V Y H L Á ŠK AÚradu podpredsedu vlády SR pre investície a informatizáciu

z dd. mesiac 2019,
ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Úrad podpredsedu vlády SR pre investície a informatizáciu podľa § 31 písm. a) a i) zákona č. 95/2019 Z. z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1Základné ustanovenia

1. Táto vyhláška upravuje jednotlivé kategórie informačných technológií verejnej správy (ďalej len „ITVS“) a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu[[1]](#footnote-1) na účely podľa § 11 ods. 4 zákona.
2. Táto vyhláška upravuje podrobnosti o bezpečnosti ITVS podľa § 18 až 23 zákona, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsahu bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov.
3. Správca vo vzťahu k ITVS v jeho pôsobnosti identifikuje a udržiava zoznam svojich aktív podľa prílohy č. 1, identifikuje časti aktív, ktorých nedostupnosť alebo znížená kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb.
4. Správca vo vzťahu k ITVS v jeho pôsobnosti realizuje minimálne bezpečnostné opatrenia príslušnej kategórie.
5. Orgán vedenia pre potreby implementácie požiadaviek zákona a tejto vyhlášky poskytne správcovi súbor materiálov, ktorý bude obsahovať šablóny a vzory dokumentácie bezpečnosti ITVS, návody, školiace materiály a ukážky.

§2

Bezpečnostné opatrenia

1. Bezpečnostné opatrenia tvoria minimálne bezpečnostné opatrenia troch úrovní.
2. V prípade rozporu minimálnych bezpečnostných opatrení rôznych úrovní, ktoré majú byť aplikované na konkrétne ITVS, majú prednosť ustanovenia opatrenia vyššej úrovne.
3. V prípade ak má správca aplikovať bezpečnostné opatrenia aj podľa osobitného predpisu[[2]](#footnote-2), aplikuje bezpečnostné opatrenia podľa zákona, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa osobitného predpisu.[[3]](#footnote-3)
4. Správca vypracuje a implementuje bezpečnostný projekt pre informačný systém verejnej správy (ďalej len „ISVS“) v jeho správe v rozsahu podľa prílohy č. 2.

§3

Minimálne bezpečnostné opatrenia

1. Minimálne bezpečnostné opatrenia sú upravené v prílohe č. 3 a sú rozdelené do Kategórie I, Kategórie II a Kategórie III v rámci rôznych oblastí kybernetickej a informačnej bezpečnosti (ďalej len „KIB“).
2. Minimálne bezpečnostné opatrenia z Kategórie I jednotlivých oblastí KIB vo vzťahu k ITVS, ktorých je správcom zavedie najmä:
	1. obec do 6000 obyvateľov,
	2. obec so štatútom mesta do 6000 obyvateľov,
	3. právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v § 5 ods. 2 písmenách a) až d) zákona iná, ako sú vymenované v ods. 3 a ods. 4 tejto vyhlášky,
	4. osoba neuvedená v § 5 ods. 2 v písmenách a) až f) zákona, okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitného predpisu.
3. Minimálne bezpečnostné opatrenia z Kategórie I a Kategórie II jednotlivých oblastí KIB vo vzťahu k ITVS, ktorých je správcom zavedie najmä:
4. obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,[[4]](#footnote-4)
5. mestská časť s vlastnou právnou subjektivitou,[[5]](#footnote-5)
6. Úrad pre Slovákov žijúcich v zahraničí,
7. komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,
8. Kancelária verejného ochrancu práv,
9. Úrad komisára pre deti,
10. Úrad komisára pre osoby so zdravotným postihnutím,
11. Rada pre vysielanie a retransmisiu.
12. Minimálne bezpečnostné opatrenia z Kategórie I, Kategórie II a Kategórie III jednotlivých oblastí KIB vo vzťahu k ITVS, ktorých je správcom zavedie najmä:
13. obec so štatútom mesta nad 6000 obyvateľov, ktorá je aj krajským mestom,[[6]](#footnote-6)
14. samosprávny kraj,
15. ministerstvo a ostatný ústredný orgán štátnej správy,[[7]](#footnote-7)
16. Úrad pre reguláciu sieťových odvetví,
17. Úrad pre reguláciu elektronických komunikácií a poštových služieb,
18. Najvyšší kontrolný úrad Slovenskej republiky,
19. Úrad pre dohľad nad zdravotnou starostlivosťou,
20. Úrad na ochranu osobných údajov Slovenskej republiky,
21. Generálna prokuratúra Slovenskej republiky,
22. Dopravný úrad,
23. Ústav pamäti národa,
24. Tlačová agentúra Slovenskej republiky,
25. Rozhlas a televízia Slovenska,
26. Kancelária Súdnej rady Slovenskej republiky,
27. Kancelária Najvyššieho súdu Slovenskej republiky,
28. Kancelária Ústavného súdu Slovenskej republiky,
29. Kancelária prezidenta Slovenskej republiky,
30. Národná rada Slovenskej republiky,
31. Finančné riaditeľstvo Slovenskej republiky,
32. Národná agentúra pre sieťové a elektronické služby,
33. Zbor väzenskej a justičnej stráže,
34. DataCentrum Ministerstva financií Slovenskej republiky,
35. DataCentrum elektronizácie územnej samosprávy Slovenska,
36. Sociálna poisťovňa,
37. Zdravotné poisťovne.
38. Orgán vedenia môže určiť minimálne bezpečnostné opatrenia konkrétnej úrovne vo vzťahu k ITVS, ktorých je správcom iný štátny orgán, ktorý nie je uvedený v odsekoch 2, 3 a 4.

§4

Záverečné a prechodné ustanovenia

1. Akékoľvek výnimky z implementácie bezpečnostných opatrení sú správcom zdokumentované, odôvodnené, schválené štatutárom a zaslané orgánu vedenia na schválenie.
2. Správca existujúci ku dňu účinnosti tejto vyhlášky je povinný plniť povinnosti vyplývajúce z tejto vyhlášky do dvoch rokov odo dňa nadobudnutia účinnosti tejto vyhlášky.
3. Správca zriadený po nadobudnutí účinnosti tejto vyhlášky je povinný plniť povinnosti vyplývajúce z tejto vyhlášky do dvanástich mesiacov odo dňa jeho zriadenia.

**Príloha č. 1**

**k vyhláške č. xx/2019 Z. z.**

ZOZNAM AKTÍV

Zoznam aktív obsahuje označenie operačného systému alebo firemného softvéru (firmware) a jeho aktuálne používanej verzie na všetkých nasledovných komponentoch ITVS:

1. pracovná stanica,
2. ~~komerčný~~ aplikačný software,
	* kancelársky software (MS Office, Acrobat Reader a pod.),
	* internetový prehliadač,
	* antivírusový software,
	* komunikačný software,
	* ďalší využívaný ~~komerčný~~ software.
3. server,
4. virtualizačné prostredie,
5. databázové prostredie,
6. emailový server,
7. webový server,
8. ~~komerčný~~ podnikový software (napr. ERP systém SAP a pod.),
9. sieťový firewall,
10. sieťový router,
11. sieťový prepínač (switch),
12. komunikačné prostredie (VoIP a pod.),
13. zálohovacie prostredie,
14. mobilné zariadenia (smartfóny, tablety).

 Doplniť aktíva ? (priestor, infraštruktúra, tlačové služby)

Kategórie, nie explicitne vymenovanie ???

**Príloha č. 2**

**k vyhláške č. xx/2019 Z. z.**

**OBSAH A ŠTRUKTÚRA BEZPEČNOSTNÉHO PROJEKTU ISVS**

1. Pri spracovaní bezpečnostného projektu ISVS sa prihliada najmä na zložitosti ISVS, komplexnosti agendy pokrytej ISVS a stanoveným bezpečnostným požiadavkám na ISVS. Zohľadniť sa musí taktiež kategória, do ktorej je ISVS zaradený (s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov).
2. Bezpečnostný projekt ISVS pozostáva z dvoch hlavných výstupov (bezpečnostného zámeru a analýzy bezpečnosti). Jednotlivé výstupy musia vzniknúť v stanovenom poradí a sú vypracované priebežne počas celého projektu ISVS realizovaného v súlade s vyhláškou č. xx/2019 Z. z. o riadení projektov.
3. Ako prvý výstup bezpečnostného projektu ISVS musí byť vytvorený dokument *bezpečnostný zámer*. Bezpečnostný zámer musí byť zo strany orgánu riadenia formálne predložený orgánu vedenia, jeho vytvorenie je potrebné zabezpečiť najneskôr po vytvorení technickej špecifikácie a detailného návrhu riešenia. Bezpečnostný zámer stanovuje najmä kontext a zameranie bezpečnostného projektu, musí preto obsahovať minimálne:
4. formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,
5. zoznam právnych predpisov aplikovaných v bezpečnostnom projekte ako aj interných predpisov,
6. vysvetlenie metodického prístupu ku kvalitatívnej analýze rizík, ktorá bude v bezpečnostnom projekte vykonaná,
7. rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany ISVS, jeho služieb a údajov v ňom spracúvaných,
8. vymedzenie okolia ISVS a jeho vzťah k možnému narušeniu bezpečnosti ISVS vrátane zoznamu integrácií na ISVS,
9. vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
10. ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu ISVS),
11. postupy revízie/aktualizácie bezpečnostného zámeru.
12. Ako hlavný výstup bezpečnostného projektu ISVS musí vzniknúť dokument *analýza bezpečnosti,* ktorého súčasťou je kvalitatívna *analýza rizík.* Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami. Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív ISVS a jeho okolia. Analýza rizík musí byť pre ISVS vykonávaná priebežne počas celého projektu (viď vyhláška č. xx/2019 Z. z. o riadení projektov) a priamo nadväzuje na dokument bezpečnostný zámer. Analýza rizík pozostáva z výkonu nasledovných činností:
13. vytvorenie podkladových katalógov pre analyzované riziká, slúžiacich na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu dopadov,
14. identifikácia a popis analyzovaných rizík v štruktúre podľa oblastí stanovených osobitným predpisom[[8]](#footnote-8) alebo normou[[9]](#footnote-9),
15. priradenie aktív, hrozieb, zraniteľností a dopadov ku každému z identifikovaných rizík,
16. identifikácia realizovaných bezpečnostných opatrení,
17. vyhodnotenie rizík spôsobom kombinácie pravdepodobnosti realizácie scenáru rizika a závažnosti dopadu,
18. popis navrhovaných bezpečnostných opatrení.
19. Pri každom riziku sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny dopad na aktíva orgánu riadenia. Pri hodnotení závažnosti výsledného dopadu sa zohľadňuje celková závažnosť dopadov, ktoré by boli spôsobené v prípade realizácie rizika. Úroveň dopadov sa určuje zvlášť pre každé analyzované riziko a zahŕňa všetky aktíva dotknuté príslušným rizikom. Analyzované riziko môže mať na aktíva orgánu riadenia viaceré dopady, ktoré je potrebné sumárne vyhodnotiť a zdokumentovať. Výsledná miera rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.
20. Metodický postup výkonu analýzy rizík musí byť v súlade s technickou normou.[[10]](#footnote-10) Výsledné vyhodnotenie rizík podľa použitej metodiky musí byť premietnuté do trojstupňovej stupnice nízke riziko, stredné riziko, vysoké riziko.
21. Pri tvorbe navrhovaných bezpečnostných opatrení je potrebné popísať prostriedky a procesy odstraňovania nedostatkov zistených v rámci jednotlivých rizík. Cieľom návrhu bezpečnostných opatrení je vytvorenie takého okruhu bezpečnostných opatrení, aby po ich potenciálnej implementácii a následnom prehodnotení rizík boli všetky zvyškové riziká akceptovateľné. Pri niektorých typoch opatrení je prípustné sa odkazovať aj na dokumentáciu k ISVS (viď vyhláška č. xx/2019 Z. z. o riadení projektov). Popis navrhovaných bezpečnostných opatrení zohľadňuje:
22. opatrenia stanovené touto vyhláškou alebo osobitným predpisom,[[11]](#footnote-11)
23. požiadavky vyplývajúce z aplikovateľnej legislatívy,
24. náležitosti implementácie a prevádzky analyzovaného ISVS a spôsob uplatňovania bezpečnostných opatrení v konkrétnych podmienkach orgánu riadenia,
25. opatrenia realizovateľné v pôsobnosti analyzovaného ISVS, ale aj opatrenia vo vzťahu k jeho okoliu,
26. dostupné možnosti prístupu k riadeniu rizika (redukcia, prenesenie, obídenie),
27. spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení.
28. Výstupný dokument analýzy bezpečnosti s výsledkami analýzy rizík obsahuje najmä:
29. ciele a priority analýzy rizík,
30. opis použitej metodiky analýzy rizík,
31. opis rizík založený na identifikácii aktív, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností a na identifikácii dopadov na aktíva najmä v dôsledku straty dôvernosti, integrity a dostupnosti,
32. vyhodnotenie rizík podľa použitej metodiky,
33. popis navrhovaných bezpečnostných opatrení pre identifikované riziká v závislosti od ich závažnosti,
34. celkové zhrnutie výsledkov analýzy rizík, vrátane prioritizovaného zoznamu vysokých a stredných rizík s popisom navrhovaného postupu ich riadenia a kľúčových navrhovaných bezpečnostných opatrení,
35. postupy revízie/aktualizácie analýzy bezpečnosti.
36. Štruktúra výstupu analýzy bezpečnosti musí zodpovedať oblastiam stanoveným osobitným predpisom[[12]](#footnote-12) alebo normou[[13]](#footnote-13). Finalizácia dokumentácie bezpečnostného projektu ISVS musí byť realizovaná v etape IMPLEMENTÁCIA A TESTOVANIE (vyhláška č. xx/2019 Z. z. o riadení projektov).

**Príloha č. 3**

**k vyhláške č. xx/2019 Z. z.**

**MINIMÁLNE BEZPEČNOSTNÉ OPATRENIA**

1. **Organizácia kybernetickej a informačnej bezpečnosti**

**Kategória I.**

1. Určenie pracovníka zodpovedného za koordináciu KIB.
2. Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre organizáciu správcu záväzný a obsahuje minimálne:
	1. určenie povinností, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu KIB,
	2. základné zásady a opatrenia KIB, ktoré organizácia správcu má zavedené a riadi sa nimi.

**Kategória II.**

1. Vypracovanie a implementácia interného riadiaceho aktu Politika kybernetickej a informačnej bezpečnosti, (ďalej len „bezpečnostná politika“), ktorý je pre organizáciu správcu záväzný a obsahuje minimálne:
	1. určenie povinností, zodpovednosti a právomoci manažéra informačnej bezpečnosti a všetkých zamestnancov v oblasti KIB,
	2. základné zásady a opatrenia KIB v štruktúre oblastí definovaných touto vyhláškou.
2. Určenie a personálne pokrytie role manažéra informačnej bezpečnosti v organizácii správcu zodpovedného za koordináciu a plnenie nasledovných úloh:
	1. vypracovať, udržiavať a aktualizovať bezpečnostnú politiku a ďalšie interné riadiace akty podľa písm. c),
	2. riadiť a zaisťovať KIB podľa všeobecne záväzných právnych predpisov a Interných riadiacich aktov,
	3. metodicky viesť správcov ITVS, gestorov ITVS, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov,
	4. analyzovať, definovať a monitorovať bezpečnostné hrozby a riziká organizácie správcu,
	5. navrhovať opatrenia k zamedzeniu alebo minimalizácii rizík a dopadov hrozieb, bezpečnostných udalostí, incidentov, mimoriadnych situácií a monitorovať plnenie a efektivitu týchto opatrení,
	6. koordinovať vypracovanie plánov kontinuity a obnovy činností organizácie správcu,
	7. predkladať odborné stanoviská, analýzy k procesom, projektom, zmenám a ostatným aktivitám spoločnosti majúcich dopad na KIB organizácie správcu,
	8. zabezpečiť preskúmanie stavu informačnej bezpečnosti a spolupracovať pri realizácii auditov vykonávaných internými a externými subjektmi,
	9. zabezpečovať školenia zamestnancov v oblasti informačnej bezpečnosti.
	10. spolupráca s ostatnými autoritami (Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, Národný bezpečnostný úrad, CSIRT-SK).
3. Vypracovanie a implementácia dielčích interných riadiacich dokumentov pre vybrané oblasti KIB, v rozsahu a detailu zodpovedajúcom veľkosti a štruktúre organizácie správcu a významu ITVS v jeho správe, s detailným popisom jednotlivých opatrení a postupov pre nasledovné oblasti:
	1. organizácia informačnej bezpečnosti,
	2. riadenie aktív, hrozieb a rizík,
	3. personálna bezpečnosť,
	4. riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
	5. technické zraniteľnosti systémov a zariadení,
	6. riadenie bezpečnosti sietí a informačných systémov,
	7. riadenie prevádzky,
	8. riadenie prístupov,
	9. kryptografické opatrenia,
	10. riešenie kybernetických bezpečnostných incidentov,
	11. monitorovanie, testovanie bezpečnosti a bezpečnostné auditov,
	12. fyzická bezpečnosť a bezpečnosť prostredia,
	13. riadenie kontinuity procesov.
4. Vykonávanie pravidelných auditov KIB minimálne každé dva roky.

Úlohy podľa písm. d), e), f) je možné plniť vypracovaním a implementáciou bezpečnostného projektu ISVS.

**Kategória III.**

1. Vytvorenie bezpečnostného výboru, ktorý je poradným orgánom štatutára organizácie správcu.
2. Bezpečnostný výbor plní najmä nasledovné úlohy:
	1. definovanie a riadenie stratégie v oblasti KIB,
	2. riadenie bezpečnostných rizík, akceptácia bezpečnostných rizík, ktoré sa týkajú viac ako jednej organizačnej jednotky organizácie správcu,
	3. schvaľovanie a rozhodovanie o implementácie významných bezpečnostných opatrení a postupov,
	4. schvaľovanie odporúčaní, návrhov strategických a koncepčných materiálov v oblasti KIB, predkladaných manažérom informačnej bezpečnosti,
	5. definovať zodpovednosť za implementáciu a prevádzku jednotlivých opatrení a postupov KIB.
3. Bezpečnostný výbor sa skladá minimálne z:
4. štatutára správcu, jeho zástupcu, alebo ním poverenej osoby,
5. manažéra informačnej bezpečnosti,
6. vedúceho zamestnanca organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry,
7. vedúceho zamestnanca organizačného útvaru zodpovedného za právne a legislatívne služby,
8. zodpovednej osoby za ochranu osobných údajov,
9. ďalších osôb.
10. Vytvorenie pozície manažéra informačnej bezpečnosti v organizácii správcu mimo organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry, alebo zabezpečenie jeho nezávislého postavenia prostredníctvom interných riadiacich aktov.
11. Manažér informačnej bezpečnosti okrem úloh uvedených v Kategórii II. plní nasledovné ďalšie úlohy:
12. informovanie bezpečnostného výboru alebo štatutára správcu o stave informačnej bezpečnosti v organizácii správcu minimálne jeden krát ročne,
13. bezodkladné informovanie bezpečnostného výboru alebo štatutára správcu závažných bezpečnostných rizikách, incidentoch a významných bezpečnostných udalostiach,
14. zabezpečenie vypracovania bezpečnostného projektu ISVS v súčinnosti s vedúcim zamestnancom organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry,
15. zabezpečenie nezávislého preskúmanie stavu informačnej bezpečnosti a spolupráca pri realizácii auditov vykonávaných internými a externými subjektmi.
16. Zabezpečenie kontinuálneho vzdelávania manažéra informačnej bezpečnosti.
17. Monitorovanie a vyhodnocovanie dodržiavania Politiky kybernetickej a informačnej bezpečnosti a efektivity jednotlivých opatrení a postupov.
18. Aktualizácia Politiky kybernetickej a informačnej bezpečnosti minimálne na ročnej báze.
19. Uplatňovanie princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie správcu, tak aby rovnaká osoba nebola zodpovedná za vykonávanie a zároveň aj schvaľovanie, alebo kontrolu bezpečnostne relevantných aktivít a činností.
20. Zabezpečenie preskúmania a identifikácie bezpečnostných rizík v počiatočných fázach procesu riadenia projektov v organizácii správcu a stanovenie adekvátnych opatrení pre zníženie každého identifikovaného rizika na prijateľnú úroveň. Definovanie osoby zodpovednej za KIB v projektovom tíme.
21. Vykonávanie pravidelných nezávislých auditov KIB minimálne každý rok.
22. **Riadenie rizík KIB**

**Kategória I**

1. Vypracovanie analýzy rizík KIB.
2. Kontinuálne riadenie rizík KIB.

**Kategória II**

1. V organizácii správcu musia byť identifikované všetky významné informačné aktíva a určený ich vlastník, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
2. Informačné aktíva musia byť zaradené podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných tried, pre ktoré sú stanovené bezpečnostné opatrenia minimálne pre ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
3. Klasifikačné triedy pre informačné aktíva podľa osobitného predpisu[[14]](#footnote-14) sú:
	* verejné,
	* interné,
	* chránené a
	* prísne chránené.
4. Vypracovanie a implementácia interného riadiaceho aktu pre Riadenie bezpečnostných rizík, ktorý musí obsahovať minimálne:
5. zodpovednosť za vykonanie analýzy rizík KIB,
6. proces vykonávania analýzy rizík,
7. matica určenia závažnosti rizika,
8. periodicitu vykonávania analýzy rizík,
9. spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v zmysle stanovenej matice určenia závažnosti rizika.
10. Vykonávanie analýzy rizík minimálne každé dva roky.

**Kategória III**

1. Vytvorenie a udržiavanie zoznamu informačných aktív každého organizačného útvaru organizácie správcu, ktorý je zároveň ich vlastníkom a ktorý stanový požiadavky na dôvernosť, dostupnosť a integritu každého informačného aktíva v jeho vlastníctve.
2. Vypracovanie a implementácia interného riadiaceho aktu pre Riadenie rizík KIB, ktorý musí obsahovať podľa predchádzajúceho odseku.
3. Vykonávanie analýzy rizík a vyhodnocovanie súladu implementovaných opatrení s touto vyhláškou minimálne každý rok.
4. **Personálna bezpečnosť**

**Kategória I**

1. Vykonanie bezpečnostného vzdelávania za účelom zvýšenia bezpečnostného povedomia minimálne každé tri roky.
2. Zabezpečenie, aby boli zamestnanci povinnej osoby a tretia strana poučení o svojich právach a povinnostiach predtým, ako získajú prístup k ITVS.
3. Zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty pracovníkovi , ktorý je zodpovedný za koordináciu KIB.
4. Stanovenie postupu pri ukončení pracovného pomeru zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí
	1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,
	2. navrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
	3. odstránenie informácií správcu zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
	4. zrušenie prístupových práv v informačných systémoch verejnej správy,
	5. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

**Kategória II**

1. Musí vypracovať a pravidelne aktualizovať interný riadiaci akt Bezpečnostné zásady pre koncových používateľov, ktorý bude obsahovať súhrn všetkých povinností a oprávnení v oblasti KIB pre koncových používateľov najmä:
2. prideľovanie prístupových práv,
3. zásady tvorby a používania hesiel,
4. zásady ochrany pred infiltráciou škodlivým kódom,
5. zásady bezpečného používania elektronickej pošty,
6. zásady bezpečného používania internetu,
7. zásady bezpečného používania komunikačných nástrojov a sociálnych sietí,
8. zásady používania prenosných zariadení a médií,
9. zálohovanie údajov,
10. riešenie bezpečnostných incidentov,
11. ochrana fyzického majetku,
12. pohyb v priestoroch organizácie správcu.
13. Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktami týkajúcimi sa KIB.
14. Zavedenie procesu preukázateľného oboznámenia správcov ITVS s internými riadiacimi aktami týkajúcimi sa KIB.
15. Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti KIB ako aj opatreniami a postupmi zvedenými v organizácii správcu pre ich elimináciu.
16. Každý zamestnanec musí absolvovať zvyšovanie bezpečnostného povedomia minimálne každé dva roky.
17. Každá osoba s prístupom k ITVS musí byť:
	1. oboznámená so spôsobom používania ITVS a bezpečnostných mechanizmov ITVS v rozsahu svojej pracovnej náplne,
	2. poučená, aby vedela rozoznať bezpečnostný incident od bežnej prevádzky a zvládnuť postup v prípade incidentu,
	3. oboznámená o zamestnancovi, na ktorého sa môže obracať s otázkami a nejasnosťami pri používaní ITVS a bezpečnostných mechanizmov ITVS.
18. Prípady porušenia interných riadiacich aktov v oblasti KIB musia byť sankcionované prostredníctvom disciplinárneho procesu organizácie správcu.

**Kategória III**

1. Vytvorenie evidencie ITVS s priradením konkrétnych správcov každého informačného ITVS, ktorý sú zodpovední za implementáciu a prevádzku bezpečnostných opatrení a postupov.
2. Každý zamestnanec musí absolvovať zvyšovanie bezpečnostného povedomia minimálne raz ročne.
3. **Riadenie prístupov**

**Kategória I.**

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do ITVS.
2. Zavedenie identifikácie používateľa a následnej autentifikácie pri vstupe do ITVS.
3. Zavedenie pravidiel pre zmenu používateľských hesiel s frekvenciou aspoň 1 rok.

**Kategória II.**

1. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám ITVS založenom na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh.
2. Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
3. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
4. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.
5. Vytvorenie a presadzovanie politiky a systému správy hesiel ktorá umožní používateľom najmä:
6. zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,
7. presadzovať určenú štruktúru hesla,
8. vyžadovať pravidelnú zmenu hesla,
9. uchovávať a prenášať používateľské heslá bezpečným spôsobom (zamedzenie prezradenia hesla inej osobe vrátane administrátora systému).
10. Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do ITVS a ich obmedzenie iba na nevyhnutné prípady.
11. Preskúmavanie privilegovaných prístupových v pravidelných intervaloch najmenej však každý rok.
12. Určenie bezpečnostných zásad pre mobilné pripojenie do ITVS a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač, smartfón alebo tablet.
13. Automatické zaznamenávanie každého prístupu administrátora do ITVS a automatické zaznamenávanie prístupu používateľa.
14. Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov ITVS.

**Kategória III.**

1. Implementácia centrálnej správy identít (IDM).
2. Preskúmanie prístupových opatrení v spolupráci s vlastníkom minimálne každý rok.
3. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých 6 mesiacov.
4. Implementácia, vynucovanie prístupových rolí v ITVS.
5. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do ITVS, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov po dobu aspoň 6 mesiacov.
6. Používanie silných autentizačných metód pre overenie identity používateľov ako viacfaktorová autentizácia (PKI karty, tokeny, biometrické prostriedky a pod.) pri ITVS, ktoré obsahujú prísne chránené informačné aktíva v zmysle klasifikácie informačných aktív.
7. **Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami**

**Kategória I**

1. V zmluve s dodávateľmi musí byť stanovená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa KIB. (môže byť odkaz na zákon o ITVS a túto vyhlášku ITVS, nariadenie GDPR a pod.).

**Kategória II**

1. Požiadavky v oblasti KIB musia byť stanovené, odsúhlasené a formálne zdokumentované formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup, alebo akékoľvek používanie ITVS.
2. Zmluvné požiadavky na KIB musia obsahovať najmä záväzok:
	1. plnenia stanovených požiadaviek a kritérií pre oblasť KIB pri dodávke predmetu zmluvy,
	2. ochrany informácií (informačných aktív), ku ktorým bude poskytnutý prístup,
	3. oboznámenia sa a dodržiavania všetky interné riadiace akty týkajúce sa KIB a ďalšie opatrenia a postupy KIB špecifické pre účel plnenia predmetu zmluvy,
	4. riadenia a monitorovania prístupov do ITVS vrátane spôsobu a mechanizmu,
	5. možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
	6. oznámenia všetkých bezpečnostných rizík, nedostatkov, alebo zraniteľností ITVS zistených v rámci plnenia predmetu zmluvy ako aj povinnosť a proces ich ošetrenia,
	7. spolupráce pri riešení bezpečnostných incidentov najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
	8. zachovania úrovne KIB pri významných zmenách vrátane spôsobu a formy prechodu k inému dodávateľovi.
3. V prípade využívania dodávateľských reťazcov musia byť pred začatím využívania služieb identifikované možné riziká KIB a posúdené najmä:
	1. kritické komponenty a prvky služby,
	2. možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
	3. možné riziká KIB vo vzťahoch medzi dodávateľmi a subdodávateľmi,
	4. ďalšie možné riziká KIB vyplývajúce zo životného cyklu dodávanej služby a možnosti ukončenia dodávky služieb, alebo prechodu k inému dodávateľovi.
4. Pri zmenách služieb poskytovaných treťou stranou musí byť posúdený dopad týchto na KIB a ak je to potrebné, navrhnuté a implementované ďalšie opatrenia a postupy KIB.
5. Do zmluvného vzťahu s tretími stranami musí byť zavedený proces implementácie zmien v oblasti riadenia KIB v organizácii správcu (napr. zmena politík, štandardov, zavedenie nových opatrení a postupov).
6. Pri vývoji aplikácií a systémov realizovaného treťou stranou musia byť v zmluve stanovené jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.

**Kategória III**

1. Pre ITVS, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu musí byť implementovaná technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.
2. Správca vypracuje a implementuje interný predpis stanovujúci zásady KIB pre dodávateľov a tretie strany pokrývajúci minimálne:
	1. bezpečnostné požiadavky pri riadení vzťahov s dodávateľmi,
	2. bezpečnostné požiadavky pri ošetrení KIB v zmluvách s dodávateľmi,
	3. bezpečnostné požiadavky dodávateľských reťazcov ITVS,
	4. bezpečnostné požiadavky monitorovania a preskúmavania dodávateľských služieb,
	5. bezpečnostné požiadavky riadenia zmien v službách dodávateľa,
	6. bezpečnostné požiadavky pre prístupové práva a účty,
	7. bezpečnostné požiadavky na fyzickú bezpečnosť,
	8. bezpečnostné požiadavky pre ochranu a zálohovanie dát,
	9. bezpečnostné požiadavky pre mobilné prostriedky a vzdialený prístup.
3. Musí byť vytvorený a využívaný proces pravidelného monitorovania a preskúmavania KIB vo vzťahu s dodávateľmi.
4. **Bezpečnosť pri prevádzke informačných systémov a sietí**

**Kategória I**

1. Pre účinnú prevenciu pred stratou dát musí byť v organizácii správcu zavedený proces pre vytváranie záložných kópií dôležitých informácií a softvéru.
2. V organizácii správcu musí byť vypracovaná a dodržiavaná politika zálohovania, ktorá definuje požiadavky organizácie správcu na zálohovanie, vrátane doby uchovávania, testovania záloh ako aj opatrenia pre ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií musia byť uložené do uzamykateľného priestoru.

**Kategória II**

1. Archivačná záloha musí byť vyhotovená v dvoch kópiách.
2. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a v prípade nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
3. Zabezpečenie vykonania testu obnovy ITVS a údajov z prevádzkovej zálohy najmenej raz za jeden rok.
4. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte ako sa nachádzajú technické prostriedky ITVS, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.
5. Prevádzkové postupy ITVS musia byť dokumentované, udržiavané a dostupné pre všetkých používateľov, ktorí ich potrebujú. Za aktuálnosť prevádzkovej dokumentácie zodpovedajú správcovia jednotlivých ITVS.
6. Všetky zmeny v prevádzkovaných ITVS, ako aj procesoch, alebo fyzických objektoch spoločnosti, ktoré môžu mať vplyv na bezpečnosť informačných aktív musia byť formálne dokumentované a schválené v procese riadenie zmien.
7. Správca vypracuje a implementuje interný riadiaci aktu pre riadenie zmien, ktorý musí obsahovať posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrhom adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.
8. Zmeny pri ktorých ich iniciátor nedokáže jednoznačne určiť, alebo vylúčiť možný dopad na bezpečnosť posudzuje manažér informačnej bezpečnosti.
9. V rámci formálneho procesu riadenia zmien musí byť stanovený aj postup pre kontrolovanú a autorizovanú implementáciu urgentných zmien (napr. pri riešení bezpečnostného incidentu, náhleho výpadku kritického zariadenia a pod.).
10. Na jednotlivých prvkoch ITVS musia byť implementované bezpečnostné nastavenia (hardening) podľa odporúčania výrobcov, alebo podľa interného riadiaceho dokumentu. Bezpečnostné nastavenia musia byť implementované najmä na nasledovných prvkoch ITVS:
	1. operačné systémy,
	2. virtualizačné prostredia ,
	3. aplikačný software,
	4. pracovné stanice,
	5. sieťové zariadenia, vrátane bezpečnostných zariadení,
	6. databázové prostredia.
11. ITVS musia byť monitorované za účelom identifikácie ich kapacitných požiadaviek a ich trendov tak, aby nedošlo ku kritickému výpadku, spomaleniu, alebo inej neočakávanej poruche funkčnosti.
12. Vývojové, testovacie a prevádzkové prostredia musia byť kde je to možné vzájomne oddelené, za účelom prevencie neautorizovaného prístupu alebo zmien v prevádzkovom prostredí.
13. **Hodnotenie zraniteľností a bezpečnostné aktualizácie**

**Kategória I**

1. Nastavenie automatickej aktualizácie operačného systému a aplikácií.

**Kategória II**

1. V organizácii správcu musí byť stanovený efektívny proces pre pravidelné zisťovanie a riešenie technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
2. Všetky zistené kritické zraniteľnosti musia byť odstránené 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. Hodnotenie zraniteľností musí byť vykonávané minimálne raz ročne.
4. V organizácii správcu musí byť vypracovaný a zavedený proces pre riadenie implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov ITVS.
5. Správca musí vytvoriť a udržiavať inventárny zoznam hardware a software jednotlivých prvkov ITVS, vrátane prvkov v správe tretích strán pre identifikáciu relevantných zraniteľností a aktualizácií.
6. Správcovia jednotlivých prvkov ITVS sú povinní monitorovať zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky ITVS v ich správe.
7. Primárnymi zdrojmi pre identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú:
	1. informácie zo systémov a automatizovaných technológií pre aktualizáciu,
	2. informačný servis výrobcov technológií (napr. mailing list, webportály, webstránky apod.),
	3. výstupy z bezpečnostných technológií,
	4. výsledky penetračných testov,
	5. oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti (napr. CSIRT.SK, SK-CERT),
	6. webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti (napr. https://www.cvedetails.com/, https://www.symantec.com/security-center/vulnerabilities s pod.).
8. Na základe zaradenia do konkrétnej úrovne zraniteľnosti je bezpečnostným aktualizáciám priradená priorita pre ich implementáciu. Priorita je vyjadrená maximálnym časovým obdobím počas ktorého musí byť konkrétna bezpečnostná aktualizácia implementovaná.
9. Pred implementáciou aktualizácií musí byť podľa možnosti vykonané testovanie na identickom, alebo aspoň podobnom testovacom prostredí, alebo systéme s cieľom identifikácie možných problémov, výpadkov, alebo neočakávaných chýb.
10. Hodnotenie zraniteľností je postavené na ich skóre v súlade s medzinárodne uznávaným systémom pre hodnotenie zraniteľností CVSS (Common Vulnerability Scoring System).
11. Priority pre inštaláciu bezpečnostných aktualizácií od ich vydania, vrátane testovania, sú nasledovné:
	1. Kritická (CVSS skóre 9.0 – 10.0) najneskôr do 30 dní od vydania,
	2. Vysoká (CVSS skóre 7.0 - 8.9) najneskôr do 60 dní od vydania,
	3. Stredná (CVSS skóre 4.0 - 6.9) najneskôr do 90 dní od vydania,
	4. Nízka (CVSS skóre 0.2- 3.9) podľa rozhodnutia správcu.
12. Výnimky z implementácie bezpečnostných aktualizácií musia byť schválené a evidované manažérom informačnej bezpečnosti, ktorý musí určiť bezpečnostné opatrenia pre ochranu pred zneužitím zraniteľnosti pre elimináciu ktorej bola bezpečnostná aktualizácia vydaná.
13. Súbory s bezpečnostnými aktualizáciami musia byť získavané výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. V prípade nejasností, alebo iného zdroja je potrebné porovnanie kontrolných súčtov (hash) jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu, tak aby nedošlo k podvrhnutiu škodlivých aktualizácií.
14. Bezprostredne pred implementáciou aktualizácií musí správca vykonať opatrenia pre možnosť obnovenia pôvodného stavu prvku ITVS pred aktualizáciou v prípade neočakávaných stavov, chýb, alebo odchýlok od požadovanej funkcionality spôsobených aktualizáciou napr. vytvoriť plnú zálohu dotknutého prvku ITVS.
15. Po implementácii aktualizácie musí správca aktualizovaného prvku ITVS verifikovať najmä jeho správnu funkcionalitu.

**Kategória III**

1. Preskúmavanie a odstraňovanie zraniteľností musí byť vykonávané minimálne každých šesť mesiacov.
2. Bezpečnostné a ostatné aktualizácie musia byť implementované najmä prostredníctvom automatizovaného nástroja.
3. **Ochrana proti škodlivému kódu**

**Kategória I**

1. Musia byť prijaté adekvátne opatrenia pre prevenciu, detekciu škodlivého kódu ako aj pre efektívnu reakciu (obnovu) v prípade infiltrácie škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho, alebo nepovoleného software.
3. Prevencia a detekcia škodlivého kódu musí byť pravidelná a zameraná hlavne na:
	1. používanie prenosných médií (USB kľúče, flash disky, CD, DVD a pod.)
	2. škodlivé emailové prílohy a odkazy,
	3. podozrivé, škodlivé webové stránky a odkazy,
	4. externú a internú sieťovú komunikáciu v spoločnosti vrátane webových sídiel,
	5. prenos súborov z externých sietí.
4. Pre prenos súborov z externých sietí musí byť vytvorený proces, alebo postup, ktorý zaistí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.

**Kategória II**

1. Zavedenie ochrany ITVS pred škodlivým kódom najmenej v rozsahu:
2. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu
3. a nepovolených typov príloh,
4. detekcie prítomnosti škodlivého kódu na všetkých používaných ITVS,
5. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na
6. prítomnosť škodlivého softvéru,
7. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu,
8. Zavedenie ochrany pred nevyžiadanou elektronickou poštou.

**Kategória III.**

1. V organizácii správcu musí byť implementovaný centralizovaný systém riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení.
2. Detekcia inštalácie nelegálneho, alebo nepovoleného software musí byť vykonávaná prostredníctvom automatizovaných nástrojov.
3. Pre efektívne zvládanie infiltrácie škodlivým kódom musia byť vypracované postupy pre obnovu a odstránenie infiltrácie škodlivým kódom aspoň pre kritické systémy.
4. **Sieťová a komunikačná bezpečnosť**

**Kategória I**

1. Všetky koncové stanice musia byť chránené prostredníctvom softvérového personálneho firewallu (súčasť operačného systému alebo samostatný softvér).
2. Na sieťových zariadeniach musia byť implementované minimálne nasledovné bezpečnostné opatrenia:
	1. pravidelná aktualizácia firmvéru,
	2. zmena továrensky nastavených autentifikačných údajov,
	3. pre bezdrôtové siete musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
	4. vypnutie možnosti správy zariadenia na diaľku.
3. Ochrana vonkajšieho a interného prostredia musí byť realizovaná prostredníctvom firewallu.

**Kategória II**

1. Prenos informácií akýmkoľvek spôsobom musí byť riadený. Pre jednotlivé druhy komunikácie musia byť stanovené bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.
2. Bezpečnostné opatrenia musia zabezpečiť ochranu prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.
3. Správa počítačových sietí musí byť riadená a kontrolovaná.
4. Pri prenose údajov prostredníctvom verejnej siete, alebo bezdrôtovej siete musia byť implementované opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia pre zaistenie požadovanej dostupnosti sieťových služieb.
5. Pre všetky sieťové služby musia byť identifikované a dokumentované bezpečnostné mechanizmy, úroveň služieb, požiadavky na manažment.
6. Sieťové služby, používatelia a jednotlivé prvky ITVS 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 aj na fyzickej úrovni.
7. Ochrana vonkajšieho a interného prostredia musí byť realizovaná prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia,
8. Bezdrôtové siete musia byť chránené a umiestené tak aby bol zamedzený priamy prístup k citlivým údajom správcu.
9. Musí byť vytvorená a pravidelne aktualizovaná dokumentácia počítačovej siete obsahujúca najmä evidencia všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológia siete a využitie IP rozsahov.
10. Pre prenos informácií k tretím stranám musí byť uzavretá zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami ako aj právomocami a zodpovednosťami (napr. kontaktné osoby, spolupráca pri úniku prenesených informácií a pod.).
11. Všetky formy výmeny elektronických správ musia byť riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii, alebo zneužitiu.
12. Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť musí byť s treťou stranou uzavretá zmluva o mlčanlivosti, alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe, alebo verejne dostupné informácie o spoločnosti,
13. Vzdialený prístup do vnútornej siete organizácie správcu musí podliehať autentifikácii a autorizácii.

**Kategória III.**

1. Organizácia správcu musí mať implementovanú technológiu detekcie a prevencie prieniku IPS (Intrusion Prevention Systému) minimálne na perimetri siete umiestnenú medzi firewall a chránenú časť siete.
2. Na všetkých serveroch podporujúcich základné služby ITVS správcu musí byť implementované sondy detekcie a prevencie prieniku technológia HIPS (Host Intrusion Prevention System).
3. Všetkých verejne dostupné a kritické webové aplikácie musia byť chránené webovým aplikačným firewallom (WAF).
4. **Akvizícia, vývoj a údržba ITVS**

**Kategória I**

1. Obstarávanie alebo vytváranie nových, alebo úprava stávajúcich ITVS musia byť zdokumentované a realizované v súčinnosti s pracovníkom zodpovedným za koordináciu KIB.

**Kategória II**

1. Pri vytváraní nových, alebo úprave stávajúcich ITVS musia byť identifikované a špecifikované požiadavky na KIB.
2. Pri identifikácii požiadaviek musia byť brané do úvahy najmä požiadavky na dôvernosť, dostupnosť a integritu informačných aktív (klasifikácia), všetky známe bezpečnostné hrozby, incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu ako aj požiadavky všeobecne záväzných právnych predpisov.
3. Informácie prenášané prostredníctvom verejných sietí musia byť adekvátne chránené najmä pred neoprávneným prístupom, modifikáciou, alebo nedostupnosťou šifrovaním.
4. Informácie v transakciách ITVS, alebo medzi ITVS musia byť chránené tak, by sa zabránilo nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam a to najmä použitím elektronických podpisov, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.
5. Všetky zmeny v ITVS a aplikáciách počas ich vývoja musia byť riadené prostredníctvom formálnych postupov riadenia zmien.
6. Počas vývojového cyklu kritických ITVS musí byť vykonávané bezpečnostné testovanie v pravidelných intervaloch podľa možnosti pri všetkých vydaniach, alebo verziách, tak aby bolo možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky, alebo prípadné chyby v dizajne.
7. Súčasťou akceptačného testovania ITVS musí byť aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov ako sú autentizačné, autorizačné mechanizmy, prístupové role a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.
8. Testovacie dáta sa musia byť vybrané s ohľadom ich citlivosti pre organizáciu správcu ako aj požiadavky regulácie. Ak je to možné musia byť citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak aby zostali zachované logické súvislosti avšak ich spätné obnovenie nebolo možné. Osobné údaje je možné použiť pri testovaní iba vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.
9. **Zaznamenávanie udalostí a monitorovanie**

**Kategória I.**

1. Úspešné a neúspešné autentifikačné udalosti (prihlásenie a odhlásenie sa zo systému).

**Kategória II.**

1. Všetky významné udalosti ITVS musia byť zaznamenávané, uchovávané a pravidelne kontrolované.
2. Pre každý prvok ITVS musia byť vyšpecifikované a zdokumentované udalosti, ktoré majú byť zaznamenávané a jednotlivé prvky ITVS musia byť podľa tejto špecifikácie nakonfigurované.
3. Podľa typu systému, alebo zariadenia (napr. pracovná stanica, server, sieťové zariadenie) musia byť zaznamenávané do log súborov minimálne nasledovné udalosti:
	1. úspešné a neúspešné autorizačné udalosti ,
	2. úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
	3. úspešné a neúspešné prístupy k log súborom,
	4. úspešné a neúspešné prístupy k systémovým zdrojom,
	5. vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
	6. zmeny v prístupových oprávneniach,
	7. aktivácia a deaktivácia bezpečnostných mechanizmov (antivírusový systém, osobný firewall, IDS/IPS,
	8. spustenie a zastavenie procesov (služby, daemony a pod.),
	9. konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
	10. spustenie, vypnutie, reštartovanie systému, alebo aplikácie, chyby a výnimky,
	11. významné aktivity v sieťovej komunikácii (internej aj v rámci prístupu na Internet)
	12. požiadavka na autentizačné služby vrátane označenia požadujúcej entity
	13. IP adresy pridelené prostredníctvom služby DHCP
4. Jednotlivé záznamy v log súboroch musia obsahovať minimálne nasledovné informácie o každej zaznamenanej udalosti, ak sú k dispozícii:
	1. čas a dátum udalosti,
	2. identifikácia používateľa (User ID),
	3. identifikácia zariadenia (IP adresa, alebo hostname)
	4. informácie týkajúca sa udalosti (správa, alebo kód)
	5. indikácia úspešnosti, alebo zlyhania operácie
	6. pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port
5. Záznamy udalostí (logy) musia byť uchovávané minimálne po dobu 6 mesiacov a musia byť adekvátne chránené pred zničením, alebo modifikáciou.
6. Kontrolu zaznamenaných udalostí ako aj výstrahy generovaných ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov ITVS (serverov, systémov a pod.), ak to nie je možné, použitím automatizovaných nástrojov minimálne na dennej báze.
7. Bezpečnostne relevantné udalosti musia byť analyzované bezodkladne s cieľom stanoviť či sa jedná o kybernetický bezpečnostný incident.
8. Pre zachovanie správnosti, presnosti a možnosti spätného dohľadania musí byť čas na všetkých relevantných prvkoch ITVS synchronizovaný prostredníctvom presného časového zdroja.

 **Kategória III**

1. Správca musí vypracovať a zaviesť do praxe interný riadiaci akt pre zaznamenávania udalostí (logovanie) a monitorovanie bezpečnosti ITVS.
2. Záznamy udalostí (logy) musia byť uchovávané aj mimo konkrétneho prvku ITVS, ktoré ich vytvára tak aby sa vylúčilo ich odstránenie, alebo modifikácia.
3. Kontrola a vyhodnocovanie zaznamenaných udalostí musí byť vykonávaná automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia v prípade bezpečnostne významných udalostí.
4. Výstrahy z monitorovacích nástrojov ako aj výstrahy generované ostatnými bezpečnostnými technológiami musia byť preverené bezodkladne, kritické výstrahy okamžite po ich obdržaní.
5. Bezpečnostný dohľad podľa bodu c) a d) musí byť vykonávané v režime 24 hodín denne 7 dní v týždni
6. Systémy určené pre vytváranie záznamov o udalostiach ako aj samotné tieto súbory musia byť zabezpečené pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä zmenami a zničením.
7. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna, tak aby nedochádzalo k nežiaducim prepisovaním týchto záznamov, alebo znefunkčneniu systému logovania.
8. **Fyzická bezpečnosť a bezpečnosť prostredia**

**Kategória I**

1. ITVS musia byť umiestnené a prevádzkované takým spôsobom aby boli chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

**Kategória II**

1. ITVS musia byť umiestnené v takom priestore, aby ich najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“), zabezpečeným priestorom je najmä serverovňa.
2. Zabezpečené priestory musia byť oddelené od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami.
3. Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktorý tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom musí byť umožnený iba pre oprávneným osobám.
4. Správca musí vypracovať a implementovať interný riadiaci akt, ktorý upravuje prácu v zabezpečených priestoroch ako aj pravidlá pre:
	1. údržbu, uchovávanie a evidenciu technických komponentov ITVS a zariadení ITVS,
	2. používanie zariadení ITVS na iné účely, na aké boli pôvodne určené,
	3. používanie zariadení ITVS mimo určených priestorov,
	4. vymazávanie, vyraďovanie a likvidovanie zariadení ITVS a všetkých typov relevantných záloh,
	5. prenos technických komponentov ITVS alebo zariadení ITVS mimo priestorov orgánu riadenia,
	6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi ITVS tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii."
5. Prvky ITVS s požiadavkou na vysokú dostupnosť musia byť zabezpečené opatreniami na ochranu pred výpadkom zdroja elektrickej energie.

**Kategória III**

1. Budovy kde sa nachádzajú zabezpečené priestory musia byť chránené strážnou službou, ktorá vykonáva kontrolu vstupov a bezodkladné zásahy v prípade incidentu fyzickej bezpečnosti.
2. Serverové a sieťové komponenty ITVS musia byť prevádzkované v miestnostiach opatrených certifikovanými bezpečnostnými dverami, tehlovými alebo betónovými dverami bez okien, alebo do miestností s nerozbitnými nepriehľadnými sklami s detektormi rozbitia sklenenej výplne.
3. Miestnosti, v ktorých sú umiestnené serverové a sieťové komponenty musia byť vybavené senzormi teploty, vlhkosti, dymu, úniku vody, prachu, detektormi pohybu a vibrácií s možnosťou zasielania varovaní a notifikácií do centrálneho monitorovacieho systému, automatizovanej reakcie na základe definovaných hodnôt.
4. Prístup tretích strán do priestorov organizácie správcu môže byť realizovaný iba len v sprievode interného zamestnanca.
5. Prístup do zabezpečených priestorov a budov kde sa nachádzajú prísne chránené informačné aktíva musí byť realizovaný prostredníctvom prístupových tokenov s ukladaním a zálohovaním záznamov o vstupoch aspoň 6 mesiacov.
6. Na jednotlivých komponentoch opatrení fyzickej bezpečnosti musí byť vykonaná technická revízia v pravidelných intervaloch minimálne však jeden krát za dva roky,
7. Podporná infraštruktúra ITVS s požiadavkou na vysokú dostupnosť musí byť zabezpečená ochranou pred výpadkom zdroja elektrickej energie pomocou diesel generátorov.
8. Pre ITVS s požiadavkou na vysokú dostupnosť musia byť zabezpečené záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto ITVS, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.
9. **Riešenie kybernetických bezpečnostných incidentov**

**Kategória I**

1. V organizácii správcu musí byť stanovené kontaktné miesto a spôsob pre nahlasovanie kybernetických bezpečnostných incidentov podľa § 23 ods. 3 písm. a) zákona a § 23 ods. 4 zákona.

**Kategória II**

1. Všetci používatelia ITVS vrátane správcom jednotlivých komponentov ako aj zamestnanci tretích strán, ktorí vykonávajú správu, alebo podporu ITVS sú povinní ohlasovať stanoveným spôsobom bezpečnostné incidenty podľa § 23 ods. 3 písm. a) zákona a § 23 ods. 4 zákona, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabiny ITVS, ktoré zistili pri ich používaní, alebo správe.
2. V organizácii správcu musí byť za účelom včasného prijatia preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt pre riešenie bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri ohlasovaní, spôsob riešenia a evidencie bezpečnostných incidentov.
3. Interný riadiaci akt podľa písm. a) musí obsahovať aktuálne kontaktné údaje správcov jednotlivých komponentov ITVS, zamestnancov tretích strán zodpovedných za správu, alebo podporu ITVS potrebných pri riešení bezpečnostných incidentov ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.
4. S interným riadiacim aktom podľa písm. a), najmä povinnosťou ohlasovať bezpečnostné incidenty musia byť primeraným a preukázateľným spôsobom oboznámení všetci používatelia ITVS vrátane správcom jednotlivých komponentov ako aj zamestnanci tretích strán, ktorý vykonávajú správu, alebo podporu ITVS.
5. Pre ohlasovanie bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných ITVS musí byť vytvorené kontaktné miesto.
6. Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť, alebo bezpečnostná slabina ITVS musí byť odborne posúdená za účelom stanovenia či sa jedná o bezpečnostný incident bez zbytočného odkladu.
7. Za proces odborného posúdenia a analýzy oznámení podľa písm. f) je zodpovedný Manažér informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a vlastníkom/gestorom ITVS, alebo príslušnou jednotkou CSIRT/CERT.
8. Jednotlivé aktivity pri riešení bezpečnostných incidentov musia byť dokumentované v evidencii bezpečnostných incidentov.
9. Pre identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov musia byť stanovené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy (trestno-právne, pracovno-právne, občiansko-právne, obchodno-právne sporoch) najmä v prípadoch kde je pravdepodobné, že k takým sporom dôjde.
10. Poznatky získané z procesu riešenia bezpečnostného incidentu najmä z analýzy a spôsobu vyriešenia musia premietnuté do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov ako aj na zlepšenie detekcie, alebo spôsobu riešenia obdobných bezpečnostných incidentov.

**Kategória III**

1. Interný riadiaci akt pre riešenie bezpečnostných incidentov okrem uvedených náležitostí musí obsahovať povinnosti a zodpovednosti najmä v oblastiach:
	1. plánovania a prípravy na riadené zvládnutie bezpečnostných incidentov,
	2. monitorovania, detekcie, posúdenia a ohlasovania bezpečnostne relevantných udalostí a incidentov,
	3. hodnotenia a rozhodovania o bezpečnostných udalostiach, slabinách a incidentoch,
	4. klasifikačnú schému bezpečnostných incidentov,
	5. evidencie bezpečnostných incidentov,
	6. nakladania s forenznými dôkazmi,
	7. externej a internej komunikácie,
	8. eskalácie a kontrolovanej obnovy,
	9. plánovania a implementácie opatrení pre zlepšenie prevencie, detekcie, alebo reakcie na bezpečnostný incident.
2. Zamestnanci poverení riešením bezpečnostných incidentov musia byť odborne spôsobilí, pravidelne školení a zastupiteľní.
3. V organizácii správcu sú vytvorené plány pre riešenie počítačových incidentov aspoň tohto typu: prienik, nákaza škodlivým kódom, DoS útok, sociálne inžinierstvo (phishing, baiting, impersonácia a pod.), ransomware.
4. **Kryptografické opatrenia**

**Kategória I**

1. Webové sídlo správcu musí byť prístupný prostredníctvom protokolu zabezpečeného protokolu HTTPS s využitím TLS.

**Kategória II a III**

1. Pri ITVS s vysokou požiadavkou na integritu musia byť na zabezpečenie autenticity a integrity súborov použité kryptografické prostriedky, ktorým je najmä elektronický podpis.
2. Pri ITVS s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie a to najmä:
	1. elektronických dokumentov,
	2. dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
	3. emailovej komunikácie prostredníctvom PGP alebo S/MIME,
	4. komunikačných kanálov na výmenu nešifrovaných dát,
	5. centrálnych úložísk,
	6. záloh.
3. Pre zaistenie správneho a efektívneho používania kryptografické prostriedky a šifrovania musia byť vytvorený a implementovaný interný riadiaci akt, ktorý obsahuje najmä:
	1. princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
	2. definovanie požadovanej úrovne ochrany a štandardy šifrovania (typ, sila, algoritmy a pod.),
	3. role a zodpovednosti jednotlivých subjektov pri používaní šifrovania.
	4. riadenie šifrovacích kľúčov
4. Každé použitie kryptografického prostriedku v ITVS musí byť zdokumentované v dokumentácii k ITVS, minimálne na úrovni využívaného algoritmu a verzie.
5. Správca pravidelne prehodnocuje využívané kryptografické prostriedky a overuje či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.
6. **Kontinuita prevádzky ITVS**

**Kategória II a III**

1. Za účelom zachovania kontinuity prevádzky musí byť vykonaná analýza rizík a posúdenie dopadov na dostupnosť jednotlivých ITVS a služieb, ktoré zabezpečujú.
2. Pre ITVS s vysokou požiadavkou na dostupnosť musí byť vypracovaný formálny plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu v prípade mimoriadnej udalosti, alebo núdzovej situácii s cieľom minimalizácie rizika prerušenia prevádzky ITVS a čo najrýchlejšej obnovy v prípade, že k prerušeniu prevádzky ITVS dôjde.
3. Plán kontinuity prevádzky musí obsahovať najmä:
	1. role a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
	2. možné dopady na prevádzku ITVS,
	3. časový rámec obnovy,
	4. identifikácia zdrojov potrebné k obnove prevádzky,
	5. identifikácia zamestnancov potrebných pre obnovu prevádzky,
	6. identifikácia dát a systémov potrebných pre obnovenie prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
	7. identifikácia priestorov potrebných pre obnovenie prevádzky,,
	8. stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov)
	9. identifikáciu vybavenia potrebného pre obnovenie prevádzky (procesy obnovy alebo výmeny kľúčových zariadení; alternatívne zdroje; vzájomná pomoc),
	10. spotrebný materiál potrebný pre obnovenie prevádzky (procesy výmeny zásob a kľúčových dodávok; zabezpečenie núdzových súčastí),
	11. konkrétne havarijné procedúry slúžiace na obnovu prevádzky.
4. Funkčnosť a aktuálnosť plánu kontinuity musí byť overovaná v ročnej periodicite.

1. **Audit a kontrolné činnosti**

**Kategória II**

1. Správca musí vykonávať audity bezpečnosti ITVS aspoň raz za 24 mesiacov.
2. Správca vypracuje program auditov na definované ITVS, ktorý zahŕňa interné a externé audity, posúdenie zraniteľností a penetračné testy.
3. Pre výkon auditu musí byť vypracovaný plán auditu, ktorý obsahuje ciele auditu, referenčné dokumenty, dátumy a miesta vykonania auditu, organizačné útvary, ktoré sú predmetom auditu, roly a zodpovednosti.
4. Audítor vykonávajúci audit musí byť nezávislý , skúsený, musí byť znalý príslušnej legislatívy a štandardov a musí mať vhodné osobnostné predpoklady.
5. Správa z auditu musí obsahovať aspoň zoznam účastníkov auditu, zoznam zistených nezhôd, odporúčaní a príležitostí na zlepšenie.
6. Vedúci zamestnanci sú povinní v rámci plnenia svojich manažérskych úloh preverovať aj dodržiavanie politík, štandardov, postupov a ostatných opatrení stanovených v oblasti KIB a identifikovať prípadný nesúlad.
7. Pri každom prípade, kde bol identifikovaný nesúlad s opatreniami KIB musia byť prijaté opatrenia na jeho odstránenie. V prípade, že je zistená nízka efektivita, alebo neúčinnosť opatrení musia byť tieto opatrenie prehodnotené a upravené tak aby bolo bezpečnostné riziko znížené na prijateľnú úroveň.

**Kategória III**

1. Správca musí vykonávať audity bezpečnosti ITVS aspoň raz za 12 mesiacov.
1. Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. [↑](#footnote-ref-1)
2. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov [↑](#footnote-ref-2)
3. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [↑](#footnote-ref-3)
4. Zákon č. 221/1996 Z. z. o územnom a správnom usporiadaní Slovenskej republiky. [↑](#footnote-ref-4)
5. Zákon č. 377/1990 Zb. o hlavnom meste Slovenskej republiky Bratislave v znení neskorších predpisov, zákon č.401/1990 Zb. o meste Košice a zákon SNR č. 369/1990 Zb. o obecnom zriadení. [↑](#footnote-ref-5)
6. Zákon č. 221/1996 Z. z. o územnom a správnom usporiadaní Slovenskej republiky. [↑](#footnote-ref-6)
7. [§ 3](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/#paragraf-3) a 21  zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov. [↑](#footnote-ref-7)
8. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [↑](#footnote-ref-8)
9. ISO/IEC 27002:2013 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti. [↑](#footnote-ref-9)
10. ISO/IEC 27005:2018 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti. [↑](#footnote-ref-10)
11. Napríklad vyhláška č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. [↑](#footnote-ref-11)
12. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [↑](#footnote-ref-12)
13. ISO/IEC 27002:2013 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti. [↑](#footnote-ref-13)
14. Vyhláška č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. [↑](#footnote-ref-14)