Dohoda o spolupráci

pri určení rozsahu zodpovedností za realizáciu opatrení kybernetickej a informačnej bezpečnosti

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ďalej len „dohoda“)

Článok 1
Účastníci dohody

Prevádzkovateľ č. 1:

Názov:	Národný inšpektorát práce
Zastúpený:	Mgr. Hedviga Machayová, MBA, generálna riaditeľka
Adresa sídla:	Masarykova 10, 040 01 Košice
IČO:	00166405
IČ DPH:	SK2020830284,
	registrácia podľa § 7 zákona č. 222/2004 Z. z. o DPH
Kontaktná osoba:	Ing. Ján Turza, manažér KB a IB
	email: jan.turza@ip.gov.sk, tel.:+421 918 704 692

(ďalej ako „NIP“)

Prevádzkovateľ č. 2:

Názov:	Inšpektorát práce Trenčín
Zastúpený:	Ing. Vladimír Kopecký, hlavný inšpektor práce
Adresa sídla:	Hodžova 36, 911 01 Trenčín
IČO:	35627620
IČ DPH:	SK 2021257876,
	registrácia podľa § 7 zákona č. 222/2004 Z. z. o DPH
Kontaktná osoba:	Jaroslav Bariš, manažér KIB
	email: jaroslav.baris@ip.gov.sk, tel.:+421 907 904 874

(ďalej ako „IP“)

(Prevádzkovateľ č. 1 a Prevádzkovateľ č. 2 ďalej spolu ako „účastníci dohody“)

Článok 2
Výklad pojmov a skratky

1. Pre účely tejto dohody sa zavádzajú nasledovné pojmy:
   a) **Aktívum** je hmotný alebo nehmotný objekt, ktorý sa podieľa na fungovaní a vytváraní informačného systému rezortu MPSVR SR.
   b) **Bezpečnosť** je stav spoločenského, prírodného, technického, technologického systému alebo iného systému, ktorý v konkrétnych vnútorných a vonkajších podmienkach umožňuje plnenie určených funkcií a ich rozvoj v záujme človeka a spoločnosti.
   c) **Bezpečnostná politika** je súhrn zásad a postupov využívaných na dosahovanie požadovanej miery bezpečnosti systému. Dokument, v ktorom sú určené ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti alebo mechanizmy riadenia bezpečnosti informačných technológií verejnej správy.
   d) **Bezpečnostné role** slúžia na zabezpečenie úloh súvisiacich s riadením kybernetickej a informačnej bezpečnosti, pridelené vybraným zamestnancom na základe organizačnej štruktúry, určujú ich postavenie, povinnosti a oprávnenia v bezpečnostnom tíme alebo v štruktúre.
   e) **Dostupnosť** znamená, že dáta, údaje, informácie alebo zariadenia sú prístupné v okamihu ich potreby.
   f) **Dôvernosť** znamená, že dáta, údaje alebo informácie sú prístupné iba oprávneným osobám.
   g) **Informačná a komunikačná technológia** predstavuje súbor technických (hardvérových), programových (softvérových), komunikačných, sieťových a iných podporných prostriedkov, pomocou ktorých sa spracovávajú a uchovávajú informácie a údaje automatizovaným spôsobom. Pod informačné a komunikačné technológie sú zahrnuté aj informačné systémy.
   h) **Informačná bezpečnosť** je skupina procesov a nástrojov, ktoré chránia fyzické a digitálne údaje pred neoprávneným prístupom, použitím, zverejnením, narušením, úpravou, zaznamenaním alebo zničením.
   i) **Informačná technológia** je prostriedok alebo postup, ktorý slúži na spracovávanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.
   j) **Informačná technológia verejnej správy** je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Povinnosti v rámci správy informačných technológií verejnej správy sa vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy o sebe slúžia na spracovávanie údajov alebo informácií v elektronickej podobe.
   k) **Informačný systém** je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.
   l) **Informačný systém verejnej správy** je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

m) **Integrita** znamená, že dáta, údaje alebo informácie nemôžu byť ľubovoľne zmenené.

n) **Kybernetická bezpečnosť** je stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.

o) **Kybernetický bezpečnostný incident** je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:
   a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
   b) obmedzenie alebo odmietnutie dostupnosti základnej služby,
   c) vysoká pravdepodobnosť kompromitácie činností základnej služby alebo
   d) ohrozenie bezpečnosti informácií.

2. Pre účely tejto dohody sa zavádzajú nasledovné skratky:

IKT	Informačné komunikačné technológie
IS	Informačný systém
ISVS	Informačné systémy verejnej správy
ITVS	Informačná technológia verejnej správy
KB	Kybernetická bezpečnosť
KIB	Kybernetická a informačná bezpečnosť
MIB	Manažér informačnej bezpečnosti
MKB	Manažér kybernetickej bezpečnosti
MPSVR SR	Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky
N/A	Neaplikované, nepožadované
Rezort MPSVR SR	MPSVR SR a Právnické osoby v pôsobnosti MPSVR SR
SOCNET	Rezortná informačná sieť MPSVR SR
NIP	Národný inšpektorát práce
IP	Inšpektorát práce
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
ZoITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Vyhláška č. 179	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

Vyhláška č. 362	Vyhláška č. 362/2018 Z. z. Národného bezpečnostného úradu z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Predpisy o KIB	Právna úprava o KIB - t. j. Zákon o KB, Zákon o ITVS, Vyhláška č. 179 a Vyhláška č. 362

Článok 3
Úvodné ustanovenia

1. NIP a IP sú prevádzkovateľmi základných služieb podľa § 3 písm. l) prvý bod ZoKB s názvom: správa a prevádzkovanie sietí a informačných systémov verejnej správy v pôsobnosti orgánu riadenia podľa ZoITVS.
2. Ako základný dokument určujúci KIB je pre účastníkov dohody stratégia kybernetickej bezpečnosti rezortu Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky (ďalej len „stratégia"), ktorá definuje základný rámec organizácie bezpečnosti, stanovuje rozdelenie všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej a informačnej bezpečnosti a určenie príslušných bezpečnostných rolí v rámci rezortu potrebných na riadenie kybernetickej a informačnej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh.
3. NIP v zmysle zákona č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov okrem iného riadi a kontroluje výkon štátnej správy uskutočňovanej inšpektorátmi práce a zabezpečuje prevádzku informačného systému ochrany práce a jeho programové a technické vybavenie.
4. Stratégia vo svojich cieľoch definuje aj zaistenie jednotného systému riadenia kybernetickej a informačnej bezpečnosti v rezorte MPSVR SR. NIP metodicky riadi zabezpečenie plnenia cieľov informačnej a kybernetickej bezpečnosti prostredníctvom manažérov KIB.
5. Manažéri KIB sú povinní aplikovať, koordinovať a usmerňovať implementáciu schválených predpisov MPSVR SR a NIP. Poskytujú súčinnosť pri napĺňaní cieľov, predchádzajú a minimalizujú vplyv kybernetických bezpečnostných incidentov.

Článok 4
Predmet dohody

1. Predmetom tejto dohody je stanovenie rozsahu zodpovednosti účastníkov dohody za realizáciu opatrení v zmysle predpisov o KIB v nadväznosti na Bezpečnostnú stratégiu kybernetickej a informačnej bezpečnosti rezortu Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky. Účastníci dohody uzatvárajú túto dohodu za účelom dosiahnutia jednotnej organizácie, správy, administrácie ITVS, riadenia KIB, špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v rámci rezortu z úrovne MPSVR SR a NIP. V Prílohe č. 1 tejto dohody je uvedený zoznam bezpečnostnej

dokumentácie, ktorá je v zmysle tejto dohody záväzná pre účastníkov dohody.

2. Účastníci dohody si plne uvedomujú svoje zodpovednosti, ktoré im vyplývajú zo ZoKB, ZoITVS, z Vyhlášky č. 362 a z Vyhlášky č. 179.
3. IP vyjadruje záujem o koordinovanie svojich činnosti s NIP v rámci svojich kompetencií a zákonom určenej pôsobnosti a fyzických a logických hraníc svojich informačných systémov a sietí, presadzovať procesy a opatrenia kybernetickej bezpečnosti, ktoré sú stanovené v bezpečnostnej dokumentácií NIP a MPSVR SR. Účastníci dohody sa v zmysle tejto dohody zaväzujú poskytovať súčinnosť druhej strane dohody bezodplatne.

Článok 5
Všeobecné požiadavky

1. Účastníci dohody pri plnení záväzkov vyplývajúcich z legislatívy vystupujú ako samostatné organizácie, vedomé si svojich práv a povinnosti, ktoré sú spojené s týmito zákonmi a vyhláškami, pričom rozsah vzájomnej kooperácie, prenosu zodpovednosti a práv za plnenie jednotlivých bodov predpisov o KIB je upravený v prílohe č. 2 tejto dohody.
2. Účastníci dohody prehlasujú, že si vo vzťahu k druhej strane dohody nebudú uplatňovať práva, najmä autorské, na akúkoľvek bezpečnostnú dokumentáciu, ktorú vypracovala alebo používa druhá strana dohody, pričom každý účastník dohody môže slobodne používať alebo prepracovať bezpečnostnú dokumentáciu druhej strany dohody pre svoju potrebu.
3. Účastníci dohody sa zaväzujú, že nebudú bezpečnostnú dokumentáciu zatajovať a budú ju postupovať, či už v podpísanej alebo v pracovnej podobe všetkým osobám definovaným v bode 5 tohto článku.
4. Účastníci dohody sa dohodli, že v prípade nezrovnalostí alebo nedorozumení vzniknutých pri vzájomnom postupovaní alebo využívaní bezpečnostnej dokumentácie druhej strany dohody budú tieto nedorozumenia primárne prerokované s manažérom kybernetickej bezpečnosti NIP.
5. Prílohou č. 3 tejto dohody je zoznam pracovných rolí strán dohody a k nim prislúchajúci menný zoznam osôb podľa § 8 ods. 2 písm. g) Vyhlášky č. 362, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby. Každú zmenu v personálnom obsadení pracovných rolí podľa prechádzajúcej vety je každá zmluvná strana povinná najneskôr 5 dní pred plánovaným začatím výkonu činnosti touto osobou písomne oznámiť druhej strane dohody. Účastníci dohody sú povinní zabezpečiť, aby sa osoby evidované v zozname podľa prvej vety tohto bodu dohody zaviazali pred začatím výkonu činnosti dodržiavať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s výkonom činnosti dozvedeli podľa článku 8 tejto dohody.

Článok 6
Špecifikácia a rozsah bezpečnostných opatrení a činností

1. Účastníci dohody primerane implementujú základné bezpečnostné pravidlá uvedené v bezpečnostných dokumentáciách podľa prílohy č. 1 tejto dohody.
2. Konkrétne bezpečnostné opatrenia zohľadňujúce špecifiká prostredia konkrétnej strany dohody, vrátane bezpečnostnej dokumentácie budú rozpracované v rozsahu podľa Prílohy č. 1 a Prílohy č. 2 dohody.

Článok 7
Riadenie aktív, hrozieb a rizík

1. IP sa zaväzuje aktívne podieľať na splnení povinností podľa § 6 Vyhlášky č. 362.
2. IP sa zaväzuje pravidelne, podľa bodu 4 tohto článku, postupovať NIP vo forme štruktúrovaného zoznamu identifikované **svoje** aktíva.
3. IP sa zaväzuje pravidelne, podľa bodu 4 tohto článku, postupovať NIP výsledky svojich aktivít vypracovaných v rámci procesu riadenia aktív[1], hrozieb[2] a rizík[3] a bude aktívne spolupracovať s NIP pri vyhodnocovaní pôsobenia hrozieb špecifických pre svoje prostredie, bude navrhovať a aplikovať opatrenia na ošetrovanie rizík.
4. IP sa zaväzuje v intervale 1x za rok predkladať podklady do správy o riadení rizík, ktoré budú obsahovať minimálne:
   a) Zoznam aktív.
   b) Vyhodnotenia stavu kybernetickej bezpečnosti za uplynulé obdobie.
   c) Identifikáciu a hodnotenie rizík.
   d) Realizované bezpečnostné opatrenia.
   e) Vyhodnotenie bezpečnostných incidentov.

Článok 8
Riešenie kybernetických bezpečnostných incidentov

1. Účastníci dohody sú povinní si navzájom hlásiť závažné kybernetické bezpečnostné incidenty[4] (ďalej len „KBI") a spolupracovať pri riešení prevádzkových incidentov.[5]
2. Hlásenie závažných KBI bude účastníkmi dohody realizované podľa prílohy č. 3 k smernici č. 2/2021 o riešení incidentov a kybernetických bezpečnostných incidentov platnej na MPSVR SR a schválenej ministrom.
3. IP sa zaväzuje, za podmienky aplikovania svojich špecifikácií a v primeranej miere, aplikovať vo svojom prostredí obdobnú smernicu ako MPSVR SR uvedenú v bode 2 tohto článku, a to najmä v bodoch týkajúcich sa definovania stavu riešenia KBI, jeho

[1] § 6 ods. 3 vyhlášky NBÚ č. 362/2018 Z. z.
[2] § 6 ods. 9 vyhlášky NBÚ č. 362/2018 Z .z.
[3] § 6 ods. 6 vyhlášky NBÚ č. 362/2018 Z. z.
[4] § 1 ods. 2 vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
[5] § 16 ods. 1 písm. b) 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 „zákon č. 95/2019 Z. z")

analyzovania a zberu dôkazov.

4. IP je povinný hlásiť NIP vznik KBI prostredníctvom formulára podľa smernice uvedenej v bode 2 tohto článku.
5. Účastníci dohody sa zaväzujú, že budú včas informovať druhú stranu dohody prostredníctvom manažérov kybernetickej bezpečnosti alebo ním poverených pracovníkov o všetkej komunikácií s nasledovnými subjektmi: Národné centrum kybernetickej bezpečnosti SK-CERT (NBÚ), SK CERT NBÚ a CSIR.SK (MIRRI).
6. Účastníci dohody sa zaväzujú aktívne spolupracovať pri riešení KBI, odstraňovaní jeho následkov a prípadnom trestno-právnom konaní.

Článok 9
Zabezpečenie kontinuity

1. Účastníci dohody sa zaväzujú k úzkej spolupráci v oblasti kontinuity procesov a v rámci obnovy dôležitých technologických celkov.
2. IP sa zaväzuje k obsadzovaniu svojich pracovníkov do pracovných skupín, pričom títo pracovníci budú povinní plniť príkazy vedúcich skupín. Obsadzovanie pracovníkov IP je podmienené na výkon činností a na riešenie problémov spojených s aktívami v ich prevádzke alebo spojených s touto prevádzkou.
3. IP je povinný poskytovať NIP všetku dokumentáciu a informácie spojené s riadením kontinuity[6], stratégie a krízových plánov[7], komunikačných plánov[8], doby obnovy prevádzky[9], určenia plánov havarijnej obnovy a postupov zálohovania.[10]

Článok 10
Audit kybernetickej bezpečnosti a kontrolná činnosť

1. Účastníci dohody sú si vedomí, že ako samostatné subjekty majú povinnosť vykonávať audit kybernetickej bezpečnosti. Vzhľadom na to, že obidve strany dohody spolu prevádzkujú viaceré informačné systémy, nie je možné jednoznačne určiť ich logické aj fyzické hranice.
2. Účastníci dohody v zmysle bodu 1 tohto článku sa zaväzujú, že si budú navzájom koordinovať svoje aktivity súvisiace s vykonávaním auditu kybernetickej bezpečnosti, budú si poskytovať maximálnu súčinnosť a podporu a budú postupovať jednotne v procese prípravy, realizácie auditu a odstraňovania nálezov audítora.
3. Audity procesne zastrešujú manažéri kybernetickej bezpečnosti strán dohody.
4. Účastníci dohody sú povinní poskytnúť osobe vykonávajúcej audit všetky informácie, ktoré majú k dispozícii a umožniť jej prístup do všetkých relevantných priestorov.

+

[6] § 17 ods. 1 vyhlášky NBÚ č. 362/2018 Z. z.
[7] § 17 ods. 2 písm. a) vyhlášky NBÚ č. 362/2018 Z .z.
[8] § 17 ods. 2 písm. c) vyhlášky NBÚ č. 362/2018 Z .z.
[9] § 17 ods. 2 písm. d) a písm. e) vyhlášky NBÚ č. 362/2018 Z. z.
[10] § 17 ods. 2 písm. g) vyhlášky NBÚ č. 362/2018 Z. .z.

Článok 11
Mlčanlivosť a ochrana informácií

1. Účastníci dohody sú povinní zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedeli v súvislosti s plnením úloh podľa tejto dohody, najmä nevyužiť ani nesprístupniť tretím osobám žiadne skutočnosti, informácie, poznatky, podklady alebo iné záležitosti, o ktorých boli počas platnosti tejto dohody informovaní, alebo o ktorých sa dozvedeli počas plnenia tejto dohody. Povinnosť zachovávať mlčanlivosť trvá aj po zániku tejto dohody.
2. Účastníci dohody sú povinní písomne zaviazať všetky osoby, svojich zamestnancov, subdodávateľov a ich zamestnancov, ktoré sú zúčastnené na plnení tejto dohody zachovávať mlčanlivosť v zmysle § 12 ods. 1 ZoKB. Účastníci dohody v plnej miere zodpovedajú za dodržiavanie záväzku mlčanlivosti týmito osobami aj po zániku dohody.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje ZoKB.
4. Účastníci dohody sú povinní chrániť všetky informácie, ktoré im boli poskytnuté, a to najmä pred ich neoprávneným vymazaním, zmenou alebo pred ich poskytnutím neoprávnenej osobe.

Článok 12

Pravidlá komunikácie a kontaktné osoby

1. Akákoľvek komunikácia a hlásenie informácií súvisiacich s plnením povinností vyplývajúcich zo ZoKB alebo majúcich vplyv na zabezpečenie kybernetickej a informačnej bezpečnosti alebo plnenie tejto dohody, musí byť realizované niektorou z nasledovných foriem: pošta (DMS), elektronická pošta, telefón alebo osobne, ak v tejto dohode nie je uvedené inak.
2. Účastníci dohody sa dohodli, že akékoľvek písomnosti týkajúce sa skončenia trvania tejto dohody budú doručované len prostredníctvom pošty (DMS), osobne alebo kuriérnou službou, a to na adresu sídiel účastníkov dohody uvedených v tejto dohode. Súčasne sa účastníci dohody dohodli, že tieto písomnosti si budú zasielať na vedomie aj elektronickou poštou na adresu uvedenú v kontaktných údajoch účastníkov dohody.
3. Účastníci dohody sa dohodli, že obsah komunikácie a hlásení informácií, ktoré boli realizované telefonicky alebo osobne, si budú zmluvné strany bezodkladne zasielať aj elektronickou poštou na adresu uvedenú v kontaktných údajoch účastníkov dohody.
4. Účastníci dohody sa dohodli, že komunikácia vykonávaná elektronickou poštou sa bude riadiť nasledovnými pravidlami:
   a) elektronická pošta bude zasielaná pre oblasť hlásenia výhradne na adresy elektronickej pošty (e-mail) v zmysle tohto článku,
   b) elektronická pošta bude zasielaná v chránenej forme (napr. chránená heslom, chránená šifrovaním), v závislosti od dohody komunikujúcich strán a citlivosti informácií, ktoré sú obsahom komunikácie.
5. Kontaktné údaje strán dohody sa nachádzajú v prílohe č. 3 dohody.

6. Každú zmenu kontaktných údajov uvedených v prílohe č. 3 dohody je jedna strana dohody povinná bezodkladne oznámiť druhej strane dohody a to v preukázateľnej forme.
7. Podanie prostredníctvom elektronickej pošty (e-mailu) sa vždy považuje za doručené uplynutím dvanástich hodín od jeho odoslania na správnu e-mailovú adresu, pokiaľ nie je odosielateľovi v tejto lehote doručená informácia od zhotoviteľa služby alebo serveru o neúspešnom doručení e-mailu alebo ak nie je doručenie elektronickej pošty preukázané skôr.
8. Podanie, ktoré strany dohody doručujú osobne sa považuje za riadne doručené v deň, ktorý strana dohody prevezme podanie a tento dátum vyznačí na origináli podania, na ktorej bude vyznačený dátum doručenia podania a podpis osoby, ktorá podanie prevzala.

Článok 13
Zapojenie ďalšieho dodávateľa (subdodávatelia)

1. Obidvaja účastníci dohody sú oprávnení pri výkone činností podľa tejto dohody využiť subdodávateľa, pričom o tejto skutočnosti sa účastníci dohody navzájom informujú.
2. Súčasťou zmluvného vzťahu so subdodávateľom musí byť ustanovenie o zachovaní bezpečnosti o ochrane informácií (bezpečnostná doložka).

Článok 14
Sankcie a zodpovednosť za škodu

1. Ak konaním účastníka dohody ako samostatného subjektu dôjde ku spáchaniu správneho deliktu v zmysle ZoKB a na základe toho bude strane dohody udelená sankcia, každá strana dohody zodpovedá voči správnemu orgánu samostatne.
2. V prípade nedodržania akejkoľvek povinnosti alebo záväzku strany dohody vyplývajúceho z tejto dohody, je účastník dohody oprávnený písomne vyzvať porušujúcu stranu dohody na nápravu porušovanej povinnosti. V prípade, ak nedôjde k náprave porušovanej povinnosti na základe výzvy v stanovenej lehote, je účastník dohody oprávnený odstúpiť od tejto dohody.
3. Ak ktorákoľvek strana z účastníkov dohody poruší svoju povinnosť podľa tejto dohody, je povinná nahradiť škodu spôsobenú druhej strane dohody. Tejto zodpovednosti sa účastník dohody, ktorá škodu spôsobila, môže zbaviť iba ak sa preukáže, že porušenie povinnosti bolo spôsobené okolnosťami vylučujúcimi zodpovednosť. Pri uplatňovaní náhrady škody sa účastníci dohody riadia príslušnými ustanoveniami zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „Obchodný zákonník").

Článok 15
Zánik dohody

1. Táto dohoda sa uzatvára na dobu neurčitú. Táto dohoda môže zaniknúť:
   a) odstúpením od dohody,
   b) dohodou obidvoch strán dohody.
2. Účastníci dohody sú oprávnení odstúpiť od tejto dohody v prípade, ak druhá strana dohody poruší akúkoľvek povinnosť alebo záväzok plynúci mu z tejto dohody a súčasne nevykoná nápravu v stanovenej lehote podľa článku 14. ods. 2 dohody.
3. Po ukončení tejto dohody je IP povinný vrátiť, previesť, alebo zničiť všetky informácie, ku ktorým mal IP prístup počas trvania tejto Dohody, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane IP. Informáciou podľa predchádzajúcej vety sa rozumejú najmä, avšak nie len systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach MPSVR SR a NIP.
4. Po ukončení tejto dohody je IP povinný udeliť, poskytnúť, previesť alebo postúpiť na NIP, ak tak určí NIP, všetky licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovaných služieb NIP a MPSVR SR.

Článok 16
Záverečné ustanovenia

1. Dohoda nadobúda platnosť a účinnosť dňom jej podpísania stranami dohody.
2. Účastníci dohody prehlasujú, že v čase uzavretia tejto zmluvy im nie sú známe žiadne okolnosti, ktoré by bránili, alebo vylučovali uzavretie tejto dohody, resp. ktoré by mohli byť vážnou prekážkou jej plnenia.
3. Náklady, ktoré sú spojené s auditom v zmysle § 29 ods. 6 ZoKB, znáša každá strana dohody samostatne.
4. Žiadna strana dohody nemá právo požadovať akúkoľvek finančnú alebo inú úhradu, napr. refundácia nákladov, pridelenie tabuľkových miest, náhradu za materiál a pod. od druhej strany, t. j. všetky náklady spojené s plnením záväzkov stanovených touto dohodou sú vykonávané navzájom bezodplatne.
5. Účastníci dohody svojím podpisom potvrdzujú autentickosť tejto dohody a zároveň potvrdzujú, že ich spôsobilosť na právne úkony nie je ničím obmedzená, právny úkon je urobený v predpísanej forme, prejavy vôle strán dohody sú hodnoverné, dostatočne zrozumiteľné, ich dohodová (zmluvná) voľnosť nie je ničím obmedzená, a dohoda bola uzavretá slobodne, vážne, určite a zrozumiteľne a nie v tiesni za nápadne nevýhodných podmienok.
6. Ak ktorékoľvek ustanovenie tejto dohody je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto dohody tým nebude dotknuté ani narušené. Účastníci dohody sa týmto zaväzujú bezodkladne rokovať o nahradení akéhokoľvek nezákonného, neplatného

alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.

7. Účastníci dohody sa týmto zaväzujú, že vynaložia všetko úsilie, ktoré je od nich možné spravodlivo požadovať, aby došlo k urovnaniu všetkých sporov, rozporov alebo nárokov vzniknutých medzi nimi na základe tejto dohody a v súvislosti s ňou zmierom. Ak strany dohody nevyriešia akýkoľvek spor zmierom, bude takýto spor predložený na rozhodnutie príslušnému všeobecnému súdu v Slovenskej republike.
8. Dohoda sa riadi platným právnym poriadkom Slovenskej republiky. Na práva a povinnosti explicitne neupravené touto dohodou sa vzťahujú príslušné ustanovenia platných právnych predpisov Slovenskej republiky, najmä zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy a zákona č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov, ZoKB, ZoITVS, Vyhl. 362 a Vyhl. 179.
9. Táto dohoda môže byť doplnená a zmenená len písomným dodatkom v listinnej forme podpísaným oboma stranami.
10. Dohoda je vyhotovená v štyroch rovnopisoch, pričom každý má platnosť originálu, z čoho sú dva rovnopisy určené pre NIP a dva rovnopisy sú určené pre IP .
11. Prílohou tejto Dohody je:
    Príloha č. 1 - Zoznam bezpečnostnej dokumentácie,
    Príloha č. 2 - Prehlásenie o aplikovateľnosti opatrení,
    Príloha č. 3 - Zoznam pracovných rolí strán dohody a k nim prislúchajúci menný zoznam osôb a ich kontaktných údajov
12. Strany dohody vyhlasujú, že si dohodu prečítali, jej obsahu porozumeli a bez výhrad s ňou súhlasia, na znak čoho ju vlastnoručne podpisujú.

V Košiciach dňa 21.1.2022

V Trenčíne dňa 21.1.2022

Príloha č. 1
k Dohode o určení rozsahu zodpovedností za realizáciu
opatrení kybernetickej a informačnej bezpečnosti

Zoznam bezpečnostnej dokumentácie

1. Stratégia kybernetickej a informačnej bezpečnosti MPSVR SR
2. Bezpečnostné politiky a štandardy MPSVR SR
3. Smernica č. 02/2022 o riešení incidentov a kybernetických bezpečnostných incidentov na NIP
4. Smernica č. 03/2022 o rozvoji bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti NIP
5. Smernica č. 04/2022 o riadení kontinuity procesov a činností kybernetickej bezpečnosti NIP

PREHLÁSENIE O APLIKOVATEĽNOSTI opatrení medzi MPSVR SR , NIP a IP (ďalej len "Subjekt") o rozsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostnej dokumentácie a rozsahu všeobecných bezpečnostných opatrení, ktoré prijíma prevádzkovateľ základnej služby podľa § 3 písm. l) zákona pre informačné systémy a siete, prostredníctvom ktorých zabezpečuje základnú službu podľa § 3 písm. k) zákona a pre informačné systémy a siete, ktorých výpadok alebo poškodenie môže spôsobiť poškodenie alebo znemožnenie poskytovania základnej služby.

Časť vyhlášky 362/2018 Z. z.		Aplikovanie opatrení			Popis zodpovedností za dokumentovanie opatrení	
	Požadovaný obsah (stručne)	Centrálne (MPSVR)	Subjektom (NIP)	Popis zodpovedností za aplikáciu opatrení (stĺpec E)	Centrálna bezpečnostná dokumentácia rezortu MPSVR SR (spracovanie zabezpečuje MPSVR) (stĺpec F)	Bezpečnostná dokumentácia Subjektu (spracovanie zabezpečuje Subjekt) (stĺpec G)
§ 2 Obsah a štruktúra bezpečnostnej dokumentácie	(1) Bezpečnostná dokumentácia obsahuje a) schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti, b) klasifikáciu informácií a kategorizáciu sietí a informačných systémov a ďalšie opatrenia odst. (1), (2), (3).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu bezpečnostnej dokumentácie uvedenej v stĺpci F a zabezpečuje jej dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu bezpečnostných pravidiel uvedených v dokumentácii MPSVR SR vo svojom prostredí podľa čl. 1 až 14 zmluvy. Subjekt zabezpečuje rozpracovanie dokumentácie MPSVR SR a jej aktualizáciu v rozsahu uvedenom v stĺpci G.	Bezpečnostná stratégia kybernetickej a informačnej bezpečnosti rezortu MPSVR SR. Bezpečnostná politika MPSVR SR pre oblasť kybernetickej a informačnej bezpečnosti + príloha č. 1 - Bezpečnostné politiky a štandardy Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky a rezortu práce, sociálnych vecí a rodiny Slovenskej republiky.	Požiadavky definované v odst. (2) pre časti, ktoré sú v správe Subjektu
§ 3 Bezpečnostná stratégia kybernetickej bezpečnosti	(1) Bezpečnostná stratégia kybernetickej bezpečnosti určuje ciele, ktoré je potrebné na základe výsledkov analýzy rizík kybernetickej bezpečnosti dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za riadenie kybernetickej bezpečnosti a ďalšie opatrenia odst. (1), (2), (3).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu stratégie kybernetickej bezpečnosti rezortu MPSVR SR a zabezpečuje jej dostupnosť pre Subjekt. Subjekt sa podieľa na spracovaní cieľov stratégie prostredníctvom svojich zástupcov v Bezpečnostnom výbore MPSVR SR.	Bezpečnostná stratégia kybernetickej a informačnej bezpečnosti rezortu MPSVR SR a) príloha č. 1 - Stanovenie a vymedzenie stratégie kybernetickej bezpečnosti rezortu MPSVR SR, b) príloha č. 2 - Vyhlásenie o záväzku o podpore kybernetickej a informačnej bezpečnosti, c) príloha č. 3 - Prehľad najdôležitejších dokumentov kybernetickej a informačnej bezpečnosti Slovenskej republiky a aktuálny zoznam zákonov, vykonávacích predpisov a právnych poriadkov, d) príloha č. 4 - Bezpečnostné politiky a súvisiace bezpečnostné štandardy.	Definovanie/Návrh cieľov za Subjekt
§ 4 Klasifikácia informácií a kategorizácia sietí a informačných systémov	(1) Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa § 20 ods. 2 zákona sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 a ďalšie opatrenia odst. (1) až (10)	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu politiky Riadenie informačných aktív a nadväzných štandardov a zabezpečuje jej dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel vo svojom prostredí. Rozpracuváva Štandard Registratúrny poriadok a registratúrny plán na svoje podmienky.	Politika riadenia informačných aktív. Štandard - Zodpovednosť za aktíva Štandard - Klasifikácia informácií a kategorizácia IS a sietí Štandard - Zaobchádzanie s médiami Štandard - Registratúrny poriadok a registratúrny plán	Registratúrny poriadok a registratúrny plán Subjektu musí spĺňať požiadavky Politiky a štandardov
§ 5 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. a) zákona	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej zásada a) určenia manažéra kybernetickej bezpečnosti, b) najnižších privilégií, c) dodržiavania a vykonávania nezávislého hodnotenia, d) jasného vymedzenia právomoci, povinnosti a zodpovednosti, e) jasného vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností.	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu politiky organizácie bezpečnosti a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel vo svojom prostredí. Subjekt vymenuje zodpovednú osobu do role manažér KB (Bezpečnostného správcu Subjektu pre kybernetickú bezpečnosť). Subjekt zabezpečuje kvalifikáciu, vedomosti a skúsenosti osoby v tejto úlohe k riadnemu plneniu role.	Politika organizácie bezpečnosti. Štandard - Riadenie bezpečnostnej architektúry Štandard - Systém riadenia kybernetickej bezpečnosti Štandard – Riadenie prístupov, identít a prístupových práv Štandard - Zodpovednosť používateľov Štandard - Riadenie privilegovaných prístupov Štandard - Bezpečnostný monitoring a správa bezpečnostných záznamov	Vymenovanie Manažéra KB, formálne upravenie pracovnej/služobnej zmluvy

Časť vyhlášky 362/2018 Z. z.		Aplikovanie opatrení			Popis zodpovedností za dokumentovanie opatrení	
	Požadovaný obsah (stručne)	Centrálne (MPSVR)	Subjektom (NIP)	Popis zodpovedností za aplikáciu opatrení (stĺpec E)	Centrálna bezpečnostná dokumentácia rezortu MPSVR (spracovanie zabezpečuje MPSVR) (stĺpec F)	Bezpečnostná dokumentácia Subjektu (spracovanie zabezpečuje Subjekt) (stĺpec G)
§ 6 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. b) zákona	(1) Riadenie aktív, hrozieb a rizík. Riadenie aktív pozostáva z identifikácie a evidencie všetkých a) aktív, od ktorých závisí poskytovanie základnej služby, b) podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby, c)zodpovedných osôb za identifikáciu a evidenciu aktív a d) vlastníkov aktív a ďalšie opatrenia odst. (1) až (11).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Metodiky hodnotenia rizík a Metodiky hodnotenia aktív a zabezpečuje ich dostupnosť pre Subjekt. MPSVR SR vykonáva pravidelné preskúmanie rizík a spracováva Správu z hodnotenia rizík. Subjekt zabezpečuje implementáciu pravidiel v oblasti riadenia aktív, hrozieb a rizík vo svojom prostredí.	Politika Riadenia bezpečnostných rizík. Štandard - Testovanie a bezpečnostná certifikácia systémov Štandard - Metodika posudzovania vplyvu na ochranu OÚ Štandard - Metodika posudzovania a riadenia rizík Štandard - Fyzická bezpečnosť a bezpečnosť prostredia Štandard - Fyzická bezpečnosť sietí a informačných systémov a bezpečnosť zariadení Štandard - Aktíva pri presune a bez obsluhy	Zoznam informačných aktív (vlastníctvo a ohodnotenie aktív), ktoré nie sú súčasťou centrálneho zoznamu aktív MPSVR SR. Zavedenie štandardov pre aktíva, ktoré nie sú súčasťou centrálneho zoznamu aktív MPSVR SR: Štandard - Fyzická bezpečnosť a bezpečnosť prostredia Štandard - Fyzická bezpečnosť sietí a informačných systémov a bezpečnosť zariadení Štandard - Aktíva pri presune a bez obsluhy
§ 7 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. c) zákona	Personálna bezpečnosť pozostáva najmenej z a) Písomné postupy pri zaradení osoby do niektorých z bezpečnostných rolí, b) zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, c) kontrola dodržiavania bezpečnostných politík, d) hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia a ďalšie opatrenia písm. e) až h).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky pravidiel správania a dobrej praxe a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti personálnej bezpečnosti. Subjekt zabezpečuje rozpracovanie a politiky správania a dobrej praxe a nadväzných štandardov vo svojom prostredí.	Politika pravidiel správania a dobrej praxe. Štandard - Mobilné zariadenia a práca na diaľku Štandard - Riadenie personálnej bezpečnosti Štandard - Vzdelávanie zamestnancov, bezpečnostné povedomie Štandard - Pravidlá komunikácie	Pre IKT v správe Subjektu: Politika pravidiel správania a dobrej praxe (v podmienkach Subjektu). Štandard - Riadenie personálnej bezpečnosti(v podmienkach Subjektu). Štandard - Práca na diaľku a používanie mobilných zariadení (v podmienkach Subjektu).
§ 8 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. d) zákona	(1) Na riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov sa pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 zákona analyzujú riziká dodávateľských služieb, akvizície, vývoja a údržby informačných systémov spôsobom podľa § 6 a ďalšie opatrenia odst (2) až (5).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenia vzťahov s dodávateľmi a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti riadenia dodávateľských služieb. Ak Subjekt uzatvára zmluvný vzťah na dodávky IS a sietí kategórie III a II bez účasti MPSVR SR, zabezpečuje v plnom rozsahu presadenie pravidiel kybernetickej bezpečnosti do zmluvy s dodávateľom, vrátane rozpracovania politiky riadenia vzťahov s dodávateľmi a nadväzných štandardov uvedených v stĺpci F v prostredí svojej organizácie.	Politika riadenia vzťahov s dodávateľmi Štandard - Riadenie dodávateľských služieb a vzťahov Štandard - Akvizícia informačných systémov	Zoznam dodávateľov IS a sietí kategórie III a II, s ktorými Subjekt uzavrel zmluvný vzťah bez účasti MPSVR SR. Dokumentácia podľa stĺpca F na riadenie dodávateľských vzťahov uzavretých spôsobom popísaným v stĺpci E. Vypracovanie zmlúv s treťou stranou pre IKT s vlastnou základnou službou
§ 9 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. e) zákona	Technické zraniteľnosti informačných systémov sa identifikujú prostredníctvom a) nástroja na detegovanie zraniteľnosti programových prostriedkov b) nástroja na detegovanie zraniteľností technických prostriedkov, c) využitia verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti.	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenia Vývoj a údržby v oblasti IKT a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti riadenia pravidiel technických zraniteľností systémov.	Politika riadenia vývoja a údržby v oblasti IKT. Štandard - Bezpečnostné požiadavky na informačné systémy Štandard - Vývoj a testovanie informačných systémov Štandard - Postupy údržby informačných systémov Štandard - Riadenie technických zraniteľností a manažment záplat	Realizácia opatrení pre IKT/základné služby v pôsobnosti Subjektu

Časť vyhlášky 362/2018 Z. z.		Aplikovanie opatrení			Popis zodpovedností za dokumentovanie opatrení	
	Požadovaný obsah (stručne)	Centrálne (MPSVR)	Subjektom (NIP)	Popis zodpovedností za aplikáciu opatrení (stĺpec E)	Centrálna bezpečnostná dokumentácia rezortu MPSVR SR (spracovanie zabezpečuje MPSVR) (stĺpec F)	Bezpečnostná dokumentácia Subjektu (spracovanie zabezpečuje Subjekt) (stĺpec G)
§ 10 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. f) zákona	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej a) riadenie prístupov používateľov k sieťam a informačným systémom podľa § 1, 2 b) prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov a ďalšie opatrenia písm. c) až p).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenia Vývoj a údržby v oblasti IKT a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti zaistenia integrity sietí a informačných systémov.	Politika riadenia vývoja a údržby v oblasti IKT. Štandard - Riadenie bezpečnosti v sieťach Štandard - Pravidlá prepájania systémov a prenosu elektronických informácií	Realizácia opatrení pre IKT/základné služby v pôsobnosti Subjektu
§ 11 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. g) zákona	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených pravidiel a postupov na a)riadenie zmien, b) riadenie záplat a aktualizácií, c) riadenie kapacít, d) pravidelné zálohovanie a testovanie obnovy informácií zo záloh, e) ochranu pred škodlivým kódom, f) inštaláciu softvéru v sieťach a informačných systémoch a ďalšie opatrenia písm. g) až h).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenia Vývoj a údržby v oblasti IKT a nadväzných štandardov a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel bezpečnej prevádzky sietí a IS.	Politika riadenia vývoja a údržby v oblasti IKT. Štandard - Prevádzkové postupy a zodpovednosti - riadenie zmien a kapacít Štandard - Ochrana proti škodlivým softvérom	Realizácia opatrení pre IKT/základné služby v pôsobnosti Subjektu
§ 12 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. h) zákona	Riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom a ďalšie opatrenia odst. (2) až (4)	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu štandardov: Riadenie prístupov, identít a prístupových práv a Riadenie privilegovaných prístupov. a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti riadenia prístupovej osôb k sieti a informačnému systému. Ak je Subjekt oprávnený prideľovať a riadiť privilegované prístupové práva, zabezpečuje rozpracovanie a dodržiavanie štandardov Riadenie privilegovaných prístupov vo svojom prostredí.	Štandard - Riadenie prístupov, identít a prístupových práv Štandard - Riadenie privilegovaných prístupov.	Štandard - Riadenie privilegovaných prístupov (v podmienkach Subjektu). Realizácia opatrení pre IKT/základné služby v pôsobnosti Subjektu
§ 13 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. i) zákona	Dôvernosť, integrita, dostupnosť a hodnovernosť údajov v rámci sietí a informačných systémov, prostredníctvom ktorých je poskytovaná základná služba, sa zabezpečuje pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy a ďalšie opatrenia odst. (2).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenia a prevádzky IKT a štandardu Riadenie kryptografických opatrení a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti riadenia kryptografických opatrení.	Politika riadenia prevádzky IKT. Štandard - Riadenie kryptografických opatrení	N/A

Časť vyhlášky 362/2018 Z. z.		Aplikovanie opatrení			Popis zodpovedností za dokumentovanie opatrení	
	Požadovaný obsah (stručne)	Centrálne (MPSVR)	Subjektom (NIP)	Popis zodpovedností za aplikáciu opatrení (stĺpec E)	Centrálna bezpečnostná dokumentácia rezortu MPSVR SR (spracovanie zabezpečuje MPSVR) (stĺpec F)	Bezpečnostná dokumentácia Subjektu (spracovanie zabezpečuje Subjekt) (stĺpec G)
§ 14 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. j) zákona	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej a) z prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov, b) z monitorovania a analyzovania udalostí v sieťach a informačných systémoch, c) z detekcie kybernetických bezpečnostných incidentov, d) zo zberu relevantných informácií o kybernetických bezpečnostných incidentoch a ďalšie opatrenia odst. (1) až (6).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu štandardu Riešenie bezpečnostných incidentov (Riadenie incidentov kybernetickej a informačnej bezpečnosti) a zabezpečuje jeho dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti riešenia bezpečnostných incidentov v rozsahu podľa čl. 11 zmluvy. Zaisťuje rozpracovanie Štandardu Riešenie bezpečnostných incidentov pre svoje prostredie.	Štandard - Riešenie bezpečnostných incidentov	Štandard - Rozpoznávanie a hlásenie udalostí a incidentov bezpečnosti v podmienkach Subjektu. Hlásenie incidentov Spolupráca pri riešení incidentov
§ 15 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) zákona	(1) Monitorovanie bezpečnosti sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov a ďalšie opatrenia odst. (1) až (5)	x	x	MPSVR SR zabezpečuje monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, prevádzka nástroja je centralizovaná. Subjekt zabezpečuje implementáciu preventívnych opatrení proti narušeniu bezpečnosti informačných systémov a sietí.	Štandard - Bezpečnostný monitoring a správa bezpečnostných záznamov	N/A
§ 16 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. l) zákona	(1) Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom a) umiestnenia siete a informačného systému v takom priestore, že sieť a informačný systém alebo aspoň ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor") a ďalšie opatrenia odst. (1) a (2).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu politiky Riadenie informačných aktív a štandardu Fyzická bezpečnosť a bezpečnosť prostredia a zabezpečuje ich dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu opatrení fyzickej bezpečnosti sietí a informačných systémov vo svojich lokalitách. Zaisťuje rozpracovanie pravidiel MSPVR SR v oblasti fyzickej ochrany na svoje podmienky, prevádzkuje pravidlá a vyhodnocuje ich účinnosť.	Politika Riadenie informačných aktív. Štandard - Fyzická bezpečnosť a bezpečnosť prostredia	Štandard - Fyzická bezpečnosť a bezpečnosť prostredia (v podmienkach Subjektu). Realizácia opatrení v podmienkach Subjetku.
§ 17 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. m) zákona	(1) Prevádzkovateľ základnej služby určí požiadavky na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti pri vzniku kybernetického bezpečnostného incidentu a ďalšie opatrenia odst. (1) a (3).	x	x	MPSVR SR zabezpečuje spracovanie a aktualizáciu Politiky riadenie kontinuity procesov a činností a nadväzujúcich štandardov a zabezpečuje jej dostupnosť pre Subjekt. Subjekt zabezpečuje implementáciu pravidiel v oblasti kontinuity riadenia kybernetickej bezpečnosti v rozsahu svojich systémov. Zaisťuje vypracovanie havarijných plánov a plánov kontinuity lokalít, kde sú prevádzkované systémy alebo ukladané dáta informačných aktív IS kategórie III a II.	Politika riadenie kontinuity procesov a činností. Štandard - Plány kontinuity prevádzkových činností Štandard - Redundancia Štandard - Zálohovanie a obnova informácií	Plán havarijnej obnovy lokalit (v podmienkach Subjektu). Realizácia opatrení v podmienkach Subjetku. Súčinnosť pri tvorbe plánov obnovy, preverovaní záloh a precvičovaní krízových plánov.

Príloha č. 3
k Dohode o určení rozsahu zodpovedností za realizáciu
opatrení kybernetickej a informačnej bezpečnosti

Zoznam pracovných rolí strán dohody a k nim prislúchajúci menný zoznam osôb a ich kontaktných údajov

NIP

Meno a priezvisko	**Rola**	**Telefónne číslo Email**	**Oblasť/zodpovednosť**
Ing. Ján Turza	Manažér KB a IB	Mob. č.: +421 918 704 692 email: jan.turza@ip.gov.sk	Všeobecné povinnosti v zmysle ZoKB a ZoITVS
Ing. Tibor Zádori	Riaditeľ odboru IKT	Tel.: +421 55 79 79 929 Mob. č.: +421 917 520 399 email: tibor.zadori@ip.gov.sk	L2 – eskalácia: - hlásenie kybernetických incidentov, - bezpečnostné opatrenia a činnosti - kontrolná činnosť a audit, všeobecné požiadavky

IP

Meno a priezvisko	**Rola**	**Telefónne číslo Email**	**Oblasť/zodpovednosť**
Jaroslav Bariš	Manažér KB a IB	Mob. č.: +421 907 904 874 email: jaroslav.baris@ip.gov.sk	Všeobecné povinnosti v zmysle ZoKB a ZoITVS