Obec [●][[1]](#footnote-1)

**Politika kybernetickej bezpečnosti a informačnej bezpečnosti**

**Interný riadiaci akt č. [●]**

Obec [●] podľa ustanovení pre Kategóriu I Časti A., písm. b) Prílohy č. 2 k Vyhláške 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* (ďalej len „**vyhláška**“) ustanovuje:

**Čl. 1  
Základné ustanovenia**

1. Tento interný riadiaci akt:
   1. určuje povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti (ďalej len „**kybernetická bezpečnosť**“) pre obec [●] (ďalej len „**správca**“);
   2. stanovuje základné zásady a opatrenia kybernetickej bezpečnosti správcu.
2. Tento interný riadiaci akt je pre správcu záväzný.

**Čl. 2  
Organizácia kybernetickej bezpečnosti**

1. Za koordináciu kybernetickej bezpečnosti informačných systémov správcu je zodpovedný určený pracovník správcu (ďalej len „**koordinátor kybernetickej bezpečnosti**“). Funkciu koordinátora kybernetickej bezpečnosti správcu plní [*uvedenie pozície a kontaktných údajov v rozsahu e-mail, telefónne číslo*].

[pozn.: Uveďte názov pozície, súčasťou ktorej je v rámci obce aj funkcia *koordinátora kybernetickej bezpečnosti* v zmysle tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti;

- alternatívne -

opisným spôsobom uveďte osobu, ktorá je v rámci obce zodpovedná za výkon funkcie *koordinátora kybernetickej bezpečnosti*, ak sa nejedná o zamestnanca obce (napr. spôsobilý zamestnanec externého dodávateľa výpočtovej techniky/ software atď.)]

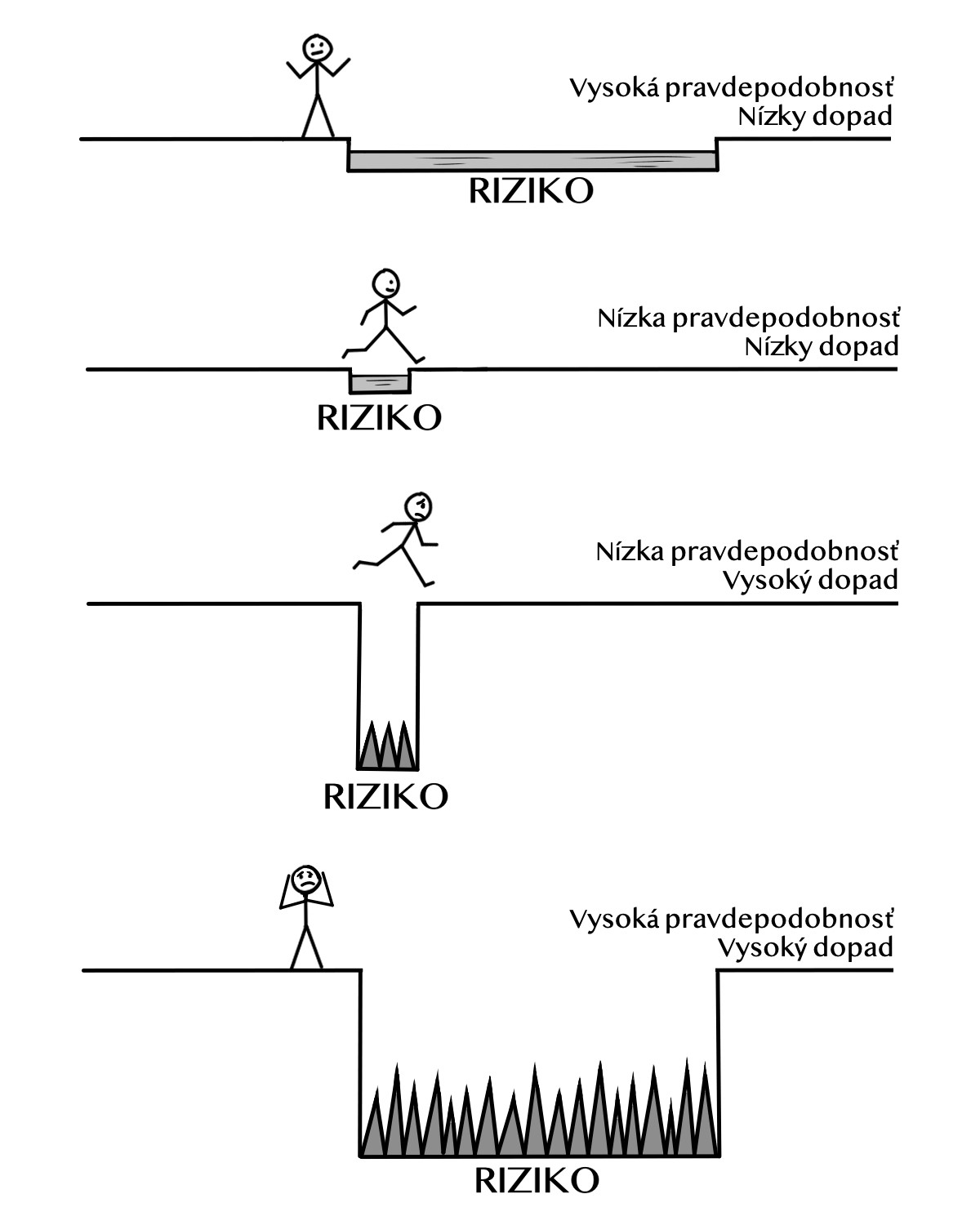
1. Koordinátor kybernetickej bezpečnosti v rámci svojho pôsobenia:
   1. vypracúva analýzu rizík kybernetickej bezpečnosti a navrhuje opatrenia na ich minimalizáciu,
   2. podieľa sa na prijímaní bezpečnostných opatrení kybernetickej bezpečnosti,
   3. analyzuje a riadi riziká kybernetickej bezpečnosti,
   4. pripravuje plán školení kybernetickej bezpečnosti najmenej každé tri roky,
   5. sa podieľa na výbere, nákupe, implementácii, prevádzke a vyraďovaní informačných technológií správcu,
   6. prijíma hlásenia o bezpečnostných incidentoch a ďalej ich nahlasuje Vládnej jednotke CSIRT[[2]](#footnote-2).

[alternatívne pre subjekty, ktoré sú prevádzkovateľmi základných služieb:

*„f) prijíma hlásenia o bezpečnostných incidentoch a ďalej ich nahlasuje prostredníctvom Jednotného informačného systému kybernetickej bezpečnosti*“]

**Čl. 3  
Riadenie rizík kybernetickej bezpečnosti**

1. Scenárom rizika kybernetickej bezpečnosti sa rozumie akýkoľvek súhrn udalostí, ktoré môžu nastať s určitou pravdepodobnosťou a spôsobiť negatívny dopad, ktorým je poškodenie informačných technológií alebo iných aktív správcu. Preskúmaním a identifikáciou rizika a prijatím vhodných bezpečnostných opatrení sa pravdepodobnosť naplnenia scenáru rizika minimalizuje.
2. Za účelom identifikácie rizík, určenia opatrení na ich minimalizáciu a riadenia rizík správca každoročne vykonáva analýzu rizík kybernetickej bezpečnosti.
3. Pri analýze rizík je potrebné zohľadniť pravdepodobnosť naplnenia scenára rizika a potenciálny negatívny dopad pri jeho naplnení. V obrázku nižšie je pre jednoduché vysvetlenie zobrazená súvislosť rizika, pravdepodobnosti a dopadu:



1. Pre všetky identifikované riziká koordinátor kybernetickej bezpečnosti deklaruje konkrétny spôsob riešenia (prijatia konkrétneho opatrenia alebo viacerých opatrení), ktorým je akceptácia rizika, obídenie rizika, prenesenie rizika, redukcia rizika alebo kombinácia viacerých z týchto spôsobov.
2. Akceptáciou rizika sa rozumie rozhodnutie prijať následky potenciálnej realizácie rizika,
3. obídením rizika sa rozumie rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy (napríklad riziko zatopenia servera môže byť obídené umiestnením servera na vyššom nadzemnom podlaží),
4. prenesením rizika sa rozumie rozhodnutie preniesť následky realizácie rizika mimo organizácie správcu, napríklad uzavretím poistnej zmluvy,
5. redukciou rizika sa rozumie rozhodnutie pomocou vhodných opatrení dosiahnuť zníženie následkov realizácie rizika alebo zníženie pravdepodobnosti jeho realizácie.

**Čl. 4  
Personálna bezpečnosť**

1. Dôležitou súčasťou personálnej bezpečnosti je zvyšovanie, rozvoj a udržiavanie bezpečnostného povedomia prostredníctvom návrhu a realizácie plánu rozvoja bezpečnostného povedomia a vzdelávania.
2. Udržiavanie bezpečnostného povedomia spočíva najmä v oboznámení používateľov, administrátorov a dodávateľov s bezpečnostnými zásadami kybernetickej bezpečnosti správcu a v pravidelnom zvyšovaní ich bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu.
3. Zvyšovanie bezpečnostného povedomia zamestnancov formou školení, inštruktáží, účasti na odborných podujatiach a pod. sa vykonáva priebežne a kontinuálne. Súčasťou praktických školení je aj vysvetlenie zodpovednosti používateľov, upozornenie na bezpečnostné riziká a popis spôsobu nahlasovania bezpečnostných incidentov.
4. Koordinátor kybernetickej bezpečnosti ustanoví plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a zabezpečí bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky.
5. Hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia vykonáva koordinátor kybernetickej bezpečnosti priebežne, pričom berie do úvahy najmä počty nahlásených a úspešne vyriešených bezpečnostných incidentov.
6. Správca aj tretia strana (dodávateľ) zabezpečia, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, s ktorými budú v rámci plnenia úloh pre správcu oboznámení, a to predtým, ako získajú prístup k informačným technológiám správcu. Povinnosť mlčanlivosť je všeobecná a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
7. Každý pracovník správcu je povinný všetky zistené bezpečnostné incidenty bezodkladne oznámiť koordinátorovi kybernetickej bezpečnosti.
8. Pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca správcu a pri ukončení spolupráce správcu s externým pracovníkom alebo treťou stranou (ďalej len „**bývalý pracovník**“) koordinátor kybernetickej bezpečnosti zabezpečí:
   1. vrátenie všetkých zariadení pridelených bývalému pracovníkovi, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
   2. zablokovanie prístupu v zariadeniach pridelených bývalému pracovníkovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
   3. zrušenie prístupových práv bývalého pracovníka v informačných systémoch verejnej správy, ktoré správca prevádzkuje, alebo ku ktorým môže svojim zamestnancom a dodávateľom zabezpečiť zriadenie prístupu,
   4. odovzdanie výsledkov práce bývalého pracovníka (napríklad programy vrátane dokumentácie, vlastné elektronické dokumenty) a prevedenie prístupových oprávnení na poverenú osobu v súčinnosti s koordinátorom kybernetickej bezpečnosti.
9. Koordinátor kybernetickej bezpečnosti priebežne monitoruje personálne zmeny u správcu a zmeny v dodávateľských vzťahoch. Pri zmene postavenia používateľov, administrátorov alebo zamestnancov dodávateľa zabezpečení zmeny prístupových oprávnení.
10. V prípade porušenia interných predpisov správcu alebo platných právnych predpisov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti zamestnancom správcu alebo dodávateľa sa môže uplatniť disciplinárny proces alebo ďalšie sankcie (v závislosti od typu porušenia).

**Čl. 5  
Riadenie prístupov**

1. Vo všetkých situáciách, kedy je vyžadovaná identifikácia používateľa, je potrebné v prostredí správcu prezentovanú identitu overiť procesom autentifikácie. Pri autentifikácii sa overujú niektoré z nasledovných faktorov alebo ich kombinácia:
   1. heslo alebo PIN,
   2. hardwarové prístupové zariadenia - napríklad čipová karta s certifikátom, USB kľúč, SIM karta,
   3. biometrické overenie identity používateľa - napríklad odtlačok prsta.
2. Každý používateľ musí mať v informačnom systéme správcu vytvorený vlastný používateľský účet, voči ktorému sa identifikuje a autentifikuje pri vstupe. Zdieľané a skupinové účty nie sú povolené.
3. V prostredí informačných systémov správcu sa v rámci riadenia prístupov k informačným technológiám verejnej správy a ich službám:
4. každému používateľovi informačného systému prideľuje jednoznačný identifikátor na vstup do informačného systému,
5. zabezpečuje riadenie jednoznačných identifikátorov vrátane prístupových oprávnení,
6. využívajú nástroje na správu autentifikačných a autorizačných mechanizmov na overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému,
7. v pravidelných intervaloch vykonáva kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov.
8. Používateľské heslá a autentifikačné prostriedky do informačných technológií verejnej správy je zakázané zdieľať, osoba ktorej boli pridelené, má výhradné právo na ich použitie.
9. Dĺžka nového hesla používateľských účtov musí byť minimálne:
10. 12 znakov v prípade bežného používateľa informačného systému,
11. 15 znakov v prípade správcu informačného systému.
12. Nové používateľské heslo musí obsahovať:
13. malé písmeno abecedy,
14. veľké písmeno abecedy a
15. číslicu a špeciálny znak.
16. Nové používateľské heslo nesmie obsahovať:
17. ľahko uhádnuteľné slová, ako napríklad „heslo“, „password“, „Slovensko“ a podobne,
18. slová odvodené z prihlasovacieho mena,
19. slová alebo čísla odvodené z pracovnej pozície alebo iných všeobecne známych údajov o užívateľovi (napríklad dátum narodenia, meno domáceho zvieraťa, meno rodinného príslušníka a pod.).
20. Vhodné, ľahko zapamätateľné a ťažko prelomiteľné používateľské heslo sa odporúča tvoriť aj formou ľahko zapamätateľnej ale dostatočne dlhej frázy (napríklad  
    *NajtazsieHesloMaAspon12Znakov!*)[[3]](#footnote-3).
21. Používateľské heslo sa musí zmeniť najneskôr:
22. po 1 roku v prípade používateľských hesiel,
23. po 180 dňoch v prípade hesiel pre správcov informačných systémov,
24. okamžite v prípade bezpečnostne významnej udalosti (napríklad kompromitácia hesla).
25. V prípade využívania autentifikačných prostriedkov ako napríklad čipová karta s certifikátom, USB kľúč či pridelená SIM karta na prístup z mobilných zariadení sa postupuje podľa postupov definovaných v dokumentácii k príslušnému informačnému systému.
26. V prípade využívania biometrických vlastností na účely autentifikácie musí byť tento spôsob v súlade s legislatívnymi požiadavkami osobitných predpisov[[4]](#footnote-4) a schválený koordinátorom kybernetickej bezpečnosti.
27. Koordinátor kybernetickej bezpečnosti je zodpovedný za nastavenie riadenia prístupov používateľov do informačných systémov a za prideľovanie a odoberanie prístupových oprávnení používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov.

**Čl. 6  
Riadenie kybernetickej bezpečnosti vo vzťahoch s tretími stranami**

1. Všetky zmluvy uzatvorené medzi správcom a dodávateľmi musia obsahovať záväzok dodávateľa dodržiavať všetky interné riadiace dokumenty správcu v oblasti kybernetickej bezpečnosti a všeobecne záväzné predpisy v oblasti kybernetickej bezpečnosti.
2. Prístup tretích strán ako aj ich vzdialený prístup musí byť riadený, kontrolovaný a prístupové oprávnenia musia byť udelené len v minimálnom rozsahu potrebnom na vykonávanie pracovných činností.
3. Pred udelením prístupu tretej strany k informačným aktívam správcu musia byť vždy definované bezpečnostné požiadavky na tretie strany, ktoré tretia strana dodržiava za účelom ochrany týchto informačných aktív.
4. Dohodnuté zmluvné podmienky musia vyžadovať aj umožnenie výkonu kontroly dodržiavania stanovených podmienok treťou stranou zo strany správcu.
5. Tretia strana a jej zamestnanci musia byť poučení koordinátorom kybernetickej bezpečnosti o bezpečnostných požiadavkách, ktoré sú kladené na používateľov zo strany správcu, vrátane spôsobov identifikácie, nahlasovania a riešenia bezpečnostných incidentov.
6. Na komunikáciu alebo výmenu údajov s tretími stranami sa na základe analýzy rizík používajú kryptografické prostriedky podľa čl. 14.

**Čl. 7  
Bezpečnosť pri prevádzke informačných systémov a sietí**

1. Postupy pri prevádzke informačných systémov musia zohľadniť výsledky analýzy rizík kybernetickej bezpečnosti vykonanej podľa čl. 3 a musia byť riadne zadokumentované.
2. Súčasťou prevádzkových postupov informačných technológií verejnej správy a dokumentácie k nim je najmä:
   1. popis správy používateľov (kto a ako ju vykonáva),
   2. vysvetlenie spôsobu konfigurácie aplikácií a informačných technológií verejnej správy, ktoré správca využíva,
   3. popisy konfigurácie (vrátane bezpečnostných nastavení) a zapojenia informačných technológií verejnej správy,
   4. zoznam kontaktných osôb v prípade výskytu neočakávaných udalostí,
   5. popis procesu zálohovania údajov,
   6. popis pravidelne vykonávaných činností údržby informačných technológií verejnej správy,
   7. plán výkonu servisu a kontakty na servisných partnerov.
3. Na účinnú prevenciu pred stratou dát sa zavádza nasledovný proces na vytváranie záložných kópií dôležitých informácií a softvéru:

[KONKRÉTNE POPÍSAŤ, AKO FUNGUJE ZÁLOHOVANIE, AKÉ ÚDAJE SA ZÁLOHUJÚ, KDE SÚ UMIESTNENÉ MÉDIA SO ZÁLOHAMI, KTO K NIM MÁ PRÍSTUP, AKÁ JE DOBA UCHOVÁVANIA ÚDAJOV, AKO ČASTO SA TESTUJE FUNKČNOSŤ MÉDIÍ.]

1. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií musia byť uložené v zabezpečenom uzamykateľnom priestore.

**Čl. 8  
Hodnotenie zraniteľností a bezpečnostné aktualizácie**

1. Bezpečnostné aktualizácie operačných systémov sa vykonávajú pravidelne. Koordinátor kybernetickej bezpečnosti zaistí nastavenie automatickej aktualizácie operačného systému a aplikácií, pokiaľ je to technicky možné.
2. Hodnotenie zraniteľností sa vykonáva v kontexte spracovania analýzy rizík.
3. Všetky zistené kritické technické zraniteľnosti musia byť odstránené v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie alebo ich výrobcom.

**Čl. 9  
Ochrana proti škodlivému kódu**

1. Používanie informačných technológií správcu na sťahovanie, inštaláciu a používanie nelegálneho alebo škodlivého softvéru je zakázané.
2. Činnosti súvisiace s prevenciou a detekciou škodlivého kódu sú v prostredí správcu realizované na pravidelnej báze a zamerané najmä na:
   1. detekciu prítomnosti škodlivého kódu na všetkých používaných informačných zariadeniach a prvkoch informačných technológií verejnej správy,
   2. používanie prenosných médií (napr. USB kľúče, flash disky, CD, DVD a pod.),
   3. kontrolu prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
   4. rozpoznanie podozrivých a škodlivých webových stránok a odkazov,
   5. externú a internú sieťovú komunikáciu vrátane webových sídiel,
   6. kontrolu súborov prijímaných zo siete internet a odosielaných do siete internet,
   7. detekciu prítomnosti škodlivého kódu na všetkých webových sídlach.
3. Pri inštalácii systémov na ochranu pred škodlivým kódom na serveroch je nutné brať do úvahy odporúčania výrobcov a zohľadniť možné konflikty so softvérom prevádzkovaným na serveroch.
4. Inštaláciu a konfiguráciu systémov na ochranu proti škodlivému kódu môžu realizovať len administrátori, ktorým to vyplýva z pracovnej náplne, alebo osoby, ktoré boli touto činnosťou poverené po odsúhlasení koordinátorom kybernetickej bezpečnosti.
5. Na prenos súborov z externých sietí musí byť stanovený postup, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu (napríklad automatická kontrola antivírusovým nástrojom)

**Čl. 10  
Sieťová a komunikačná bezpečnosť**

1. Všetky koncové stanice správcu musia byť chránené prostredníctvom softvérového personálneho firewallu.
2. Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:
   1. pravidelná aktualizácia firmvéru,
   2. zmena továrensky nastavených autentifikačných údajov,
   3. pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
   4. vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.
3. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.
4. Použité zariadenia (napríklad komunikačné smerovače alebo routery a prepínače) je nutné zabezpečiť proti neautorizovanej zmene ich konfigurácie. Každé použité zariadenie sa konfiguruje podľa konfiguračného štandardu, ktorý popisuje jeho bezpečnú konfiguráciu.
5. Zapájanie ľubovoľných zariadení do počítačových sietí a ostatnej komunikačnej infraštruktúry vykonávajú iba oprávnené osoby so súhlasom koordinátora KIB a tretia strana na základe zmluvného vzťahu. Zmeny v komunikačnej infraštruktúre a jej prepojenia s externými sieťami schvaľuje koordinátor kybernetickej bezpečnosti, ich vykonanie musí byť zdokumentované.

**Čl. 11  
Akvizícia, vývoj a údržba informačných technológií verejnej správy**

1. Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy správca zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Pred nákupom informačných technológií verejnej správy správca stanoví základné bezpečnostné požiadavky (napríklad softvér musí byť legálny a zakúpený z dôveryhodného zdroja, musí mať zabudované mechanizmy autentifikácie, musí byť k nemu dodaná aktuálna administrátorská a prevádzková dokumentácia a pod. podľa špecifických požiadaviek správcu v úzkej spolupráci s koordinátorom kybernetickej bezpečnosti).
3. V prípade, že to je možné, obsahuje zmluva s dodávateľom záväzok dodávateľa dodržiavať stanovené bezpečnostné požiadavky správcu.

**Čl. 12  
Zaznamenávanie udalostí a monitorovanie**

1. Správca vykonáva:
   1. zaznamenávanie úspešných a neúspešných autentifikačných udalostí (prihlásení do systémov, aplikácií a zariadení),
   2. monitorovanie hlásení bezpečnostného softvéru (firewall, antivírus, atď.),
   3. priebežnú kontrolu dôležitých konfiguračných nastavení zariadení a systémov (napríklad zakázané wifi na notebookoch, ak sa nevyužíva),
   4. priebežnú kontrolu stavu zaplnenia diskových kapacít (napríklad voľné miesto na systémovom disku),
   5. monitorovanie neštandardných udalostí súvisiacich s pripojením na Internet (napríklad opakované bezdôvodné spomalenie).
2. Prípade potreby asistencie s monitorovaním a jeho výsledkami kontaktuje správca   
   jednotku CSIRT[[5]](#footnote-5).

**Čl. 13  
Fyzická bezpečnosť a bezpečnosť prostredia**

1. Správca umiestňuje a prevádzkuje zariadenia takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

**Čl. 14  
Riešenie kybernetických bezpečnostných incidentov**

1. Správca je povinný zistené kybernetické bezpečnostné incidenty bezodkladne nahlásiť orgánu riadenia, ktorým je Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky. Za účelom nahladovania kybernetických bezpečnostných incidentov sa v rámci organizácie správcu určuje jeden centrálny kontaktný bod, ktorým je [●] – opísať kontaktné miesto.

**Čl. 15  
Kryptografické opatrenia**

1. Správca využíva iba štandardizované kryptografické nástroje, funkcie a algoritmy (napríklad šifrovanie, hash, elektronický podpis). V prípade potreby a ak nie je možné technické otázky v súvislosti s ich nasadením uspokojivo vyriešiť na úrovni správcu, je koordinátor kybernetickej bezpečnosti oprávnený tieto otázky konzultovať s jednotkou CSIRT. Každé miesto nasadenia a spôsobu využívania kryptografickej funkcie musí byť zdokumentované a evidované (napríklad šifrované disky, šifrované e-maily a pod.)
2. Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS.

**Čl. 16  
Audit a kontrolné činnosti**

1. Kontrolné činnosti vykonáva koordinátor kybernetickej bezpečnosti priebežne, zameriava sa najmä na:
   1. stav opatrení prijatých na základe výsledkov analýzy rizík v zmysle čl.3,
   2. stav dodržiavania opatrení prijatých a vykonávaných na základe ustanovení tejto bezpečnostnej politiky a zákona o informačných technológiách vo verejnej správe.
2. Audit kybernetickej bezpečnosti vykonáva správca prostredníctvom samo-posúdenia. Samo-posúdenie môže vykonať koordinátor kybernetickej bezpečnosti alebo ním poverený špecialista spolupracujúci so správcom na základe pracovnoprávneho alebo iného zmluvného vzťahu.

V [●], [●].2021

|  |  |  |
| --- | --- | --- |
|  |  | **[***meno štatutárneho zástupcu obce***]**  **[***funkcia***]** |

1. Tento vzor obsahuje minimálne bezpečnostné opatrenia pre **Kategóriu I** v zmysle ustanovenia § 3, ods. 2 Vyhlášky 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. Znak [●] v žltom poli alebo text v žltom poli znamená, že organizácia si na toto miesto doplní relevantné údaje. [↑](#footnote-ref-1)
2. <https://www.csirt.gov.sk/hlasenia/nahlasenie-incidentu-861.html> [↑](#footnote-ref-2)
3. Toto je len príklad, toto konkrétne heslo nepoužívajte [↑](#footnote-ref-3)
4. Napríklad Nariadenie 2016/679 *o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)* (GDPR) alebo zákon č. 18/2018 Z.z. *o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* v znení neskorších predpisov. [↑](#footnote-ref-4)
5. <https://www.csirt.gov.sk/kontakty-7db.html> [↑](#footnote-ref-5)