

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:
zapísaným:
v mene ktorého koná:

kontaktná osoba:
e-mail kontaktnej osoby:

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

a

Dodávateľom:
Obchodné meno:
Sídlo:
IČO:
DIČ:
IČ DPH:
zapísaným:
v mene ktorého koná:

kontaktná osoba:
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 uzavrel s Dodávateľom ako zhotoviteľom Zmluvu (ďalej aj len ako „**dodávateľská zmluva**“).
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. Za účelom plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a § 8 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**“); pri uzatvorení zmluvy sa vykonáva analýza rizík.
4. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na dodávateľskú zmluvu, na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi služby (činnosti), ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

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 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:
 - 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. Poskytovateľ 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 v 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 potenciálny 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 Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami Prevádzkovateľa.
4. Dodávateľ súhlasí s tým, že bezpečnostné opatrenia Prevádzkovateľa 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 od okamihu, v ktorom ho s nimi Prevádzkovateľ preukázateľne oboznámi.
5. Dodávateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti počas celej doby trvania tejto zmluvy, pokiaľ zo všeobecne záväzných právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.
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 bezpečnostnej politike Prevádzkovateľa.
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 mailovú adresu kontaktnej osoby Prevádzkovateľa.
10. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy.

11. Dodávateľ môže zapojiť do poskytovania služieb na základe dodávateľskej zmluvy ďalšieho dodávateľa (subdodávateľ), ak mu to vyplýva z ustanovení dodávateľskej zmluvy počas doby jej platnosti a účinnosti.
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 alebo 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. Poskytovateľ vykonáva len činnosti, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy, tejto zmluvy, všeobecne záväzných právnych predpisov alebo na základe požiadavky Prevádzkovateľa. Na výkon týchto činností môže poveriť Poskytovateľ 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 dodávateľskej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania dodávateľskej zmluvy.
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 dodávateľskej zmluvy 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 zmluvy na výkon činností 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 potencionálny 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 potencionálny 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
 - 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.

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 kybernetického incidentu, ktorý mal dopad na Prevádzkovateľa, zabezpečiť 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 aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve.

Článok VII. Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy na výkon činností a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli týkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa týka 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 dodávateľskej zmluvy, 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 subdodávateľa a/alebo iné tretie osoby, prostredníctvom ktorých Dodávateľ poskytuje služby podľa dodávateľskej zmluvy (ďalej len „**tretia osoba**“) sú povinní zaviazat' 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, subdodávateľa 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. dodávateľskej zmluvy. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok VIII. Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa 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 auditu znáša Prevádzkovateľ.
2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností 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 auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
4. Prevádzkovateľ môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu realizuje Prevádzkovateľom poverená tretia osoba.
5. Dodávateľ je pri 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 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 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 10 pracovných dní vopred svoj zámer vykonať u Dodávateľa audit.
9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezavahuje zodpovednosti Dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.
10. Ak Dodávateľ neumožní vykonanie 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 auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP**“) a ochrany pred požiarom 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 auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať osoby určené Objednávateľom o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone 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 dokumentovať 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.
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 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@nzcisk.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 akejkolvek 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 povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, je Dodávateľ povinný Prevádzkovateľovi zaplatiť zmluvnú pokutu vo výške 15 000,- EUR; nárok Prevádzkovateľa na náhradu škody v plnej výške, 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 povinností Dodávateľa, tým nie sú dotknuté.
8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.
9. 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.
10. 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 vyplývajúcich 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.
11. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy, ak z dodávateľskej zmluvy 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 dodávateľskej zmluve, 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, nie však skôr ako dňom nadobudnutia účinnosti dodávateľskej zmluvy.
2. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania platnosti a účinnosti dodávateľskej zmluvy.
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 za 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 alebo záväzok plynúci mu z tejto zmluvy.
5. Prevádzkovateľ je oprávnený vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou 3 mesiace. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená výpoveď Dodávateľovi.
6. 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.
7. 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 dodávateľskej zmluvy uzatvorenej s Dodávateľom.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.

13. Neoddeliteľnou súčasťou tejto zmluvy je:
Príloha č. 1 – Požiadavky na bezpečnostné opatrenia
Príloha č. 2 – Spôsob hlásenia bezpečnostného incidentu
Príloha č. 3 – Zoznam osôb a pracovných rolí Dodávateľa
14. Táto zmluva sa vyhotovuje v 4 rovnopisoch, po 2 pre každú zmluvnú stranu.
15. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa

V dňa

Za Prevádzkovateľa:

Za Dodávateľa:

.....
Mgr. Peter Lukáč, PhD.
generálny riaditeľ
Národné centrum zdravotníckych informácií

.....
.....
.....

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

1. Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre Dodávateľa záväzný a obsahuje najmenej
 - a. určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
 - b. základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré Dodávateľ má zavedené a riadi sa nimi v oblastiach:- organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
 - riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
 - personálna bezpečnosť,
 - riadenie prístupov,
 - riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
 - bezpečnosť pri prevádzke informačných systémov a sietí,
 - hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
 - ochrana proti škodlivému kódu,
 - sieťová a komunikačná bezpečnosť,
 - akvizícia, vývoj a údržba informačných technológií,
 - zaznamenávanie udalostí a monitorovanie,
 - riadenie kontinuity procesov.
 - fyzická bezpečnosť a bezpečnosť prostredia,
 - riešenie kybernetických bezpečnostných incidentov,
 - kryptografické opatrenia,
 - kontinuita prevádzky informačných technológií,
 - audit a kontrolné činnosti.

B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

1. Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Návrh a prijatie bezpečnostných opatrení.
3. Periodické preskúmavanie rizík.
 - a. Identifikácia všetkých významných informačných aktív Dodávateľa a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
 - b. Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
 - c. Vypracovanie a implementácia interného riadiaceho aktu na riadenie bezpečnostných rizík, ktorý obsahuje najmenej:
 - zodpovednosť za vykonanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
 - proces vykonávania analýzy rizík,
 - maticu určenia závažnosti rizika,
 - periodicitu vykonávania analýzy rizík,
 - spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v podľa matice určenia závažnosti rizika.
4. Vykonávanie analýzy rizík najmenej raz za rok.
5. Vytvorenie a udržiavanie zoznamu informačných aktív.

C. Personálna bezpečnosť

1. Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehľbovaním bezpečnostného povedomia.
2. Dodávateľ zabezpečí, 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 verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
3. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
4. Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, 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 verejnej správy,
 - d. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
5. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
6. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.
7. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, najmä:
 - a. pridelovanie 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.
8. Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
9. Zavedenie procesu preukázateľného oboznámenia správcov informačných technológií verejnej správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
10. Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za rok.
11. Na prístup k informačným technológiám verejnej správy sa vyžaduje:
 - a. oboznámenie so spôsobom používania informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy 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 verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy.

D. Riadenie prístupov

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy.
2. Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy.
3. Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok.
4. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.
5. Určenie postupu a zodpovednosti v súvislosti s pridelením prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
6. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
7. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.
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.
9. Zabezpečenie formálneho riadenia a autorizácie pridelenia privilegovaných prístupov do informačných technológií verejnej správy a ich obmedzenie len na nevyhnutné prípady.
10. Preskúvanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok.
11. Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií verejnej správy a na prácu na diaľku.
12. Automatické zaznamenávanie každého prístupu administrátora do informačných technológií verejnej správy a automatické zaznamenávanie prístupu používateľa.
13. Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy.
14. Implementácia centrálnej správy identít (IDM).
15. Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.
16. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúvanie každých šesť mesiacov.
17. Implementácia, vynuovenie prístupových rolí v informačných technológiách verejnej správy.
18. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov.

E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

1. 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. 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 verejnej správy.
3. 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 verejnej správy 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 verejnej správy zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrovania,
 - 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.
4. 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.
 5. 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.
 6. Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti Dodávateľa.
 7. 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.
 8. Pre informačné technológie verejnej správy, 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.
 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 ošetrovaní kybernetickej bezpečnosti a informačnej bezpečnosti v zmluvách so Subdodávateľmi,
 - c. dodávateľských reťazcov informačných technológií verejnej správy,
 - 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.
 10. Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu so Subdodávateľmi.

F. Bezpečnosť pri prevádzke informačných systémov a sietí

1. Na účinnú prevenciu pred stratou dát u Dodávateľa sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru.

2. Dodávateľ vypracuje a dodržiava politiku zálohovania, ktorá definuje požiadavky Prevádzkovateľa na zálohovanie vrátane doby uchovávaní, testovania záloh, ako aj opatrenia na ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.
4. Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.
5. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
6. Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.
7. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnnej pohromy.
8. Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú.
9. Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.
10. Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostných rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.
11. Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.
12. V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.
13. Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:
 - a. operačné systémy,
 - b. virtualizačné prostredia,
 - c. aplikačný softvér,
 - d. pracovné stanice,
 - e. sieťové zariadenia, vrátane bezpečnostných zariadení,
 - f. databázové prostredia.
14. Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.
15. Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

G. Hodnotenie zraniteľností a bezpečnostné aktualizácie

Nastavenie automatickej aktualizácie operačného systému a aplikácií.

1. Dodávateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
2. 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.
3. Vykonávanie hodnotenie zraniteľností najmenej raz ročne.
4. Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií verejnej správy.
5. Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií.

6. Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy.
7. 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.
8. 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.
9. Súbor 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.
10. Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.
11. Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verejnej správy verifikovaný, najmä jeho správna funkcionality.
12. Preskúvanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.
13. Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

H. Ochrana proti škodlivému kódu

1. Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácii škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.
3. Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na
 - a. používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
 - b. škodlivé emailové 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.
4. Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.
5. Zavedenie ochrany informačných technológií verejnej správy 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 verejnej správy,
 - 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.
6. Zavedenie ochrany pred nevyžiadanou elektronickej poštou.
7. Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu.
8. Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov.

9. Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom.

I. Sieťová a komunikačná bezpečnosť

1. Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.
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 zabráňujúcich zneužitiu vzdialeného prístupu.
3. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.
4. Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.
5. Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.
6. Správa počítačových sietí je riadená a kontrolovaná.
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.
8. Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.
9. Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy 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.
10. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.
11. Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.
12. 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.
13. 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.
14. 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 neautorizovanému prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.
15. 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.
16. Vzdialený prístup do vnútornej siete Dodávateľa musí podliehať autentifikácii a autorizácii.
17. Dodávateľ implementuje technológiu detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.
18. Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správca sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
19. Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.

J. Akvizícia, vývoj a údržba informačných technológií verejnej správy

1. Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

2. Pri vytváraní nových alebo úprave existujúcich informačných technológií verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.
3. 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.
4. Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.
5. Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpoveďami, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.
6. Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.
7. Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.
8. Súčasťou akceptačného testovania informačných technológií verejnej správy 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.
9. 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.

K. Zaznamenávanie udalostí a monitorovanie

Zaznamenávanie úspešných a neúspešných autentifikačných udalostí.

1. Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy.
2. Pre každý prvok informačných technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované.
3. 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.

4. 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, cieľový port.
5. Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.
6. Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.
7. Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.
8. Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja.
9. Dodávateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy.
10. Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
11. Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.
12. Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.
13. Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.
14. 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.
15. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

L. Fyzická bezpečnosť a bezpečnosť prostredia

1. Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.
2. Umiestnenie informačných technológií verejnej správy 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.
3. Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.
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.
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 verejnej správy a zariadení informačných technológií verejnej správy,
 - b. používania zariadení informačných technológií verejnej správy na iné účely, než na aké sú pôvodne určené,

- c. používania zariadení informačných technológií verejnej správy mimo určených priestorov,
 - d. vymazávania, vyradovania a likvidovania zariadení informačných technológií verejnej správy a všetkých typov relevantných záloh,
 - e. prenosu technických komponentov informačných technológií verejnej správy alebo zariadení informačných technológií verejnej správy mimo priestorov orgánu riadenia,
 - f. narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií verejnej správy tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.
6. Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.
 7. Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.
 8. Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

M. Riešenie kybernetických bezpečnostných incidentov

1. Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe.
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.
3. Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.
4. S interným riadiacim aktom, najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámi všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy.
5. Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto.
6. Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.
7. Proces odborného posúdenia a analýzy oznámení realizuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT.
8. Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.
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.
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.

11. Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
12. Dodávateľ má vytvorené plány na riešenie kybernetických bezpečnostných incidentov.

N. Kryptografické opatrenia

Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS

1. Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
2. Pri informačných technológiách verejnej správy 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. emailovej komunikácie prostredníctvom PGP alebo S/MIME,
 - d. komunikačných kanálov na výmenu nešifrovaných dát,
 - e. centrálnych úložísk,
 - f. záloh.
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.
4. Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.
5. Dodávateľ pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.

O. Kontinuita prevádzky informačných technológií verejnej správy

1. Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.
2. Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácii s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.
3. Plán kontinuity prevádzky obsahuje najmä:
 - a. roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
 - b. možné vplyvy na prevádzku informačných technológií verejnej správy,
 - 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.
4. Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.

P. Audit a kontrolné činnosti

1. Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa tejto Zmluvy.
2. Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy.
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.
4. Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.
5. Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijímú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravujú sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.

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	Email
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	Email
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		