bezpečnostná dokumentácia musí byť vypracovaná s ohľadom na prevádzkovanú infraštruktúru IKT, aplikačnú a bezpečnostnú architektúru a implementované bezpečnostné opatrenia, organizačné usporiadanie, pracovné roly, zodpovednosti a rozdelenie právomocí, zaužívaný rámec riadenia operačných rizík, organizačnú kultúru a spoločenskú zodpovednosť NCZI.

3.1.1Identifikáciu legislatívnych a normatívnych požiadaviek

Dokumentácia musí obsahovať komplexné posúdenie všetkých legislatívnych a normatívnych požiadaviek kladených na NCZI ako prevádzkovateľa základných služieb, ako prevádzkovateľa informačných technológií verejnej správy a ako organizáciu spracúvajúcu osobné údaje svojich zamestnancov, klientov a prípadných tretích osôb. Dokument musí určiť všetky relevantné požiadavky, mapovať ich plnenie v prostredí NCZI a stanoviť pravidlá priebežnej kontroly ich dodržiavania.

3.1.2Návrh bezpečnostných politík informačnej / kybernetickej bezpečnosti

Bezpečnostné politiky musia obsahovať základné zásady a ciele v nasledovných oblastiach riadenia IB/KB:

1. Organizácia bezpečnosti
2. Riadenie bezpečnostných rizík
3. Riadenie informačných aktív
4. Pravidlá správania a dobrej praxe
5. Riadenie dodávateľských vzťahov
6. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií
7. Riadenie a prevádzka informačno-komunikačných technológií
8. Riadenie súladu
9. Riadenie kontinuity procesov a činností

3.1.3Klasifikácia informácií a kategorizácia sietí a informačných systémov

Výstup musí obsahovať zoznam vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy a ich podporných systémov a podsystémov. Zoznam môže byť v textovej, tabuľkovej alebo grafickej forme a aktíva musia byť klasifikované v súlade s klasifikačnou schémou podľa prílohy č. 2. Vyhlášky o BO KB. Osobitne musia byť ohodnotené osobné údaje spracúvané v jednotlivých informačných systémoch.

3.1.4Vymedzenie rozsahu a spôsobu plnenia bezpečnostných opatrení

Návrh musí obsahovať popis bezpečnostných opatrení v nasledujúcich oblastiach:

3.1.4.1Organizácia informačnej bezpečnosti

Opatrenia musia pokrývať:

* menovanie a určenie zodpovedností a právomocí manažéra informačnej a kybernetickej bezpečnosti,
* aplikovanie princípu najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh, - oddelenie zodpovedností a právomocí používateľov,
* aplikovanie zásady nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík,
* zásady jasného vymedzenia právomoci, povinnosti a zodpovednosti používateľov. 3.1.4.2Riadenie aktív, hrozieb a rizík

Opatrenia musia pokrývať:

* inventarizácia všetkých aktív, od ktorých závisí poskytovanie služieb NCZI, ,
* identifikácia zodpovedných osôb za inventarizáciu aktív,
* identifikácia vlastníkov aktív,
* identifikácia zraniteľností a hrozieb,
* analýza rizík s ohľadom na identifikované aktíva,
* určenie vlastníkov rizík,
* návrh organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík,
* identifikácia implementovaných bezpečnostných opatrení,
* identifikácia bezpečnostných opatrení, ktoré nebudú implementované spolu s odôvodnením,
* analýza funkčného dopadu,
* návrh postupov pre pravidelné preskúmavanie identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení. 3.1.4.3Personálna bezpečnosť

Opatrenia musia pokrývať:

* postupy pri zaradení alebo presune osoby do niektorej z bezpečnostných rolí,
* postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,
* budovanie bezpečnostného povedomia a plán vzdelávania zamestnancov NCZI,
* hodnotenie účinnosti vzdelávania zamestnancov NCZI a dodávateľov zastávajúcich niektorú z bezpečnostných rolí,
* kontrola dodržiavania a riešenie prípadov porušenia definovaných bezpečnostných politík, vrátane disciplinárneho postupu pri ich porušení.

3.1.4.4Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov

Opatrenia musia pokrývať:

* popis spôsobu riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* analýzu rizík dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* návrh kontrolných a auditných postupov pre overenie dodržiavania bezpečnostných požiadaviek dodávateľmi služieb,
* definovanie obsahu zmluvy s treťou stranou, vývoj a akvizícia siete a informačného systému základnej služby s ohľadom na: o zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a o zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii. 3.1.4.5Riadenie technických zraniteľností systémov a zariadení

Opatrenia musia pokrývať:

* metódy a nástroje na identifikáciu a ošetrovanie existujúcich zraniteľností SW a HW a využívanie publikovaných informácií (výrobcovia, bezpečnostné organizácie, ...). 3.1.4.6Riadenie bezpečnosti sietí a informačných systémov

Opatrenia musia pokrývať:

* Pravidlá pre segmentáciu sietí a riadenie komunikácie medzi segmentami, blokovanie neautorizovaných portov a návrh segmentácie a komunikačných pravidiel s ohľadom na prevádzkované systémy a technológie v NCZI,
* Podmienky pre umiestnenie špecifikovaných služieb do vyhradených segmentov siete,
* Postupy pre bezpečnostnú konfiguráciu serverov,
* ochranu prepojenia medzi internými a externými sieťami, vytváranie black-listov,
* zaistenie bezpečného mobilného a vzdialeného prístupu do interných sietí,
* evidenciu a monitorovanie bezpečnosti všetkých vstupno-výstupných bodov na hranici siete, ochranu pred prienikom a únikom dát,
* ochranu pred škodlivým kódom na zariadeniach, ktoré sa pripájajú do internej siete z externého prostredia,
* zmluvné zaručenie bezpečnosti pripojenia dodávateľov vrátane preukázania plnenia. 3.1.4.7Riadenie bezpečnosti prevádzky siete a informačného systému

Opatrenia musia pokrývať:

* riadenie zmien,
* riadenie záplat a aktualizácií,
* riadenie kapacít,
* pravidelné zálohovanie a testovanie obnovy informácií zo záloh,
* ochranu pred škodlivým kódom,
* inštaláciu softvéru a zariadení v sieťach a informačných systémoch,
* zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov. 3.1.4.8Riadenie prístupov

Opatrenia musia pokrývať:

* zásady riadenia prístupu k informáciám,
* identifikáciu a autentizáciu používateľov,
* práva a povinnosti používateľov a rolí zodpovedných za riadenie prístupu používateľov,
* riadenie prístupu k sieťam, operačnému systému a jeho službám, prístup k aplikáciám, - riadenie vzdialeného prístupu,
* monitorovanie prístupov, vedenie prevádzkových záznamov o prístupe do siete a informačného systému,
* vykonávanie pravidelných kontrol prístupových účtov a prístupových oprávnení. 3.1.4.9Používanie kryptografických opatrení

Opatrenia musia pokrývať:

* používanie dostatočne odolných kryptografických prostriedkov na zaistenie dôvernosti, integrity, dostupnosti a hodnovernosti údajov v rámci sietí a informačných systémov,
* pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
* riadenie a ochranu kryptografických kľúčov a certifikátov počas ich celého životného cyklu,
* využívanie kryptografie pri dvojfaktorovej autentifikácii používateľov, - vykonávanie kontroly a auditu v tejto oblasti. 3.1.4.10Riešenie bezpečnostných incidentov

Opatrenia musia pokrývať:

* detekciu, evidenciu a riešenie bezpečnostných incidentov,
* určenie právomocí a zodpovedností používateľov a zodpovedných rolí,
* postupy hlásenia bezpečnostných incidentov s dosahom na spracúvanie osobných údajov voči orgánu dohľadu a voči dotknutým osobám,
* pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania. 3.1.4.11Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

Opatrenia musia pokrývať:

* bezpečnostný dohľad nad činnosťou sietí, informačných systémov a ich používateľov,
* vytváranie a zaznamenávanie prevádzkových záznamov o o manipulácii s osobnými, chránenými a prísne chránenými informáciami a údajmi alebo s nimi spojenými informačnými aktívami,
	+ iniciácii, akceptácii alebo odmietnutí pripojenia do siete alebo informačného systému,
	+ zmene prístupových práv používateľov, o zmene pravidiel bezpečnostných prvkov, o varovných alebo chybových hláseniach systémov,
	+ podozrivých alebo škodlivých aktivitách a ďalších informáciách nevyhnutných na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia,
* ochranu a uchovávanie prevádzkových záznamov,
* určenie zodpovedných rolí za monitorovanie a vyhodnocovanie prevádzkových záznamov, nahlásenie podozrivej aktivity,
* vykonávanie auditu kybernetickej bezpečnosti. 3.1.4.12Fyzická bezpečnosť a bezpečnosť prostredia

Opatrenia musia pokrývať:

* technické a organizačné opatrenia na zaistenie fyzickej ochrany siete a informačného systému alebo aspoň ich najdôležitejších komponentov pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií a fyzickým prístupom nepovolaných osôb,
* požiadavky na bezpečné uloženie fyzických záznamov obsahujúcich citlivé a osobné údaje a podmienky ich archivácie,
* ochranu prevádzkového priestoru v závislosti na kritickosti komponentov,
* kontrolu dodržiavania pravidiel na prácu v zabezpečenom priestore,
* zabezpečenie vhodného prevádzkového prostredia a dodávky podporných služieb,
* požiadavky na kapacity v bezpečne vzdialenom záložnom zabezpečenom priestore,
* zaistenie súladu prevádzky s vnútornými predpismi a zmluvnými záväzkami, zásadu „čistého stola“ a „čistej obrazovky“,
* kontrolu dodržiavania pravidiel,
* životný cyklus a ochranu technických komponentov sietí a informačných systémov a všetkých typov relevantných záloh. 3.1.4.13Riadenie kontinuity procesov

Opatrenia musia pokrývať:

* požiadavky na zabezpečenie kontinuity riadenia informačnej a kybernetickej bezpečnosti pri vzniku bezpečnostného incidentu,
* vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému,
* vykonanie analýzy dopadov bezpečnostného incidentu na prevádzkované služby,
* určenie adekvátnych zdrojov na zabezpečenie riadenia kontinuity činností,
* určenie komunikačného plánu spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti,
* určenie cieľovej doby a cieľového bodu obnovy,
* testovanie a vyhodnocovanie procesu riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
* určenie plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému,
* pravidelné preverenie záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.

3.1.5Analýza rizík

Dokument musí obsahovať posúdenie bezpečnostných rizík vyplývajúcich z hrozieb pôsobiacich na aktíva v správe NCZI.

# Osobitné požiadavky v oblasti zaistenia kybernetickej bezpečnosti

Minimálny rozsah požiadaviek zadávateľa zákazky je:

5.1Posúdenie prevádzkovaných základných služieb

Výstup musí pokrývať identifikáciu a posúdenie prevádzkovaných základných služieb so zvážením súvisiacej infraštruktúry IKT, aplikačnej a bezpečnostnej architektúry a spoločenskej zodpovednosti NCZI.

5.2Návrh bezpečnostnej stratégie kybernetickej bezpečnosti

Bezpečnostná stratégia kybernetickej bezpečnosti musí vychádzať z výsledkov analýzy rizík kybernetickej bezpečnosti a musí obsahovať formuláciu cieľov kybernetickej bezpečnosti a základné princípy na dosiahnutie týchto cieľov, určenie právomocí a zodpovedností za riadenie kybernetickej bezpečnosti, rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie. Môže byť vypracovaná ako samostatný dokument alebo ako súčasť bezpečnostných politík kybernetickej bezpečnosti.