Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov medzi

Prevádzkovateľom základnej služby:

Názov:	**Národné centrum zdravotníckych informácií**
Sídlo:	Lazaretská 26, 811 09 Bratislava 1
IČO:	00165387
DIČ:	2020830119
IČ DPH:	nie je platca DPH
v mene ktorého koná :	Mgr. Pavol Vršanský, riaditeľ
kontaktná osoba:	[redacted]
e-mail kontaktnej osoby:	

(ďalej aj len ako „**Prevádzkovateľ**“)

a

Dodávateľom:

Obchodné meno:	**DATALAN, a.s.**
Sídlo:	Krasovského 14, 851 01 Bratislava
IČO:	35810734
DIČ:	2020259175
IČ DPH:	SK2020259175
v mene ktorého koná:	Ing. Juraj Zelko, člen predstavenstva
kontaktná osoba:	[redacted]
e-mail kontaktnej osoby:	

(ďalej aj len ako „**Dodávateľ**“)
(Prevádzkovateľ a Dodávateľ spolu ďalej aj len ako „**zmluvné strany**“)

Článok I.
Úvodné ustanovenia a vyhlásenia

1. Prevádzkovateľ ako objednávateľ a Dodávateľ ako poskytovateľ uzavreli dňa 20.05.2024 nasledovné zmluvy: Zmluva o dielo na dodávku informačného systému, č. zmluvy u NCZI: 24/2024 (ďalej len ako „**Zmluva o dielo**“), Zmluva o podpore prevádzky, údržbe a rozvoji informačného systému, č. zmluvy u NCZI: 25/2024 (ďalej len ako „**SLA zmluva**“), (Zmluva o dielo a SLA zmluva ďalej spolu aj len ako „**dodávateľské zmluvy**“ a každá samostatne aj len ako „**dodávateľská zmluva**“). Na základe dodávateľských zmlúv sa Dodávateľ

zaväzuje vykonať dielo podľa Prílohy č. 1 Zmluvy o dielo a poskytovať služby podľa Prílohy č. 1 a 2 SLA zmluvy.

2. Prevádzkovateľ je podľa § 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 „**zákon o kybernetickej bezpečnosti**“) prevádzkovateľom základnej služby podľa § 3 písm. l) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

3. V súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti v spojení s § 9 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „**vyhláška OBO**“) zmluvné strany uzatvárajú túto zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**zmluva**“); pred uzatvorením tejto zmluvy sa vykonala analýza rizík a analýza funkčného dopadu.

4. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na uzavreté dodávateľské zmluvy, ktorých predmetom sú služby (činnosti) Dodávateľa, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa ako prevádzkovateľa základnej služby.

5. Vzhľadom na aktuálny stav architektúry IS ezdravie [článok 1. bod 1.1 písm. l) Zmluvy o dielo], ktorý nezohľadňuje všetky požiadavky podľa aktuálne platnej legislatívy, sa zmluvné strany dohodli, že vo vzťahu k Časti RISEZ bez redizajnu podľa článku 1. bodu 1.1 písm. e) Zmluvy o dielo a pre Doplnok ezdravie podľa článku 1. bodu 1.1 písm. k) Zmluvy o dielo je Dodávateľ povinný plniť opatrenia a povinnosti podľa tejto zmluvy primerane; pre účely tohto bodu zmluvy sa pod pojmom „primerane“ rozumie plnenie opatrení a povinností Dodávateľa uvedených v tejto zmluve v maximálnej možnej miere a rozsahu.

Článok II.
Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na dodávateľskú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa (s ktorými priamo súvisí výkon činností Dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv možných kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa.

2. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, ako aj bezpečnostná udalosť za kumulatívneho splnenia nasledovných podmienok:
   a) ktorú zistí alebo o ktorej sa dozvie Dodávateľ,
   b) ktorá sa týka informačných systémov alebo sietí vo vzťahu, ku ktorým Dodávateľ poskytuje výkon činností podľa dodávateľskej zmluvy,
   c) a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti príp. integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa.

Článok III.
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať platné bezpečnostné politiky Prevádzkovateľa, Prevádzkovateľom vydané bezpečnostné smernice a štandardy, ktorými bol Dodávateľ preukázateľne oboznámený (ďalej aj len ako „**bezpečnostná politika**“), a požiadavky na bezpečnosť definované zákonom o kybernetickej bezpečnosti, vyhláškou OBO, zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v platnom znení, ako aj ostatnými všeobecne záväznými právnymi predpismi platnými v čase plnenia tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve. Dodávateľ vyhlasuje, že sa pred podpisom tejto zmluvy oboznámil s platnou bezpečnostnou politikou Prevádzkovateľa a vyjadruje s ňou súhlas.

2. Dodávateľ súhlasí s bezpečnostnou politikou Prevádzkovateľa a s tým, že bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcich sa Dodávateľa, ktoré by mohli mať nepriaznivý vplyv na základnú službu Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať najmenej bezpečnostné opatrenia, ktoré tvoria **Prílohu č. 1** k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami. Bezpečnostné opatrenia uvedené v Prílohe č. 1 smerujú dovnútra Dodávateľa, na jeho interné procesy, ako aj na bezpečnosť poskytovania služieb v prospech Prevádzkovateľa na základe dodávateľských zmlúv; touto zmluvou zároveň nie sú dotknuté povinnosti a požiadavky na plnenia Dodávateľa podľa dodávateľských zmlúv.

4. Dodávateľ súhlasí s tým, že bezpečnostné opatrenia sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov Prevádzkovateľa, pričom nie je potrebné uzatvoriť dodatok k zmluve. Dodávateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené bezpečnostné opatrenia Prevádzkovateľa, a to po uplynutí 5 pracovných dní odo dňa oznámenia zmien alebo doplnení Prevádzkovateľom Dodávateľovi.

5. Dodávateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve, pokiaľ zo všeobecne záväzných právnych predpisov nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľských zmlúv.

6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi.

8. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy v oblastiach podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v rozsahu podľa vyhlášky OBO a v rozsahu špecifikovanom v tejto zmluve.

9. Zoznam zamestnancov Dodávateľa, subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí budú mať prístup k informáciám Prevádzkovateľa (ďalej len „**Zoznam osôb**“) tvorí **Prílohu č. 3** tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v Zozname osôb podľa tohto bodu bezodkladne na e-mailovú adresu kontaktnej osoby Prevádzkovateľa.

10. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá môže mať významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy.

11. Dodávateľ môže zapojiť ďalšieho dodávateľa (subdodávateľa) úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa za splnenia podmienok uvedených v dodávateľských zmluvách.

12. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

13. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nzcisk.sk.

14. Dodávateľ sa zaväzuje poskytnúť Prevádzkovateľovi bezodkladne všetky podklady, informácie a súčinnosť nevyhnutnú k tomu, aby si Prevádzkovateľ mohol riadne a včas plniť všetky povinnosti podľa zákona o kybernetickej bezpečnosti a vyhlášky OBO.

15. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany“ v zmysle zákona o kybernetickej bezpečnosti.

16. Dodávateľ vykonáva len činnosti, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľských zmlúv, tejto zmluvy, všeobecne záväzných právnych predpisov alebo na základe požiadavky Prevádzkovateľa. Na výkon týchto činností môže poveriť Dodávateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v **Prílohe č. 3**.

Článok IV.
Okolnosti plnenia zmluvy

1. Výklad pojmov používaných v tejto zmluve sa nesmie dostať do rozporu s významom, ktorý im je priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou záväzkov podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa podľa dodávateľských zmlúv. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania dodávateľských zmlúv.

4. Odplata za plnenie povinností Dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa dodávateľských zmlúv a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Článok V.
Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

1. Dodávateľ je povinný v rámci prevencie pred kybernetickými incidentmi:
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Dodávateľa nebolo možné ohroziť siete a informačné systémy Prevádzkovateľa,
   b) preukázateľne vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení dodávateľských zmlúv a tejto zmluvy alebo budú mať prístup k dátam alebo informáciám Prevádzkovateľa,
   c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
   d) sledovať hrozby, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   e) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Dodávateľa,
   f) v prípade vzniku kybernetických incidentov v prostredí Dodávateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
   g) prijímať od Prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   h) zasielať Prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   i) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Prevádzkovateľa.

Článok VI.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, ktorý je uvedený v **Prílohe č. 2,** vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „**Reakčné opatrenia**“), a to ako na výzvu Prevádzkovateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.

3. Dodávateľ pri reakciách na incidenty spolupracuje s Prevádzkovateľom, Národným bezpečnostným úradom a inými príslušnými orgánmi a za týmto účelom im poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami, ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

4. Dodávateľ pri riešení a reakcii na kybernetický incident postupuje v súlade so všeobecne záväznými právnymi predpismi, touto zmluvou, ako aj svojimi internými procedúrami a postupmi tak, aby bol kybernetický incident a jeho dôsledky odstránené v čo najkratšom možnom čase, a zaväzuje sa zároveň poskytnúť súčinnosť Prevádzkovateľovi pri riešení kybernetického incidentu.

5. Dodávateľ je povinný oznámiť Prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.

6. Dodávateľ je povinný v čase zistenia kybernetického incidentu, ktorý mal dopad na Prevádzkovateľa, zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho Prevádzkovateľovi.

7. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.

8. Po vyriešení kybernetického incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „**ochranné opatrenie**“) na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na návrhu nového ochranného opatrenia.

9. Po schválení ochranného opatrenia Prevádzkovateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť Prevádzkovateľovi.

10. Dodávateľ je povinný informovať Prevádzkovateľa o skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nczisk.sk.

Článok VII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením dodávateľských zmlúv a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa.

2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.

3. Dodávateľ je povinný chrániť všetky informácie, ku ktorým má prístup na základe dodávateľských zmlúv, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa oboznámil v dôsledku vlastnej činnosti s tým, že všetci dotknutí zamestnanci Dodávateľa, jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých Dodávateľ poskytuje služby podľa dodávateľských zmlúv (ďalej len „**tretia osoba**“) sú povinní zaviazať sa k zachovávaniu mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

4. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba, a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

5. Dodávateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Zozname osôb zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je Dodávateľ povinný preukázať Prevádzkovateľovi u každej z týchto osôb.

6. Ak táto zmluva neustanovuje inak a nevylučuje to všeobecne záväzný právny predpis, zmluvné strany sa pri ochrane dôverných informácií a zachovávaní mlčanlivosti spravujú ustanoveniami článku 12. Zmluvy o dielo. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľských zmlúv alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok VIII.
Kontrolná činnosť a audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa kontrolnú činnosť a audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy. Výdavky Prevádzkovateľa spojené s vykonaním kontroly alebo auditu znáša Prevádzkovateľ.

2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať kontrolu alebo audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom kontrola alebo audit budú zamerané najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností z tejto zmluvy v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Prípadné nedostatky zistené kontrolou alebo auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote šesťdesiat (60) kalendárnych dní.

4. Prevádzkovateľ môže kontrolu alebo audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti Prevádzkovateľa pri výkone kontroly alebo auditu realizuje Prevádzkovateľom poverená tretia osoba.

5. Dodávateľ je pri výkone kontroly alebo audite povinný spolupracovať s Prevádzkovateľom a sprístupniť priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, umožniť osobám určených Prevádzkovateľom voľný vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto zmluvy.

6. Prevádzkovateľ je v rámci kontroly alebo auditu oprávnený klásť otázky zamestnancom Dodávateľa a ďalším osobám, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

7. V rámci kontroly alebo auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a/alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie. Preukázanie skutočností uvedených v predchádzajúcej vete môže Dodávateľ realizovať napr. prostredníctvom predloženia relevantných certifikátov, poučení, prezenčných listín a inej dokumentácie.

8. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej desať (10) pracovných dní vopred svoj zámer vykonať u Dodávateľa kontrolu alebo audit.

9. Vykonanie alebo nevykonanie kontroly alebo auditu Prevádzkovateľom nezbavuje zodpovednosti Dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

10. Ak Dodávateľ neumožní vykonanie kontroly alebo auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

11. Prevádzkovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone kontroly alebo auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené pri návšteve priestorov Dodávateľa v rámci výkonu kontroly alebo auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP"**) a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „**PO**"), s ktorými boli v súlade s týmto bodom, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon kontroly alebo auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať osoby určené Objednávateľom o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone kontroly alebo auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

Článok IX.
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenia kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

3. Dodávateľ je povinný preukázateľným spôsobom dokumentovať (písomne, elektronicky alebo inak) svoju činnosť podľa tejto zmluvy (vrátane evidovania a riešenia kybernetických incidentov a dokumentovania školení svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy) a na žiadosť Prevádzkovateľa mu predložiť túto dokumentáciu (záznamy, správy).

4. V prípade, ak Dodávateľ plní dodávateľskú zmluvu prostredníctvom svojich subdodávateľov, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ mohol vykonať kontrolu alebo audit v súlade s touto zmluvou aj u týchto subdodávateľov.

5. Všetky informácie, ktoré majú vplyv na plnenie tejto zmluvy sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na e-mailové adresy kontaktných osôb uvedené v záhlaví tejto zmluvy a súčasne na e-mailovú adresu: csirt@nczisk.sk.

6. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť Prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, Dodávateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO a za dôsledky a škodu vzniknutú Prevádzkovateľovi alebo akejkoľvek tretej osobe v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu. Prevádzkovateľ má voči Dodávateľovi nárok na náhradu preukázateľnej škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.

7. V prípade porušenia akejkoľvek povinnosti Dodávateľa vyplývajúcej mu z tejto zmluvy, je Prevádzkovateľ oprávnený požadovať od Dodávateľa zaplatenie zmluvnej pokuty vo výške **15 000,- EUR** (slovom: pätnásťtisíc eur) za každé jednotlivé (aj opakované) porušenie zmluvnej povinnosti alebo zmluvnú pokutu vo výške **1 000,- EUR** (slovom: tisíc eur) za každý začatý deň omeškania s plnením zmluvnej povinnosti. Zmluvné strany zhodne prehlasujú, že dojednanie zmluvnej pokuty podľa predchádzajúcej vety pre porušenie zmluvnej povinnosti Dodávateľa považujú za dostatočne určité. Nárok Prevádzkovateľa na náhradu škody v plnej výške, ako aj nárok na náhradu pokút, poplatkov alebo iných peňažných sankcií uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením povinností Dodávateľa, tým nie sú dotknuté.

8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľských zmlúv alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

9. Dodávateľ je povinný odstrániť prípadné porušenie povinnosti vyplývajúcej z tejto zmluvy najneskôr do piatich (5) pracovných dní od doručenia výzvy Prevádzkovateľa, ak sa zmluvné strany nedohodnú písomne inak.

10. Po ukončení tejto zmluvy je Dodávateľ povinný podľa pokynu Prevádzkovateľa vrátiť alebo previesť na Prevádzkovateľa všetky údaje a informácie, ku ktorým mal počas trvania tejto

zmluvy prístup, ako aj údaje a informácie získané v súvislosti s plnením tejto zmluvy, resp. tieto údaje a informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach Prevádzkovateľa.

11. Dodávateľ bezodkladne po ukončení tejto zmluvy, najneskôr však do troch (3) dní, predloží Prevádzkovateľovi sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré priamo alebo nepriamo súvisia s povinnosťami vyplývajúcimi z tejto zmluvy, zo zákona o kybernetickej bezpečnosti alebo z osobitného všeobecne záväzného právneho predpisu v oblasti kybernetickej bezpečnosti a ktoré sa týkajú Prevádzkovateľa. Prevádzkovateľ na základe sumarizácie podľa predchádzajúcej vety písomne informuje Dodávateľa o tom, ktoré podklady a informácie má Dodávateľ vrátiť Prevádzkovateľovi, previesť na Prevádzkovateľa a ktoré má zničiť. Dodávateľ je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do piatich (5) dní odo dňa, kedy Prevádzkovateľ informoval Dodávateľa o spôsobe naloženia s týmito podkladmi a informáciami.

12. Najneskôr ku dňu ukončenia tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovania základnej služby, ktoré musia byť účinné najmenej po dobu piatich (5) rokov po ukončení tejto zmluvy, ak z dodávateľských zmlúv nevyplýva dlhšia doba trvania dodávateľom udelených (poskytnutých) licencií, práv a/alebo súhlasov. Ustanovenia o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľských zmluvách, nie sú týmto dotknuté.

Článok X.
Záverečné ustanovenia

1. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.

2. Táto zmluva sa uzatvára na dobu určitú, a to do skončenia platnosti a účinnosti oboch dodávateľských zmlúv.

3. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve. Odstúpenie od tejto zmluvy je možné vykonať v písomnej forme, pričom odstúpenie od zmluvy musí byť riadne doručené druhej zmluvnej strane. V prípade platného odstúpenia od tejto zmluvy sa zmluva považuje na zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strane.

4. Prevádzkovateľ je oprávnený odstúpiť od tejto zmluvy v prípade, ak Dodávateľ poruší akúkoľvek povinnosť vyplývajúcu mu z tejto zmluvy.

5. Ukončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem práv a povinností, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.

6. Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Prevádzkovateľom a Dodávateľom je zákonnou povinnosťou Prevádzkovateľa. Z uvedeného dôvodu je Prevádzkovateľ v prípade skončenia platnosti tejto zmluvy oprávnený bez ďalšieho odstúpiť od dodávateľských zmlúv uzatvorených s Dodávateľom.

7. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

8. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd Slovenskej republiky.

9. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve, ak táto zmluva neustanovuje inak.

10. Kontaktné osoby zmluvných strán a ich kontaktné údaje môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu alebo kontaktné druhej zmluvnej strane v písomnej forme, pričom nie je potrebné uzatvoriť dodatok k zmluve. Rovnako je oprávnený postupovať Prevádzkovateľ pri zmene spôsobu hlásenia bezpečnostného incidentu uvedeného v **Prílohe č. 2** tejto zmluvy.

11. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu neplatných alebo nevykonateľných ustanovení.

12. Neoddeliteľnou súčasťou tejto zmluvy je:
    Príloha č. 1 – Špecifikácia a rozsah bezpečnostných opatrení
    Príloha č. 2 – Spôsob hlásenia bezpečnostného incidentu
    Príloha č. 3 – Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa.

13. Táto zmluva sa vyhotovuje v štyroch (4) vyhotoveniach s platnosťou originálu, z toho dve (2) pre Prevádzkovateľa a dve (2) pre Dodávateľa.

14. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa	V Bratislave dňa .....
Za Prevádzkovateľa:	Za Dodávateľa:
.....	.....
Mgr. Pavol Vršanský	**Ing. Branislav Šebo**
riaditeľ	predseda predstavenstva
Národné centrum zdravotníckych informácií	DATALAN, a.s.

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

1. **<u>Bezpečnostné opatrenia sa prijímajú a realizujú podľa zákona o kybernetickej bezpečnosti najmä pre oblasti:</u>**

    a. organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
    b. riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
    c. personálna bezpečnosť,
    d. riadenie prístupov,
    e. riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
    f. bezpečnosť pri prevádzke informačných systémov a sietí,
    g. hodnotenie zraniteľností a bezpečnostné aktualizácie,
    h. ochrana proti škodlivému kódu,
    i. sieťová a komunikačná bezpečnosť,
    j. akvizícia, vývoj a údržba informačných technológií,
    k. zaznamenávanie udalostí a monitorovanie,
    l. fyzická bezpečnosť a bezpečnosť prostredia,
    m. riešenie kybernetických bezpečnostných incidentov,
    n. kryptografické opatrenia,
    o. kontinuita prevádzky,
    p. audit a kontrolné činnosti.

Jednotlivé bezpečnostné opatrenia pre oblasti vyplývajú z príslušného znenia vyhlášky OBO. Zmluvné strany berú na vedomie, že obsah povinností Dodávateľa ako tretej strany podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti prijať bezpečnostné opatrenia je daný aktuálnym znením vyhlášky OBO.

Dodávateľ ako vlastník rizík podľa analýzy rizík vyhlasuje, že prijala a bude dodržiavať bezpečnostné opatrenia pre tieto riziká.

Dodávateľ vyhlasuje, že počas trvania zmluvy bude dodržiavať a udržiavať všetky bezpečnostné opatrenia podľa tejto **Prílohy č. 1** zmluvy.

2. **<u>Bezpečnostné opatrenia v zmysle vyhlášky OBO v kontexte identifikovaných rizík:</u>**

2.1 BEZPEČNOSTNÉ OPATRENIA – ORGANIZÁCIA KYBERNETICKEJ BEZPEČNOSTI A INFORMAČNEJ BEZPEČNOSTI

2.1.1 Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2.1.2 Vymedzenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
2.1.3 Dodržiavať princíp najnižších privilégií, každému používateľovi prideliť privilégiá len v rozsahu potrebnom na splnenie pridelených úloh.
2.1.4 Zabránenie každému používateľovi používať alebo upravovať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity.
2.1.5 Zabezpečenie zastupiteľnosti kvalifikovaného personálu.

2.1.6 Dodržiavanie platnej legislatívy, štandardov a best practice,
2.1.7 Eliminovanie chyby personálu zavedením kontroly štyroch očí.
2.1.8 Zabránenie úniku informácií, poučiť personál o informačnej bezpečnosti.
2.1.9 Zabránenie zneužitia práv a kompetencií personálom, nezávislá kontrola štyroch očí.

2.2 BEZPEČNOSTNÉ OPATRENIA - RIADENIE RIZÍK KYBERNETICKEJ BEZPEČNOSTI A INFORMAČNEJ BEZPEČNOSTI

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

2.2.1 Vypracovanie analýzy rizík a funkčného dopadu.
2.2.2 Identifikovanie zraniteľností a hrozieb.
2.2.3 Určenie vlastníka rizika.
2.2.4 Navrhnutie a prijatie bezpečnostných opatrení na elimináciu rizika.
2.2.5 Pravidelné preskúmavanie rizík.
2.2.6 Aktualizovanie analýzy rizík a funkčného dopadu.
2.2.7 Vykonanie analýzy rizík u subdodávateľa.
2.2.8 Ukončenie pracovného pomeru personálu zdokumentovaným spôsobom, vrátiť všetky zverené aktíva.

2.3 BEZPEČNOSTNÉ OPATRENIA – PERSONÁLNA BEZPEČNOSŤ

2.3.1 Zavedenie postupov pri zaradení personálu do rolí a pri presune práv, povinností a zodpovedností na inú osobu.
2.3.2 Zvyšovanie bezpečnostného povedomia personálu zaradeného do jednotlivých rolí.
2.3.3 Vykonanie preukázateľného poučenia personálu zaradeného do jednotlivých rolí o informačnej a kybernetickej bezpečnosti prevádzkovateľa základnej služby.
2.3.4 Zabezpečenie preukázateľného oboznámenia sa personálu zaradeného do jednotlivých rolí s bezpečnostnou politikou prevádzkovateľa základnej služby.
2.3.5 Kontrolovanie dodržiavania bezpečnostných politík prevádzkovateľa základnej služby zo strany personálu zaradených do jednotlivých rolí.
2.3.6 Určenie pravidiel a postupov prípade porušenia bezpečnostnej politiky a interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti zo strany personálu zaradených do jednotlivých rolí.
2.3.7 Určenie postupov pri porušení bezpečnostných politík spočívajúcich v oprávnení obmedziť alebo odňať prístupové oprávnenia a privilégiá.
2.3.8 Zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu alebo zmluvného vzťahu s personálom zaradených do jednotlivých rolí a so subdodávateľom, ktorým sa zabezpečí:
a. vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
b. zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
c. zrušenie prístupových práv v informačných systémoch ,
d. odovzdanie výsledkov práce v súvislosti s informačnými systémami , ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
2.3.9 Zabezpečenie, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
2.3.10 Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
2.3.11 Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre personál zaradených do jednotlivých rolí, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, najmä:
a. prideľovanie prístupových práv,
b. zásady tvorby a používania hesiel,
c. zásady ochrany pred infiltráciou škodlivým kódom,
d. zásady bezpečného používania elektronickej pošty,
e. zásady bezpečného používania internetu,
f. zásady bezpečného používania komunikačných nástrojov a sociálnych sietí,
g. zásady používania prenosných zariadení a médií,
h. zálohovanie údajov,

i. riešenie kybernetických bezpečnostných incidentov,
j. ochranu fyzického majetku,
k. pohyb v priestoroch Dodávateľa.

2.3.12 Zabezpečenie oboznámenia sa personálu zaradených do jednotlivých rolí, že na prístup k informačným technológiám Dodávateľa a Prevádzkovateľa sa vyžaduje:
a. oboznámenie so spôsobom používania informačných technológií a bezpečnostných mechanizmov informačných technológií v rozsahu svojej pracovnej náplne,
b. poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente,
c. oboznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií a bezpečnostných mechanizmov informačných technológií.

2.4 BEZPEČNOSTNÉ OPATRENIA – RIADENIE PRÍSTUPOV

2.4.1 Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií.
2.4.2 Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií.
2.4.3 Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej raz za šesť (6) mesiacov.
2.4.4 Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.
2.4.5 Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
2.4.6 Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
2.4.7 Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.
2.4.8 Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá umožní používateľom najmä:
a. zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,
b. presadzovať určenú štruktúru hesla,
c. vyžadovať pravidelnú zmenu hesla,
d. uchovávať a prenášať používateľské heslá bezpečným spôsobom.
2.4.9 Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do informačných technológií a ich obmedzenie len na nevyhnutné prípady.
2.4.10 Pridelenie každému používateľovi siete a informačného systému jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému.
2.4.11 Overenie identity každého používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému podľa prístupových oprávnení (čítanie, zápis).
2.4.12 Preskúmavanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za šesť (6)mesiacov.
2.4.13 Zablokovanie nepoužívaných prístupových oprávnení natrvalo.
2.4.14 Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií a na prácu na diaľku.
2.4.15 Automatické zaznamenávanie každého prístupu privilegovaného používateľa do informačných technológií a automatické zaznamenávanie prístupu používateľa.
2.4.16 Vykonanie kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
2.4.17 Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom a za zmazanie, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému zmysle príslušnej bezpečnostnej politiky.
2.4.18 Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií.
2.4.19 Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť (6) mesiacov.
2.4.20 Implementácia, vynucovanie prístupových rolí v informačných technológiách.

2.4.21 Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov dvanásť (12) mesiacov.

2.5 BEZPEČNOSTNÉ OPATRENIA – RIADENIE KYBERNETICKEJ BEZPEČNOSTI A INFORMAČNEJ BEZPEČNOSTI VO VZŤAHOCH S TRETÍMI STRANAMI

2.5.1 Na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami sa pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 zákona analyzujú riziká dodávateľských služieb, spôsobom podľa § 6.

2.5.2 V zmluve so Subdodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.

2.5.3 Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií.

2.5.4 Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú najmenej záväzok:

a. plnenia určených požiadaviek a kritérií pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti pri dodávke predmetu zmluvy,

b. ochrany informácií, ku ktorým je poskytnutý prístup,

c. oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti a ďalších opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti špecifických na plnenie predmetu Základného kontraktu a tejto Zmluvy,

d. riadenia a monitorovania prístupov do informačných technológií vrátane spôsobu a mechanizmu,

e. možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,

f. oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,

g. spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,

h. zachovania úrovne kybernetickej bezpečnosti a informačnej bezpečnosti pri významných zmenách vrátane spôsobu a formy prechodu k inému Subdodávateľovi.

2.5.5 Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti a posúdia sa najmä:

a. kritické komponenty a prvky služby,

b. možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,

c. možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch medzi Dodávateľom a Subdodávateľmi,

d. ďalšie možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému Subdodávateľovi.

2.5.6 Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.

2.5.7 Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti Dodávateľa.

2.5.8 Pre informačné technológie, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.

2.5.9 Interný predpis ustanovujúci zásady kybernetickej bezpečnosti a informačnej bezpečnosti pre Subdodávateľov a tretie strany obsahuje najmenej bezpečnostné požiadavky:

a. pri riadení vzťahov so Subdodávateľmi,

b. pri ošetrení kybernetickej bezpečnosti a informačnej bezpečnosti v zmluvách so Subdodávateľmi,

c. dodávateľských reťazcov informačných technológií,

d. monitorovania a preskúmavania dodávateľských služieb,

e. riadenia zmien v službách Subdodávateľa,

f. na prístupové práva a účty,
g. na fyzickú bezpečnosť,
h. na ochranu a zálohovanie dát,
i. na mobilné prostriedky a vzdialený prístup.

2.5.10 Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu so Subdodávateľmi.

2.6 BEZPEČNOSTNÉ OPATRENIA – BEZPEČNOSŤ PRI PREVÁDZKE INFORMAČNÝCH SYSTÉMOV A SIETÍ

2.6.1 Všetky zmeny v prevádzkovaných informačných technológiách, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.

2.6.2 Vypracovanie a zavedenie interného riadiaceho aktu riadenia zmien, ktorý obsahuje:
a. posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík
b. návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň,
c. vypracovanie analýzy rizík a analýzy dopadov,
d. bezpečnostné testovanie implementovanej zmeny,
e. vyhotovenie bezpečnostnej správy (riziková analýza, security review, penetračný test).
f. zaznamenávanie vykonaných zmien

2.6.3 Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.

2.6.4 V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.

2.6.5 Zabezpečenie urgentnej bezpečnostnej aktualizácie APV.

2.6.6 Na jednotlivých prvkoch informačných technológií sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií:
a. operačné systémy,
b. virtualizačné prostredia,
c. aplikačný softvér,
d. pracovné stanice,
e. sieťové zariadenia, vrátane bezpečnostných zariadení,
f. databázové prostredia.

2.6.7 Monitorovanie informačných technológií na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.

2.6.8 Vypracovanie a zavedenie interného riadiaceho aktu riadenia kapacitných požiadaviek APV.

2.6.9 Vzájomné oddelenie vývojového, integračného, predprodukčného a produkčného prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

2.6.10 Zaznamenávanie a vyhodnocovanie bezpečnostných záznamov.

2.6.11 Zaznamenávanie a vyhodnocovanie prevádzkových záznamov.

2.7 BEZPEČNOSTNÉ OPATRENIA – HODNOTENIE ZRANITEĽNOSTÍ A BEZPEČNOSTNÉ AKTUALIZÁCIE

2.7.1 Nastavenie automatickej aktualizácie operačného systému a aplikácií.

2.7.2 Dodávateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.

2.7.3 Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných Dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.

2.7.4 Vykonávanie hodnotenie zraniteľností najmenej raz za šesť (6) mesiacov.

2.7.5 Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií.

2.7.6 Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií.

2.7.7 Jednotlivé prvky informačných technológií monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií.

2.7.8 Primárnymi zdrojmi na identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú:
a. informácie zo systémov a automatizovaných technológií pre aktualizáciu,
b. informačný servis výrobcov technológií,
c. výstupy z bezpečnostných technológií,
d. výsledky penetračných testov,
e. oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti,
f. webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti.

2.7.9 Vypracovanie a zavedenie interného riadiaceho aktu riadenia aktualizácií a záplat, ktorý obsahuje:
a. identifikáciu a posúdenie potrieb softvérových aktualizácií a záplat,
b. evidenciu softvérových aktualizácií a záplat a informácie o ich nasadení a dôvodoch nasadenia,
c. informácie o testovaní softvérových aktualizácií a záplat,
d. zabezpečenie implementácie softvérových aktualizácií a záplat,
e. aktualizáciu plánu softvérových aktualizácií a záplat.

2.7.10 Výnimky z implementácie bezpečnostných aktualizácií sa schvaľujú a evidujú manažérom kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý určuje bezpečnostné opatrenia na ochranu pred zneužitím zraniteľnosti, na elimináciu ktorej je bezpečnostná aktualizácia vydaná.

2.7.11 Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií.

2.7.12 Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.

2.7.13 Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verifikovaný, najmä jeho správna funkcionalita.

2.7.14 Implementovanie nechválených aktualizácií a záplat nie je povolené.

2.7.15 Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť (6) mesiacov.

2.7.16 Bezpečnostné a ostatné aktualizácie sa implementujú najmä prostredníctvom automatizovaného nástroja.

2.8 BEZPEČNOSTNÉ OPATRENIA – OCHRANA PROTI ŠKODLIVÉMU KÓDU

2.8.1 Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.

2.8.2 Určenie zodpovednosti používateľov informačných systémov prevádzkovateľa základnej služby za prevenciu pred škodlivým kódom.

2.8.3 Zamedzenie používateľom odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu.

2.8.4 V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.

2.8.5 Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na:
a. používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
b. škodlivé e-mailové prílohy a odkazy,
c. podozrivé a škodlivé webové stránky a odkazy,
d. externú a internú sieťovú komunikáciu u Dodávateľa vrátane webových sídiel,
e. prenos súborov z externých sietí.

2.8.6 Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.

2.8.7 Zavedenie ochrany informačných technológií pred škodlivým kódom najmenej v rozsahu:
a. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
b. detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách,

c. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
d. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu.

2.8.8 Zavedenie ochrany pred nevyžiadanou elektronickou poštou.
2.8.9 Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu.
2.8.10 Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov.
2.8.11 Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom.

2.9 BEZPEČNOSTNÉ OPATRENIA – SIEŤOVÁ A KOMUNIKAČNÁ BEZPEČNOSŤ

2.9.1 Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.
2.9.2 Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:
a. pravidelná aktualizácia firmvéru,
b. zmena továrensky nastavených autentifikačných údajov,
c. pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
d. vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.
2.9.3 Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.
2.9.4 Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.
2.9.5 Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.
2.9.6 Správa počítačových sietí je riadená a kontrolovaná.
2.9.7 Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb.
2.9.8 Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a pre vzdialený prístup, napr. bezpečným spôsobom s použitím viacfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
2.9.9 Vyžadovanie použitia dvojfaktorovej autentizácie pre každý vzdialený prístup do internej siete.
2.9.10 Zabezpečenie serverov dostupných z externých sietí podľa odporúčaní výrobcu.
2.9.11 Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
2.9.12 Umožnenie v sieťach len špecifikované služby (sieťové a informačných systémov) umiestnené vo vyhradených segmentoch počítačovej siete.
2.9.13 Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.
2.9.14 Sieťové služby, používatelia a jednotlivé prvky informačných technológií musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni.
2.9.15 Povoľovanie spojenia medzi segmentmi siete a externými sieťami, ktoré sú chránené firewallom sú na princípe zásady najnižších privilégií.
2.9.16 Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.
2.9.17 Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.
2.9.18 Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.
2.9.19 Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.

2.9.20 Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.
2.9.21 Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii.
2.9.22 Vzdialený prístup do vnútornej siete Dodávateľa musí podliehať autentifikácii a autorizácii.
2.9.23 Dodávateľ implementuje technológiu detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.
2.9.24 Na všetkých serveroch podporujúcich základné služby informačných technológií správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
2.9.25 Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.
2.9.26 Blokovanie neoprávnených spojení zo zdrojov známych adries identifikovaných ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
2.9.27 Implementovanie systému na prevenciu a detekciu prienikov a proaktívne blokovanie škodlivej sieťovej prevádzky.
2.9.28 Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
2.9.29 Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
2.9.30 Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
2.9.31 Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripájajú do internej siete prevádzkovateľa základnej služby, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

2.10 BEZPEČNOSTNÉ OPATRENIA – AKVIZÍCIA, VÝVOJ A ÚDRŽBA INFORMAČNÝCH TECHNOLÓGIÍ

2.10.1 Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2.10.2 Pri vytváraní nových alebo úprave existujúcich informačných technológií sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.
2.10.3 Zabezpečenie kontroly nad verziami softvéru a zabudovaného softvéru.
2.10.4 Zavedenie pravidiel riadenia konfigurácií, ktoré zabránia nechváleným a nezdokumentovaným zmenám konfigurácií, s cieľom udržovania sietí a informačných systémov v požadovanom, konzistentnom a očakávanom stave ich funkcií.
2.10.5 Zavedenie pravidiel pre vykonávanie údržby sietí a informačných systémov, ktoré zaručia vymedzenie zodpovedností a pracovných postupov, ktorých cieľom je minimalizácia hrozieb vyplývajúcich z neúmyselných chýb alebo úmyselnej manipulácie pri údržbe sietí a informačných systémov.
2.10.6 Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov.
2.10.7 Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.
2.10.8 Informácie v transakciách informačných technológií alebo medzi informačnými technológiami sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.
2.10.9 Všetky zmeny v informačných technológiách a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.
2.10.10 Vývoj aplikácií a systémov musí byť vyvíjaný v bezpečnom vývojovom prostredí s použitím nástrojov, ktoré musia byť:
a. získané legálnym spôsobom z dôveryhodných zdrojov,

b. stále podporované výrobcom nástroja (t. j. výrobca poskytuje bezpečnostné aktualizácie) a nesmú byť označené ako zastarané,
c. aktualizované minimálne raz za 6 mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.

2.10.11 Určenie požiadavky na metodiku softvérového vývoja s cieľom najmä:
a. začleniť bezpečnostné požiadavky a kritériá do každej fázy procesu vývoja softvéru, a to vrátane aplikačnej architektúry a koncepcií použiteľnosti softvérového produktu,
b. zaručiť, že sa použijú najnovšie a najbezpečnejšie verzie nástrojov a komponentov na vývoj softvéru,
c. zaručiť, že sa použijú len softvérové knižnice a komponenty, ktoré pochádzajú od dôveryhodných dodávateľova sú aktívne podporované,
d. zaručiť, že je kód udržateľný, konzistentný, čitateľný, efektívny a bezpečný,
e. zaručiť, že je udržovaný register softvérových komponentov,
f. zaručiť validáciu postupov tak, že softvérový modul neakceptuje nesprávny a neočakávaný vstup,
g. zaručiť, že vo vyvíjanom softvéri je nakonfigurovaný proces logovania, ktorý umožňuje včas zachytiť systémové a bezpečnostné udalosti, s cieľom identifikovať, analyzovať a riešiť neobvyklé udalosti a podozrivé správanie v rámci sietí a informačných systémov.

2.10.12 Vývoj a akvizícia siete a informačného systému sa musí uskutočniť s ohľadom na zaistenie kompatibility s existujúcimi systémami a zachovania nastavenej úrovne bezpečnosti.

2.10.13 Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.

2.10.14 Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.

2.10.15 Súčasťou akceptačného testovania informačných technológií je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.

2.10.16 Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre Prevádzkovateľa, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.

2.11 BEZPEČNOSTNÉ OPATRENIA – ZAZNAMENÁVANIE UDALOSTÍ A MONITOROVANIE

2.11.1 Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov sa uskutočňuje najmenej v rozsahu:
a. zaznamenávanie úspešných a neúspešných autentifikačných udalostí,
b. zaznamenávanie udalostí a monitorovanie sieťových prvkov a serverov, ak sú súčasťou služieb Prevádzkovateľa,
c. zaznamenávanie udalostí a monitorovanie služieb prístupných do externých sietí, ak sú súčasťou služieb pre Prevádzkovateľa,
d. zaznamenávanie udalostí a monitorovanie kritických interných serverov a služieb, ak sú súčasťou služieb pre Prevádzkovateľa,

2.11.2 Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií.

2.11.3 Pre každý prvok informačných technológií sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií musia byť podľa tejto špecifikácie nakonfigurované.

2.11.4 Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:
a. úspešné a neúspešné autorizačné udalosti,
b. úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
c. úspešné a neúspešné prístupy k log súborom,
d. úspešné a neúspešné prístupy k systémovým zdrojom,

e. vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
f. zmeny v prístupových oprávneniach,
g. aktivácia a deaktivácia bezpečnostných mechanizmov,
h. spustenie a zastavenie procesov,
i. konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
j. spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
k. významné aktivity v sieťovej komunikácii,
l. požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
m. IP adresy pridelené prostredníctvom služby DHCP.
n. aktivity vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,
o. zmenu pravidiel firewallu alebo zmenu hesla,
p. automatické varovné alebo chybové hlásenia systémov,
q. detegované podozrivé alebo škodlivé aktivity a ďalšie informácie nevyhnutné na posúdenie závažnosti bezpečnostného incidentu.

2.11.5 Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:
a. čas a dátum udalosti,
b. identifikácia používateľa,
c. identifikácia zariadenia,
d. informácia týkajúca sa udalosti,
e. indikácia úspešnosti, alebo zlyhania operácie,
f. pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port,

2.11.6 Záznamy udalostí sa uchovávajú najmenej dvanásť (12) mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.

2.11.7 Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.

2.11.8 Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.

2.11.9 Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií synchronizovaný prostredníctvom presného časového zdroja.

2.11.10 Dodávateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií.

2.11.11 Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.

2.11.12 Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.

2.11.13 Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.

2.11.14 Bezpečnostný dohľad podľa 2.11.1 písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.

2.11.15 Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.

2.11.16 Prenášanie a presmerovanie záznamov je zabezpečené prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete.

2.11.17 Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

2.11.18 Určenie a poverenie zamestnanca zodpovedného za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonanie nahlásenia podozrivej aktivity.

2.12 BEZPEČNOSTNÉ OPATRENIA – FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ PROSTREDIA

2.12.1 Informačné technológie sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

2.12.2 Umiestnenie informačných technológií v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa.

2.12.3 Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.

2.12.4 Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám.

2.12.5 Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá:

a. údržby, uchovávania a evidencie technických komponentov informačných technológií a zariadení informačných technológií,

b. používania zariadení informačných technológií na iné účely, než na aké sú pôvodne určené,

c. používania zariadení informačných technológií mimo určených priestorov,

d. vymazávania, vyraďovania a likvidovania zariadení informačných technológií a všetkých typov relevantných záloh,

e. prenosu technických komponentov informačných technológií alebo zariadení informačných technológií mimo priestorov Dodávateľa,

f. narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

2.12.6 Prvky informačných technológií s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.

2.12.7 Podporná infraštruktúra informačných technológií s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.

2.12.8 Pre informačné technológie s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

2.12.9 Zabezpečenie implementácie a kontroly dodržiavania pravidiel na prácu v zabezpečenom priestore

2.12.10 Zabezpečenie a zaručenie, že prevádzka používanie a manažment siete a informačných systémov je v súlade s vnútornými predpismi a zmluvnými záväzkami

2.13 BEZPEČNOSTNÉ OPATRENIA – RIEŠENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

2.13.1 Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií, ktoré sú zistené pri ich používaní alebo správe.

2.13.2 Dodávateľ má na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov.

2.13.3 Interný riadiaci akt obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.

2.13.4 S interným riadiacim aktom, najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií.

2.13.5 Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách sa vytvára kontaktné miesto.

2.13.6 Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.

2.13.7 Proces odborného posúdenia a analýzy oznámení realizuje manažér kybernetickej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií alebo príslušnou jednotkou CSIRT/CERT.

2.13.8 Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.

2.13.9 Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy.

2.13.10 Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov.

2.13.11 Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.

2.13.12 Dodávateľ má vytvorené plány na riešenie kybernetických bezpečnostných incidentov.

2.13.13 Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľovi.

2.13.14 Detegovanie kybernetických bezpečnostných incidentov.

2.13.15 Zabezpečenie zberu relevantných informácií o kybernetických bezpečnostných incidentoch, vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetický bezpečnostný incident.

2.13.16 Riešenie zistených kybernetických bezpečnostných incidentov a vyhodnocovanie spôsobov ich riešenia, po ich vyriešení prijatie opatrení a zavedenie nových postupov na minimalizáciu výskytu obdobných incidentov v súčinnosti s prevádzkovateľom.

2.13.17 Pridelenie zodpovednosti a určenie postupov na zvládanie kybernetických bezpečnostných incidentov.

2.13.18 Vedenie evidencie kybernetických bezpečnostných incidentov a zabezpečenie dôkazu alebo dôkazného prostriedku aj informácie, na základe ktorých sa identifikuje vznik a pôvod kybernetického bezpečnostného incidentu.

2.13.19 Tretia strana je povinná poskytnúť Prevádzkovateľovi základnej služby najmä nasledovné informácie o kybernetickom bezpečnostnom incidente:

a. funkcia a pracovné zaradenie osoby Tretej strany, ktorá hlási kybernetický bezpečnostný incident;

b. identifikačné údaje ďalších osôb dotknutých kybernetickým bezpečnostným incidentom;

c. informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu, najmä (ak relevantné):

i. kategória kybernetického bezpečnostného incidentu v zmysle Vyhlášky č. 165/2018 Z. z. , ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov;

ii. typ kybernetického bezpečnostného incidentu (napr. pokus o prienik do systému,

iii. podozrenie na úspešný prienik do systému vrátane APT, nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby), neoprávnený prístup k informáciám, únik informácií, poškodenie informácií, podvod (neautorizované využitie prostriedkov, porušenia autorských práv), iné,

iv. identifikácia nežiaduceho obsahu (napr. spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),

v. identifikácia škodlivého kódu (napr. vírus, malvér, ransomvér),

vi. spôsob identifikácie kybernetického bezpečnostného incidentu a informácií o kybernetickom bezpečnostnom incidente (skenovanie site, odpočúvanie, sociálne inžinierstvo),

vii. identifikácia zraniteľnosti,

d. časové údaje zistenia a vzniku kybernetického bezpečnostného incidentu,

e. čas začiatku incidentu (ak je známy), informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,

f. detailný opis priebehu kybernetického bezpečnostného incidentu a jeho prvotná príčina,

g. popis rozsahu a odhad výšky škôd,

h. odhad závažnosti dopadu kybernetického bezpečnostného incidentu na tretie strany, i. identifikácia ohrozenej alebo narušenej základnej služby a ďalšie v dôsledku kybernetického bezpečnostného incidentu, najmä:

i. ohrozené alebo narušené aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby,
ii. informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity základnej služby alebo činností Prevádzkovateľa základnej služby a či je aktívum v čase podávania hlásenia v prevádzke,
j. informácie o riešení kybernetického bezpečnostného incidentu,
k. stav riešenia kybernetického bezpečnostného incidentu,
l. informácia o vykonaní opatrení smerujúcich k riešeniu hláseného kybernetického bezpečnostného incidentu,
m. opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
n. výsledok prijatých opatrení,
o. dátum a čas realizácie opatrení.

2.14 BEZPEČNOSTNÉ OPATRENIA – KRYPTOGRAFICKÉ OPATRENIA

2.14.1 Pri informačných technológiách s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.

2.14.2 Pri informačných technológiách s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä:
a. elektronických dokumentov,
b. dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
c. e-mailovej komunikácie prostredníctvom PGP alebo S/MIME,
d. komunikačných kanálov na výmenu nešifrovaných dát,
e. centrálnych úložísk,
f. záloh,
g. na vykonávanie správy sietí a informačných systémov.

2.14.3 Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä:
a. princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
b. definovanie požadovanej úrovne ochrany a štandardy šifrovania,
c. roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
d. riadenie šifrovacích kľúčov.

2.14.4 Každé použitie kryptografického prostriedku v informačných technológiách sa zadokumentuje v dokumentácii k informačným technológiám, najmenej na úrovni využívaného algoritmu a verzie.

2.14.5 Dodávateľ pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.

2.14.6 Zabezpečenie bezpečného nakladania s kryptografickými kľúčmi a certifikátmi.

2.14.7 Umožnenie kontroly a auditu systému správy kryptografických kľúčov a certifikátov.

2.15 BEZPEČNOSTNÉ OPATRENIA – KONTINUITA PREVÁDZKY

2.15.1 Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií a služieb, ktoré zabezpečujú.

2.15.2 Na informačné technológie s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií.

2.15.3 Plán kontinuity prevádzky obsahuje najmä:
a. roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
b. možné vplyvy na prevádzku informačných technológií,
c. časový rámec obnovy,
d. identifikáciu zdrojov potrebných na obnovu prevádzky,
e. identifikáciu zamestnancov potrebných na obnovu prevádzky,
f. identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
g. identifikáciu priestorov potrebných na obnovu prevádzky,
h. stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),

i. identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
j. spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
k. konkrétne havarijné procedúry slúžiace na obnovu prevádzky.

2.15.4 Zabezpečenie spolupráce (súčinnosť) pri vykonávaní pravidelného preverenia záloh, testovaní obnovy záloh a precvičovaní zavedených krízových plánov (plánu kontinuity) najmenej raz ročne.

2.15.5 Zabezpečenie spolupráce (súčinnosť) pri testovaní a vyhodnocovaní jednotlivých procesov riadenia kontinuity činnosti a realizácia opatrení na zvýšenie odolnosti sietí a informačných systémov.

2.16 BEZPEČNOSTNÉ OPATRENIA – AUDIT A KONTROLNÉ ČINNOSTI

2.16.1 Zabezpečenie výkonu pravidelných interných auditov kybernetickej bezpečnosti a informačnej bezpečnosti.

2.16.2 Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie, hodnotenie zraniteľností a penetračné testy.

2.16.3 Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti.

2.16.4 Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.

2.16.5 Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.

2.16.6 Umožniť Prevádzkovateľovi základnej služby vykonávanie kontrolnej činnosti a auditu u tretej strany v oblasti kybernetickej a informačnej bezpečnosti v rozsahu tejto zmluvy.

2.16.7 Zmluvné strany sa dohodli na nasledovnom rozsahu, spôsobe a možnostiach výkonu Kontroly u Tretej strany:

a. Tretia strana je povinná na požiadanie Prevádzkovateľa základnej služby v primeranom čase nie dlhšom ako 5 dní od doručenia žiadosti Prevádzkovateľa základnej služby umožniť Kontrolu vykonávanú Prevádzkovateľom základnej služby alebo ním poverenou osobou, ktorého Prevádzkovateľ základnej služby výkonom Kontroly poveril;

b. Zástupcovia Prevádzkovateľa základnej služby zúčastňujúci sa Kontroly alebo vykonávajúci Kontrolu sú povinní dodržiavať všetky právne predpisy a interné predpisy Tretej strany, s ktorými boli Treťou stranou oboznámení;

c. Tretia strana je povinná pri Kontrole spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa Zmluvy alebo Hlavnej zmluvy;

d. Prevádzkovateľ základnej služby je v rámci Kontroly oprávnený klásť otázky zamestnancom Tretej strany, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa Zmluvy za prítomnosti osoby poverenej Treťou stranou.

e. Náklady spojené s výkonom Kontroly unáša každá Zmluvná strana samostatne.

Príloha č. 2 Spôsob hlásenia bezpečnostného incidentu

1) Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v záhlaví tejto zmluvy.

2) Pri nahlasovaní incidentu je potrebné uviesť, že sa jedná o bezpečnostný incident v zmysle tejto zmluvy a tiež kontaktnú osobu, s ktorou je možné komunikovať za účelom získania dodatočných informácií súvisiacich s procesom analýzy a riešenia bezpečnostného incidentu.

3) Samotný spôsob a forma hlásenia bezpečnostného incidentu sa bude riadiť platným predpisom Prevádzkovateľa – „Riadenie bezpečnostných incidentov“.

Príloha č. 3 Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa

Prevádzkovateľ:

Meno a priezvisko	***Rola***	***Proces súvisiaci s prevádzkou služby***	***Telefónny kontakt***	***E-mail***
[redacted]	Projektový manažér	Zodpovednosť za realizáciu projektu	[redacted]	
	Manažér kybernetickej bezpečnosti	Riadenie informačnej a kybernetickej bezpečnosti		
	Riaditeľ odboru bezpečnosti IS	Technická podpora pre oblasť bezpečnosti		
	SLA Manažér	Osoba zodpovedná za SLA		

Dodávateľ:

Meno a priezvisko	***Rola***	***Proces súvisiaci s prevádzkou služby***	***Telefónny kontakt***	***E-mail***
[redacted]	Projektový manažér	Zodpovednosť za realizáciu projektu	[redacted]	
	Hlavný SW analytik	Hlavný SW analytik		
	Architekt pre existujúcu architektúru	Architekt pre existujúcu architektúru		
	Hlavný architekt pre novú architektúru	Hlavný architekt pre novú architektúru		
	Vývojár pre existujúcu architektúru	Vývojár pre existujúcu architektúru		
	Hlavný vývojár pre novú architektúru	Hlavný vývojár pre novú architektúru		
	Hlavný tester	Hlavný tester		
	Databázový špecialista pre existujúcu architektúru	Databázový špecialista pre existujúcu architektúru		
	Hlavný databázový špecialista pre novú architektúru	Hlavný databázový špecialista pre novú architektúru		
	Špecialista pre oblasť integrácie	Špecialista pre oblasť integrácie		

[redacted]	Špecialista pre oblasť bezpečnosti	Riadenie informačnej a kybernetickej bezpečnosti	[redacted]
	Špecialista pre oblasť biznis procesov	Špecialista pre oblasť biznis procesov	
	Špecialista pre oblasť platformy orchestrácie kontajnerov	Špecialista pre oblasť platformy orchestrácie kontajnerov	
	Špecialista pre oblasť prevádzky informačných technológií	Osoba zodpovedná za SLA	