

(Návrh)

VYHLÁŠKA

Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

z ... 2026,

ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky podľa § 31 písm. i) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) ustanovuje:

§ 1

Základné ustanovenia

(1) Táto vyhláška ustanovuje

- a) zaradenie orgánov riadenia a správcov informačných technológií verejnej správy do kategórií jednotlivých oblastí bezpečnostných opatrení kybernetickej bezpečnosti a informačnej bezpečnosti,
- b) vzorový výpočet aktív informačných technológií verejnej správy, ktoré sa identifikujú a udržiavajú podľa prílohy č. 1 so zreteľom na ich dôvernosť, integritu, dostupnosť alebo zníženie kvality, ktoré môžu mať zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb,
- c) obsah bezpečnostných opatrení, rozsah bezpečnostných opatrení pre jednotlivé kategórie vo vzťahu k informačným technológiám verejnej správy podľa prílohy č. 2,
- d) obsah a štruktúru bezpečnostného projektu podľa prílohy č. 3,
- e) spôsob evidencie a hlásenia kybernetických bezpečnostných incidentov podľa prílohy č. 4,
- f) klasifikačnú schému informácií podľa prílohy č. 5.

§ 2

Bezpečnostné opatrenia

(1) Bezpečnostné opatrenia informačných technológií verejnej správy pozostávajú z minimálnych bezpečnostných opatrení podľa prílohy č. 2. Minimálne bezpečnostné opatrenia sú rozdelené do Kategórie I, Kategórie II a Kategórie III v rámci jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti. Vo vzťahu k informačným technológiám verejnej správy sú realizované bezpečnostné opatrenia aspoň na úrovni minimálnych bezpečnostných opatrení tej kategórie, do ktorej je orgán riadenia zaradený.

- (2) Pri duplicite alebo nekompatibilite minimálnych bezpečnostných opatrení rôznych kategórií, ktoré môžu byť aplikované na konkrétne informačné technológie verejnej správy, majú prednosť ustanovenia upravujúce opatrenia vyššej kategórie.
- (3) Minimálne bezpečnostné opatrenia Kategórie I jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na
- a) obec do 6000 obyvateľov,
 - b) obec so štatútom mesta do 6000 obyvateľov,
 - c) právnickú osobu podľa § 5 ods. 2 písm. e) zákona s výnimkou právnických osôb, ktoré sú kritickým subjektom podľa osobitného predpisu,¹⁾
 - d) osobu podľa § 5 ods. 2 písm. g) zákona,
 - e) záujmové združenie právnických osôb podľa § 5 ods. 2 písm. h) zákona.
- (4) Minimálne bezpečnostné opatrenia Kategórie I a Kategórie II jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na
- a) obec nad 6000 obyvateľov,
 - b) obec so štatútom mesta nad 6000 obyvateľov, ktorá nie je krajským mestom,²⁾
 - c) mestskú časť s právnou subjektivitou,³⁾
 - d) Kanceláriu verejného ochrancu práv,
 - e) Úrad komisára pre deti,
 - f) Úrad komisára pre osoby so zdravotným postihnutím,
 - g) Radu pre mediálne služby.
- (5) Minimálne bezpečnostné opatrenia Kategórie I, Kategórie II a Kategórie III jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na

¹⁾ Zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

²⁾ Zákon Národnej rady Slovenskej republiky č. 221/1996 Z. z. o územnom a správnom usporiadaní Slovenskej republiky v znení neskorších predpisov.

³⁾ Zákon Slovenskej národnej rady č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov.
Zákon Slovenskej národnej rady č. 377/1990 Zb. o hlavnom meste Slovenskej republiky Bratislave v znení neskorších predpisov.
Zákon Slovenskej národnej rady č. 401/1990 Zb. o meste Košice v znení neskorších predpisov.

- a) obec, ktorá je krajským mestom,⁴⁾
- b) vyšší územný celok,
- c) ministerstvo a ostatný ústredný orgán štátnej správy,⁵⁾
- d) Úrad pre reguláciu elektronických komunikácií a poštových služieb,
- e) Najvyšší kontrolný úrad Slovenskej republiky,
- f) Úrad pre dohľad nad zdravotnou starostlivosťou,
- g) Úrad na ochranu osobných údajov Slovenskej republiky,
- h) Generálnu prokuratúru Slovenskej republiky,
- i) Dopravný úrad,
- j) Ústav pamäti národa,
- k) Tlačovú agentúru Slovenskej republiky,
- l) Slovenskú televíziu a rozhlas,
- m) Kanceláriu Súdnej rady Slovenskej republiky,
- n) Kanceláriu Najvyššieho súdu Slovenskej republiky,
- o) Kanceláriu Ústavného súdu Slovenskej republiky,
- p) Kanceláriu prezidenta Slovenskej republiky,
- q) Kanceláriu Národnej rady Slovenskej republiky,
- r) Kanceláriu Najvyššieho správneho súdu Slovenskej republiky,
- s) Finančné riaditeľstvo Slovenskej republiky,
- t) Národnú agentúru pre sieťové a elektronické služby,
- u) Zbor väzenskej a justičnej stráže,
- v) DataCentrum Ministerstva financií Slovenskej republiky,
- w) DataCentrum elektronizácie územnej samosprávy Slovenska,
- x) Sociálnu poisťovňu,
- y) zdravotnú poisťovňu,
- z) Národné centrum zdravotníckych informácií,
- aa) komoru podľa § 5 ods. 2 písm. f) zákona,
- ab) právnickú osobu podľa § 5 ods. 2 písm. e) zákona, ktorá je kritickým subjektom podľa osobitného predpisu.¹⁾

⁴⁾ Zákon Národnej rady Slovenskej republiky č. 221/1996 Z. z. o územnom a správnom usporiadaní Slovenskej republiky v znení neskorších predpisov.

⁵⁾ § 3 a § 21 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

- (6) Minimálne bezpečnostné opatrenia konkrétnej kategórie vo vzťahu k informačným technológiám verejnej správy podľa odsekov 3 až 5 sa môžu určiť aj pre iný štátny orgán.
- (7) Bezpečnostné projekty informačných systémov verejnej správy sa vypracujú a implementujú podľa prílohy č. 3.
- (8) Správca predkladá bezpečnostný projekt podľa § 23 ods. 1 a 2 zákona na schválenie podľa § 23 ods. 3 písm. g) zákona orgánu vedenia prostredníctvom vládneho informačného systému kybernetickej bezpečnosti.
- (9) Systémové informácie z informačných technológií verejnej správy podľa § 23 ods. 3 písm. d) a § 23a ods. 2 písm. d) zákona v oblasti bezpečnosti informačných technológií verejnej správy sa zasielajú orgánu vedenia prostredníctvom vládneho informačného systému kybernetickej bezpečnosti a ich rozsah upravuje príloha č. 4.

§ 3 **Riadenie rizík**

- (1) Riadenie rizík zahŕňa
 - a) identifikáciu aktív,
 - b) identifikáciu rizík vrátane popisu prijatých bezpečnostných opatrení,
 - c) analýzu rizík vykonanú podľa metodiky zverejnenej ministerstvom investícií,
 - d) hodnotenie rizík,
 - e) prijatie bezpečnostných opatrení podľa identifikovaných rizík vrátane odôvodnenia odchýlok od opatrení z kategórie, ktorá sa na orgán riadenia alebo správcu vzťahuje,
 - f) preskúmanie rizík minimálne raz ročne a podľa potreby aj ich aktualizáciu a revíziu opatrení,
 - g) analýzu dopadov, ktorá hodnotí následky krízových scenárov na činnosť správcu, určuje cieľovú dobu obnovy a cieľový bod obnovy.
- (2) Identifikácia rizík sa vykonáva na princípe najhoršieho scenára. Úroveň rizika sa určuje podľa vopred stanovených pravidiel a metodických postupov.
- (3) Bezpečnostné opatrenie kategórie, ktorá sa na orgán riadenia alebo správcu vzťahuje, sa nemusí prijať, ak
 - a) konkrétne bezpečnostné opatrenie nie je relevantné pre dané riziko,
 - b) riziku sa možno vyhnúť ukončením alebo nezačatím činnosti, ktorá ho spôsobuje,
 - c) riziku sa možno vyhnúť iným spôsobom než prijatím bezpečnostného opatrenia.

- (4) Výsledok analýzy rizík a návrh bezpečnostných opatrení vrátane odôvodnenia podľa odseku 1 písm. e) musia byť preukázateľne schválené štatutárnym orgánom alebo ním povereným organizačným útvarom.

§ 4

Identifikácia aktív

- (1) Aktívum sa identifikuje a vedie v evidencii aktív. Evidencia aktív sa skladá z identifikovateľných primárnych aktív a podporných aktív.
- (2) Evidencia aktív je centralizovane riadená a zodpovedá aktuálnemu stavu.
- (3) Evidencia aktív sa môže skladať z textovej časti, tabuľkovej časti alebo grafickej časti a jej súčasťou je aj označenie bezpečnostných funkcií podporných aktív alebo odkazy na príslušnú časť bezpečnostnej dokumentácie týchto funkcií.
- (4) Evidencia aktív obsahuje najmä identifikáciu a evidenciu
- a) primárnych aktív,
 - b) podporných aktív,
 - c) vlastníkov aktív,
 - d) zodpovedných osôb za identifikáciu a evidenciu aktív.

§ 5

Spoločné ustanovenia

- (1) Za bezpečnosť informačných technológií verejnej správy je zodpovedný jeho správca. Ak je na bezpečnosť informačných technológií verejnej správy vhodné prijať súbor opatrení nad rámec opatrení uvedených v tejto vyhláske, zmeny v rozsahu opatrení správca zadokumentuje a odôvodní.
- (2) Ak sa v tejto vyhláske ustanovuje použitie postupu podľa technickej normy, slovenskej technickej normy, európskeho normalizačného produktu alebo európskej normy, je možné postupovať aj podľa ich ekvivalentu, ak sa takýmto postupom dosiahne rovnaký výsledok a dodržia sa požiadavky podľa tejto vyhlášky. Pri pochybnostiach o vhodnosti použitia ekvivalentnej normy alebo špecifikácie podľa prvej vety je rozhodujúce vyjadrenie orgánu vedenia k možnosti ich použitia.

§ 6

Prechodné ustanovenia

- (1) V organizácii správcu, ktorý je zriadený alebo založený pred dňom účinnosti tejto vyhlášky, sa táto vyhláška vykoná do 12 mesiacov odo dňa nadobudnutia účinnosti tejto vyhlášky.

- (2) V organizácii správcu, ktorý je zriadený alebo založený po nadobudnutí účinnosti tejto vyhlášky, sa táto vyhláška vykoná do 12 mesiacov odo dňa zriadenia alebo založenia organizácie.

§ 7

Zrušovacie ustanovenie

Zrušuje sa vyhláška 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.

§ 8

Účinnosť

Táto vyhláška nadobúda účinnosť 1. marca 2026.

TYPY AKTÍV – VZOROVÝ VÝPOČET

Typ aktíva	Názov	Popis
Primárne	Elektronické dáta v databázach	Údaje usporiadané v štruktúrovanej podobe, typicky uložené a spracované pomocou systému riadenia bázy dát.
Primárne	Elektronické dáta v súboroch	Súbory údajov uložené lokálne, na serveroch alebo v cloude.
Primárne	Ostatné nehmotné aktíva	Nehmotné aktíva, ktoré zahŕňajú dobré meno organizácie, právne požiadavky a vzťahy, autorské práva, iné duševné vlastníctvo.
Primárne	Papierové dáta	Informácie zaznamenané vo forme textu v listinnej podobe. Táto forma ukladania informácií je charakteristická svojou materiálnou podstatou, čo umožňuje uchovávanie dát bez potreby elektrickej energie alebo digitálnych zariadení.
Primárne	Proces	Štruktúrovaný súbor vzájomne súvisiacich alebo vzájomne sa ovplyvňujúcich činností, navrhnutých tak, aby transformovali vstupy na výstupy a aby bol týmito činnosťami dosiahnutý konkrétny cieľ.
Primárne	Služba	Nehmotný spôsob poskytnutia hodnoty, alebo iného prospešného výsledku používateľovi, ktorá napomáha dosiahnuť požadované výsledky.
Primárne	Služba ISVS	Služba pozostávajúca úplne alebo prevažne z prenosu, ukladania, získavania alebo spracúvania informácií prostredníctvom ISVS.
Podporné	Aplikačný softvér	Softvér, ktorý vykonáva špecifické úlohy pre koncového používateľa alebo pre inú aplikáciu.
Podporné	Cloudové služby	Digitálne služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných počítačových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach. (Počítačové zdroje zahŕňajú zdroje, ako sú najmä

		siete, servery alebo iná infraštruktúra, operačné systémy, softvér, úložiská, aplikácie a služby.)
Podporné	Hardvér	Akékoľvek zariadenie informačnej a komunikačnej technológie alebo ITVS, nevyhnutné na ukladanie dát a vykonávanie softvéru, ktoré je napájané elektrickou energiou, zvyčajne riadené pomocou firmware (BIOS).
Podporné	Kľúčový dodávateľ	Kritická externá entita, ktorá poskytuje tovary alebo služby, ktoré sú nevyhnutné pre ISVS.
Podporné	Komunikačný kanál	Prostriedok, prostredníctvom ktorého sú informácie prenášané z jedného počítačového zariadenia na druhé.
Podporné	Lokalita	Fyzické priestory alebo geografická lokalita, kde sa vykonávajú prevádzkové činnosti.
Podporné	Mobilný telefón	Elektronické zariadenie vybavené operačným systémom, ktoré kombinuje funkcie osobného počítača s funkciami telefónu a umožňuje používateľovi uskutočňovať hlasové hovory, posilať správy a pristupovať k aplikáciám.
Podporné	Notebook, prenosná pracovná stanica	Prenosné výpočtové zariadenie schopné vykonávať úlohy a pristupovať k dátam prostredníctvom aplikácií.
Podporné	Operačný systém	Softvér, ktorý riadi počítačový fyzický, alebo virtuálny hardvér a softvérové zdroje a poskytuje spoločné služby pre počítačové programy.
Podporné	Organizácia	Entita, ktorá zahŕňa viacero používateľov, procesov a služieb, ktoré spolu pracujú na dosiahnutí spoločného cieľa.
Podporné	Ostatné hmotné aktíva	Hmotné aktíva, ktoré vlastní a používa organizácia, ale nezahŕňajú nehnuteľnosti ani ITVS.
Podporné	PC, neprenosná pracovná stanica	Výpočtové zariadenie konštrukčne navrhnuté na stacionárne umiestnenie, s ohľadom na maximálnu rozširiteľnosť, schopné vykonávať úlohy a pristupovať k dátam prostredníctvom aplikácií.
Podporné	Personál	Jednotlivci zamestnaní v organizácii, ktorí vykonávajú procesy a ktorí prispievajú k tvorbe výstupov.

Podporné	Počítačová sieť	Technická infraštruktúra, ktorá spája viaceré počítače a zariadenia s cieľom zdieľania dát, zdrojov a služieb. Sieť môže byť realizovaná prostredníctvom káblových alebo bezdrôtových technológií a môže operovať v rôznych geografických rozsahoch.
Podporné	Používateľ	Jednotlivec alebo skupina, ktorá je v interakcii alebo má prospech zo služby alebo služieb; príklady používateľov zahŕňajú osobu alebo komunitu ľudí.
Podporné	Prenosné dátové médiá	Prenosné dátové médiá sú fyzické alebo elektronické zariadenia alebo médiá, ktoré umožňujú ukladanie, prenos a zdieľanie digitálnych dát medzi rôznymi počítačmi alebo systémami bez potreby priameho pripojenia cez internet alebo lokálnu sieť. Tieto médiá sú navrhnuté tak, aby boli ľahko prenosné a kompatibilné s viacerými zariadeniami.
Podporné	Virtualizačná platforma	Softvér alebo firmware, ktorý vytvára a spravuje virtuálne stroje poskytovaním abstrakcie hardvérových zdrojov (ako sú procesory, pamäť, úložisko a sieťové zariadenia) a rozdeľovaním týchto zdrojov medzi rôzne virtuálne stroje. Tento proces umožňuje viacerým operačným systémom a ich aplikáciám beh na jednej fyzickej platforme s izoláciou a nezávislosťou od seba.

MINIMÁLNE BEZPEČNOSTNÉ OPATRENIA

Položka	Bezpečnostné opatrenia pre organizáciu a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti prijíma správca informačných technológií verejnej správy tak, že:	Kat. I	Kat. II	Kat. III
1.	je určená osoba zodpovedná za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, ktorá je nezávislá od štruktúry riadenia prevádzky a vývoja služieb informačných technológií verejnej správy, a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO
2.	manažér kybernetickej bezpečnosti predkladá návrhy bezpečnostných opatrení a oznamuje informácie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti priamo štatutárnemu orgánu správcu alebo ním poverenému riadiacemu pracovníkovi		ÁNO	ÁNO
3.	je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k ITVS a za pridelenie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a ITVS podľa príslušnej bezpečnostnej politiky	ÁNO	ÁNO	ÁNO
4.	je určená osoba, ktorá je zodpovedná za riešenie kybernetických bezpečnostných incidentov, ako aj prijímanie a evidenciu hlásení voči príslušným regulátorom	ÁNO	ÁNO	ÁNO
5.	je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti, vrátane pridelenia úloh, rolí ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie		ÁNO	ÁNO

6.	je zriadený bezpečnostný výbor, ktorého členovia menovaní štatutárnym orgánom organizácie kompetentne pokrývajú riadenie všetkých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti ustanovených touto vyhláškou, fungovanie výboru upravuje jeho schválený štatút			ÁNO
7.	je zabezpečená primeranosť zdrojov na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti a vzdelávanie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti		ÁNO	ÁNO
8.	je určená osoba zodpovedná za zabezpečenie primeraného vzdelávania a preškoľovania v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre všetky zavedené roly v organizácii správcu v priebehu nástupu, ako aj pri opakovaných školiacich aktivitách	ÁNO	ÁNO	ÁNO
9.	je definovaný a zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti a informačnej bezpečnosti		ÁNO	ÁNO
10.	je uplatnená zásada najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh		ÁNO	ÁNO
11.	je uplatnená zásada oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva správcu bez autorizácie alebo overenia identity		ÁNO	ÁNO
12.	je uplatnená zásada vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností		ÁNO	ÁNO
13.	je uplatnená zásada prístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú		ÁNO	ÁNO
14.	je určený štatutárny orgán zodpovedný za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie	ÁNO	ÁNO	ÁNO

	kybernetickej bezpečnosti a informačnej bezpečnosti a za vzdelávanie v týchto oblastiach			
15.	štatutárny orgán sa preukázateľne zaväzuje dodržiavať a presadzovať dodržiavanie povinností v oblasti kybernetickej bezpečnosti v súlade so stratégiou kybernetickej bezpečnosti a informačnej bezpečnosti a určenými bezpečnostnými politikami a postupmi		ÁNO	ÁNO
16.	je definovaný, schválený a zavedený vnútorný kontrolný systém pre oblasť kybernetickej bezpečnosti		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
17.	organizácia získava informácie o zraniteľnostiach všetkých aktív podporujúcich ISVS a ITVS, vrátane hodnotenia do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu alebo úplne odstránenie	ÁNO	ÁNO	ÁNO
18.	kontinuálne získava informácie o zraniteľnostiach používaných ISVS a prijíma vhodné opatrenia na ich mitigáciu		ÁNO	ÁNO
19.	najmenej raz ročne je vykonávané pravidelné preskúmanie zraniteľností		ÁNO	
20.	najmenej raz za 6 mesiacov je vykonávané pravidelné preskúmanie zraniteľností			ÁNO
21.	je definovaný a zavedený systém kontroly dostupnosti a inštalovania aktualizácií pre všetky aktíva podporujúce ISVS a ITVS podľa ich technických možností s čo najmenším dosahom na prevádzku systémov organizácie	ÁNO	ÁNO	ÁNO
22.	sú určené priority aktualizácií na základe posúdenia rizík		ÁNO	ÁNO
23.	na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností			ÁNO
Položka	Bezpečnostné opatrenia pre správu aktív a riadenie kybernetických hrozieb a rizík zákona prijíma správca tak, že:	Kat. I	Kat. II	Kat. III

24.	identifikuje a vedenie aktuálny zoznam všetkých aktív podľa prílohy č. 1 ako súčasť všetkých ISVS a ITVS organizácie	ÁNO	ÁNO	ÁNO
25.	preskúma a aktualizuje zoznam aktív najmenej raz ročne a v závislosti od výsledkov vykoná aj aktualizáciu evidencie aktív a revíziu prijatých bezpečnostných opatrení. Príslušne systémové informácie o ISVS a ITVS zašle organizácia orgánu vedenia prostredníctvom vládneho informačného systému kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO
26.	sú zdokumentované a prijaté pravidlá používania a postupy nakladania s aktívami		ÁNO	ÁNO
27.	je definovaný a zavedený systém riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý obsahuje: - identifikáciu rizík na úrovni celej organizácie a vedenie katalógu týchto rizík, - metodiku alebo interný postup pre výkon analýzy rizík, - samotnú analýzu rizík s vyhodnotením rizík, - prijatie bezpečnostných opatrení v závislosti od identifikovaných rizík, a ktorý slúži pre určenie primeranosti prijatých bezpečnostných opatrení	ÁNO	ÁNO	ÁNO
28.	preskúma identifikované riziká organizácie najmenej raz ročne a v závislosti od výsledkov vykoná aj aktualizáciu analýzy rizík a revíziu prijatých bezpečnostných opatrení	ÁNO	ÁNO	ÁNO
29.	výsledky analýzy rizík a návrhy bezpečnostných opatrení v nadväznosti na identifikované riziká preukázateľným spôsobom schvaľuje štatutárny orgán organizácie správcu alebo ním poverený organizačný útvar alebo zodpovedná osoba	ÁNO	ÁNO	ÁNO
30.	je vypracovaný, implementovaný a pravidelne aktualizovaný interný riadiaci akt, ktorý je pre organizáciu správcu záväzný a obsahuje bezpečnostné ciele v jednotlivých oblastiach kybernetickej bezpečnosti a informačnej bezpečnosti a k ním určené povinnosti, zodpovednosti a právomoci jednotlivých osôb zastávajúcich bezpečnostné roly	ÁNO	ÁNO	ÁNO

31.	zamestnanci správcu a zamestnanci tretích strán pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom vracajú správcovi všetky aktíva, ktoré mali zverené	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre riadenie udalostí a kybernetických bezpečnostných incidentov prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
32.	je definovaný, zavedený a kontrolovaný systém riadenia bezpečnostných incidentov kybernetickej bezpečnosti a informačnej bezpečnosti organizácie, ktorý obsahuje: - postupy počas celého životného cyklu riadenia bezpečnostných incidentov, - typy identifikovaných udalostí, ich kombinácie a príslušné bezpečnostné incidenty, - komunikačné, eskalačné a nahlasovacie povinnosti, - spoluprácu s orgánom vedenia, - testovanie riešenia bezpečnostných incidentov, pri prevádzke všetkých ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie, najmä: a) správca vedie zoznam všetkých bezpečnostných incidentov v rámci správy ISVS a ITVS, b) správca určí, zavedie a používa mechanizmy a nástroje na detekciu, identifikáciu, reakciu a evidenciu bezpečnostných incidentov pri prevádzke všetkých ISVS a ITVS, c) je zabezpečené pripojenie do systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov	ÁNO	ÁNO	ÁNO
33.	je zabezpečené testovanie riešenia kybernetických bezpečnostných incidentov aspoň raz za kalendárny rok a sú definované, prijaté a oznámené procesy, úlohy a zodpovednosti v oblasti riešenia kybernetických bezpečnostných incidentov		ÁNO	ÁNO
34.	je definovaný systém reakcie na kybernetické bezpečnostné incidenty		ÁNO	ÁNO

35.	poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti		ÁNO	ÁNO
36.	sú zavedené a uplatňované postupy na identifikáciu, zhromažďovanie, získavanie a uchovávanie digitálnych stôp súvisiacich s kybernetickými bezpečnostnými incidentami		ÁNO	ÁNO
37.	sú definované a pravidelne, aspoň raz ročne testované pravidlá pre izoláciu kritických ITVS a ISVS počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva			ÁNO
Položka	Bezpečnostné opatrenia pre riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
38.	organizácia identifikuje a vedie zoznam všetkých činností, procesov a (pre fyzické osoby a právnické osoby, iné organizácie a interne pre samotnú organizáciu) vykonávaných cez ISVS a ITVS, príslušné informácie uvedie organizácia aj v portáloch orgánu vedenia, ako sú Metainformačný systém verejnej správy, Vládny informačný systém verejnej správy, Centrálny portál kybernetickej bezpečnosti a iných centrálnych systémoch podľa potreby	ÁNO	ÁNO	ÁNO
39.	je definovaný a zavedený systém určenia kritickosti činností, procesov a služieb organizácie, ktorý obsahuje: - spôsob identifikácie a vedenia všetkých činností, procesov a služieb, - metodiku pre výkon analýzy dopadov, - samotnú analýzu funkčných dopadov a určenie kritickosti pre ISVS a ITVS, - väzbu na riadenie mimoriadnych a krízových situácií podľa osobitných predpisov a zmluvných požiadaviek, ak súvisia s prevádzkou ISVS a ITVS	ÁNO	ÁNO	ÁNO
40.	organizácia preskúma a analyzuje funkčné dopady pre významné procesy organizácie správcu najmenej raz ročne a v závislosti od výsledkov vykoná aj aktualizáciu určenia kritickosti ISVS a ITVS, analýzy rizík a revíziu prijatých bezpečnostných opatrení	ÁNO	ÁNO	ÁNO

41.	prijíma opatrenia tak, aby bola dostupnosť primárnych aktív počas kybernetického bezpečnostného incidentu primerane zabezpečená v prípade potreby náhradným spôsobom v súlade s požiadavkami všeobecne záväzných právnych predpisov		ÁNO	ÁNO
42.	sú udržiavané a pravidelne, aspoň raz ročne testované záložné kópie dát, softvéru a konfigurácie ISVS a ITVS, o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva		ÁNO	ÁNO
43.	infraštruktúra ISVS a ITVS je zriadená s dostatočnou redundanciou		ÁNO	ÁNO
44.	pre ISVS alebo ITVS s vysokou požiadavkou na dostupnosť vypracuje plán kontinuity prevádzky pre riešenie krízových situácií a zabezpečí adekvátnu reakciu pri mimoriadnej udalosti a čo najrýchlejšej obnovy	ÁNO	ÁNO	ÁNO
45.	je definovaný, nastavený a zavedený systém implementácie a testovania zálohovania biznis dát a systémových, či aplikačných konfigurácií pre všetky aktíva podporujúce ISVS a ITVS podľa ich technických možností s čo najmenším dosahom na prevádzku systémov organizácie	ÁNO	ÁNO	ÁNO
46.	je zavedený, zdokumentovaný, v pravidelných intervaloch testovaný a dodržiavaný postup vytvárania, ukladania a obnovy záložných kópií údajov alebo konfigurácií do logicky a fyzicky oddelených priestorov		ÁNO	ÁNO
47.	je zavedený, zdokumentovaný, v pravidelných intervaloch testovaný a dodržiavaný princíp vytvárania, ukladania a obnovy záložných kópií údajov alebo konfigurácií, ktorý zabezpečuje dve kópie údajov alebo konfigurácií, na dvoch rozličných typoch médií, z ktorých jedna kópia je uložená v logicky, fyzicky a geograficky oddelenom priestore			ÁNO
48.	pre všetky ISVS v jeho pôsobnosti s vysokou požiadavkou na dostupnosť stanoví Recovery Time Objective a Recovery Point Objective		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
49.	sú určené, uplatnené a kontrolované pravidlá bezpečného vývoja, nákupu a údržby pre všetky ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie, najmä	ÁNO	ÁNO	ÁNO

	a) je zabezpečené prepojenie procesov vedenia aktív, riadenia rizík a projektového riadenia počas celého životného cyklu projektov, pričom sú vytvorené požiadavky na bezpečnosť na ISVS a ITVS, b) je zabezpečená bezpečný vývoj, inštalácia, konfigurácia (hardening) podľa odporúčaní výrobcu alebo dodávateľa všetkých ISVS a ITVS bez obmedzenia prevádzky zvyšných systémov, c) je zabezpečené testovanie bezpečnosti všetkých ISVS a ITVS pred ich nasadením do prevádzky.			
50.	príjme primerané procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre aplikovanie požiadaviek bezpečnosti na ISVS a ITVS pri nákupe, vývoji a údržbe systémov treťou stranou, pre zavedenie povinnosti dodržiavať vybrané bezpečnostné opatrenia treťou stranou uzavrie organizácia zmluvu s organizáciou zabezpečujúcou samotný vývoj alebo nákup	ÁNO	ÁNO	ÁNO
51.	zabezpečuje integráciu identifikovaných rizík ISVS a ITVS a navrhovaných bezpečnostných opatrení do celkového riadenia rizík v organizácii správcu		ÁNO	ÁNO
52.	sú prijaté opatrenia na zabránenie straty, poškodenia, krádeže alebo kompromitácie aktív a prerušeniu prevádzky ISVS		ÁNO	ÁNO
53.	prístup k zdrojovému kódu, vývojovým technológiám a softvérovým knižniciam na čítanie a zápis je riadený		ÁNO	ÁNO
54.	sú prijaté bezpečnostné opatrenia s požadovanými bezpečnostnými nastaveniami tak, aby konfigurácia ITVS a ISVS nebola zmenená neoprávnenými osobami		ÁNO	ÁNO
55.	pre každý projekt ITVS ustanoví osobu zodpovednú za dohľad nad plnením požiadaviek podľa vyhlášky počas trvania projektu		ÁNO	ÁNO
56.	sú určené a aplikované základné parametre pre bezpečné konfigurácie ITVS a ISVS		ÁNO	ÁNO

57.	pre každý projekt ISVS ustanoví osobu zodpovednú za dohľad nad plnením bezpečnostných požiadaviek stanovených v katalógu požiadaviek na predmet dodávky ISVS		ÁNO	ÁNO
58.	pre každý projekt ISVS ustanoví osobu zodpovednú za dohľad nad plnením zmluvných ustanovení upravujúcich riadenie bezpečnosti vo vzťahu k dodávateľovi (najmä zoznamy oprávnených osôb, pridelenie vzdialených prístupov, mlčanlivosť)		ÁNO	ÁNO
59.	je pravidelne, aspoň raz ročne vykonávaná kontrola o ktorej sa vyhotovuje záznam a aktualizácia konfigurácie ITVS a ISVS podľa vývoja hrozieb		ÁNO	ÁNO
60.	sú určené a uplatnené pravidlá bezpečného vývoja ISVS, pokiaľ tento vývoj správca vykonáva internými zdrojmi		ÁNO	ÁNO
61.	stanoví požiadavky na bezpečnosť pri integrácii nových ITVS, ISVS alebo služieb do ISVS. Tieto požiadavky by mali zahŕňať napr. kompatibilitu, vhodnú autentifikáciu, šifrovanie dát, ako aj povinnosť zdokumentovať podrobnosti súvisiace s danou integráciou		ÁNO	ÁNO
62.	určí bezpečnostné požiadavky na ISVS, ktorý ide byť obstarávaný, v súlade s požiadavkami vyplývajúcimi z aplikovateľnej legislatívy		ÁNO	ÁNO
63.	zabezpečí zahrnutie konkrétnych bezpečnostných požiadaviek do zmlúv na vývoj alebo rozvoj ISVS či do zmlúv o poskytovaní služieb (SLA) s poskytovateľmi IT služieb		ÁNO	ÁNO
64.	je automaticky odmietnuté použitie neplatných identifikátorov relácií		ÁNO	ÁNO
65.	zabezpečí vypracovanie a implementáciu bezpečnostných projektov ISVS podľa špecifikácie v prílohe č. 3 vyhlášky		ÁNO	ÁNO
66.	stanoví povinnosť riadenia rizík identifikovaných v bezpečnostných projektoch vyvíjaných alebo prevádzkovaných ISVS a zahrnie riziká do celkového systému riadenia rizík kybernetickej bezpečnosti		ÁNO	ÁNO

67.	pred nasadením nového ISVS do produkcie zabezpečí výkon externého penetračného testovania a odstránenie zistených nedostatkov a následne realizuje penetračné testovanie raz ročne		ÁNO	ÁNO
68.	sú definované a vykonávané procesy testovania bezpečnosti ITVS a ISVS		ÁNO	ÁNO
69.	sú riadené, monitorované a kontrolované činnosti súvisiace s vývojom programových prostriedkov a informačných systémov, ktoré sú dodávané treťou stranou		ÁNO	ÁNO
70.	vývojové, testovacie a produkčné prostredia sú vzájomne oddelené a zabezpečené		ÁNO	ÁNO
71.	dáta používané pre testovanie sú vhodne vybrané, chránené a spravované		ÁNO	ÁNO
72.	organizácia správcu vytvorí pre každý vyvíjaný alebo nakupovaný ISVS príslušný bezpečnostný projekt podľa § 23 zákona a prílohy č. 3. Bezpečnostný projekt predkladá organizácia správcu na schválenie orgánu vedenia pomocou vládneho informačného systému kybernetickej bezpečnosti		ÁNO	ÁNO
73.	organizácia správcu vedie zoznam všetkých projektov a podpornej dokumentácie v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
74.	je definovaný a zavedený vnútorný systém kontrol (zoznam procesno-organizačných, fyzických a technických kontrol, určenie osoby zodpovednej za výkon jednotlivých kontrol, ich periodicity a vedenie evidencie vykonaných kontrol) súvisiacich s ISVS a ITVS v oblasti kybernetickej a informačnej bezpečnosti	ÁNO	ÁNO	ÁNO
75.	riadenie kybernetickej a informačnej bezpečnosti správcu je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií		ÁNO	ÁNO

76.	súlady kybernetickej a informačnej bezpečnosti správcu s jeho bezpečnostnou dokumentáciou je prehodnocovaný najmenej raz za kalendárny rok v plánovaných intervaloch alebo pri významných zmenách procesov, ITVS alebo ISVS		ÁNO	ÁNO
77.	sú definované pravidlá pre výkon auditných činností a kontrolných činností v oblasti kybernetickej bezpečnosti		ÁNO	ÁNO
78.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany osobných údajov podľa osobitných predpisov a zmluvných požiadaviek, ak sú spracúvané v ISVS a ITVS	ÁNO	ÁNO	ÁNO
79.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany tajomstva podľa osobitných predpisov a zmluvných požiadaviek, ak sú spracúvané v ISVS a ITVS	ÁNO	ÁNO	ÁNO
80.	je zabezpečené plnenie požiadaviek na ochranu práv duševného vlastníctva a použitia patentových produktov podľa osobitných predpisov a zmluvných požiadaviek, ak sú spracúvané v ISVS a ITVS	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre kryptografické opatrenia a zásady používania kryptografie prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
81.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia pre šifrovanie komunikácie a výmenu informácií medzi organizáciou a inými subjektami, primárne však pre webové sídlo a publikované služby ISVS a ITVS	ÁNO	ÁNO	ÁNO
82.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia pre šifrovanie pevných diskov koncových zariadení a prenosných médií organizácie ISVS a ITVS	ÁNO	ÁNO	ÁNO
83.	nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov a sú dodržiavané požiadavky vyplývajúce so všeobecne záväzných právnych predpisov a požiadavky vyplývajúce zo zmlúv		ÁNO	ÁNO
84.	sú definované a zavedené pravidlá evidenciu a používanie kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov		ÁNO	ÁNO

85.	sú prijaté a aplikované postupy na pravidelné preskúmanie odolnosti zavedených kryptografických mechanizmov najmenej raz ročne		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre bezpečnosť a spôsobilosti ľudských zdrojov prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
86.	organizácia identifikuje a vedie zoznam všetkých zamestnancov, ktorí vykonávajú svoje činnosti v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
87.	sú formalizované procesy súvisiace so zaradením do pozície, zmenou pozície alebo vyradením a odobratím pozície pre používateľov, administrátorov alebo zamestnancov tretích strán zastávajúcich bezpečnostné roly	ÁNO	ÁNO	ÁNO
88.	sú určené pravidlá pre zaradenie osôb do jednotlivých pracovných rolí		ÁNO	ÁNO
89.	v pracovných zmluvách, zmluvách v súvislosti s iným obdobným pracovnoprávnym vzťahom alebo iných súvisiacich dokumentoch sú uvedené zodpovednosti za kybernetickú bezpečnosť		ÁNO	ÁNO
90.	je definovaný a zavedený systém primeraného úvodného vzdelávania a pravidelného preškolovania pre všetky roly týkajúce sa kybernetickej a informačnej bezpečnosti	ÁNO	ÁNO	ÁNO
91.	pre všetky roly je poskytované primerané vzdelávanie, aby štatutárny orgán správcu, zamestnanci správcu a tretie strany mali primerané povedomie o kybernetickej bezpečnosti v oblasti ITVS a ISVS; súčasťou školení sú aj praktické simulácie a cvičenia reakcie na kybernetické bezpečnostné incidenty	ÁNO	ÁNO	ÁNO
92.	zamestnanci organizácie správcu a tretie strany sú preukázateľne oboznámení so Zásadami bezpečného správania sa pri používaní ISVS a ITVS, postupmi pre nahlasovanie bezpečnostných incidentov, ako aj úlohami a zodpovednosťami uvedenými v príslušnej bezpečnostnej dokumentácii	ÁNO	ÁNO	ÁNO
93.	zamestnanci správcu a tretie strany sú preukázateľne oboznámení s bezpečnostnými politikami	ÁNO	ÁNO	ÁNO

94.	aktualizované verzie bezpečnostných politík sú bezodkladne sprístupňované vrcholovému vedeniu správcu, manažmentu správcu, zamestnancom správcu, a v potrebnom rozsahu aj tretej strane alebo ďalším zainteresovaným stranám		ÁNO	ÁNO
95.	sú formalizované disciplinárne procesy voči zamestnancom správcu, ktoré sa dopustili porušenia ustanovení bezpečnostných politík správcu		ÁNO	ÁNO
96.	zamestnanci organizácie správcu a tretie strany sú poučení o povinnosti zachovať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch pri správe a používaní ISVS a ITVS ešte pred získaním prístupu, pričom táto mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činností	ÁNO	ÁNO	ÁNO
97.	sú určené, zdokumentované a pravidelne, najmenej raz za dva roky, preskúmané a podpisované dohody o mlčanlivosti, ktoré odrážajú potreby správcu pre zachovanie dôvernosti	ÁNO	ÁNO	ÁNO
98.	ak zamestnanci pracujú na diaľku, sú prijaté bezpečnostné opatrenia na ochranu informácií a služieb, ku ktorým sa pristupuje, ktoré sa využívajú alebo spracúvajú alebo ktoré sa uchovávali mimo priestorov správcu	ÁNO	ÁNO	ÁNO
99.	sa používa viacfaktorové overovanie pre vzdialený prístup		ÁNO	ÁNO
100.	sú formalizované disciplinárne procesy voči zamestnancom organizácie správcu a tretích strán, ktorí sa dopustili porušenia ustanovení uvedených v bezpečnostnej dokumentácii	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre správu identít a prístupov prijíma správca tak, že:	Kat. I	Kat. II	Kat. III

101.	je definovaný, zavedený a kontrolovaný systém riadenia identít a prístupov organizácie správcu, ktorý obsahuje: - zoznam systémov a spôsob riadenia lokálnych identít a centrálne riadených identít používateľom a tretím stranám, - zoznam a jednotlivé typy identít a používateľov, technických účtov a administrátorami naprieč systémami, - spôsoby identifikácie a autentifikácie používateľov v jednotlivých systémoch, - zoznamy autorizácií a konfliktných oprávnení, pre všetky ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie správcu, najmä: a) sú určené, uplatnené a kontrolované pravidlá jedinečných a personalizovaných identifikátorov b) sú určené, uplatnené a kontrolované pravidlá autentifikačných mechanizmov c) sú určené, uplatnené a kontrolované pravidlá pridelenia autorizácií a oprávnení	ÁNO	ÁNO	ÁNO
102.	organizácia správcu vedie zoznam všetkých používateľov, ich identifikátorov a autorizácií v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
103.	organizácia správcu určí, zavedie a používa mechanizmy a nástroje na riadenie identít a prístupov pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
104.	pri riadení prístupov k ITVS a ISVS sú využívané technológie na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a technológie na riadenie prístupových oprávnení, prostredníctvom ktorých je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení, prostredníctvom ktorých sa zaznamenáva použitie prístupových oprávnení		ÁNO	ÁNO
105.	je zaručené riadenie jednoznačných identifikátorov používateľov a systémov vrátane prístupových práv a oprávnení používateľských účtov a systémových účtov, počas celého životného cyklu identít		ÁNO	ÁNO

106.	každému používateľovi a systémovému účtu je pridelený jednoznačný identifikátor na autentizáciu na prístup do siete a ISVS		ÁNO	ÁNO
107.	v pravidelných intervaloch, najmenej raz ročne je vykonávaná kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom vykonávania oprávnení, vrátane detekcie a následného zneplatnenia nepoužívaných prístupových účtov; vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia		ÁNO	ÁNO
108.	je zavedené riadenie prístupov na základe rolí a zásady najnižších oprávnení pre používateľov		ÁNO	ÁNO
109.	privilegované prístupové práva sú poskytované len oprávneným používateľom, komponentmi ITVS a ISVS a službám podľa príslušnej politiky riadenia prístupov a práv		ÁNO	ÁNO
110.	prístup k aktívam je obmedzený v súlade s určenou a definovanou politikou riadenia prístupov		ÁNO	ÁNO
111.	technológie a postupy bezpečnej autentizácie sú zavedené na základe požiadaviek na obmedzenie prístupu k informáciám podľa príslušnej politiky riadenia prístupov a práv		ÁNO	ÁNO
112.	používatelia majú prijaté primerané opatrenia na ochranu a udržiavanie pridelených autentifikačných prostriedkov, vrátane nezdieľania autentifikačných prostriedkov s inými osobami		ÁNO	ÁNO
113.	všetky prístupy do ITVS a ISVS z nedôveryhodných zdrojov sú riadené a monitorované		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre bezpečnosť pri prevádzke sietí a informačných systémov verejnej správy prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
114.	sú určené, uplatnené a kontrolované pravidlá bezpečnej prevádzky pre všetky ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie, najmä	ÁNO	ÁNO	ÁNO

	a) je určená osoba v pozícií IT administrátora systému, ktorá zodpovedá za prevádzku samotného systému pre každý ISVS a ITVS. IT administrátor má znalosti a schopnosti udržiavať systémy s prípadnými príslušnými informáciami uvedenými v ITVS prevádzkovej dokumentácii, príručkách alebo manuáloch, b) je zabezpečené prepojenie procesov vedenia aktív, riadenia rizík a zmenového konania počas prevádzky ISVS a ITVS, c) je zabezpečené pravidelné sledovanie a vyhodnocovanie aktivít tretej strany pri prevádzke ISVS a ITVS, ak je IT administrátorom pre systém dodávateľ alebo tretia strana			
115.	prevádzkové postupy pre zariadenia na spracovanie informácií, siete a informačné systémy sú zdokumentované a sprístupnené zamestnancom podľa ich potreby		ÁNO	ÁNO
116.	sa zabráňuje strate, poškodeniu alebo ohrozeniu aktív alebo prerušeniu prevádzky v dôsledku zlyhania a narušenia podporných služieb, vrátane dodávky elektrickej energie a funkčných dátových liniek		ÁNO	ÁNO
117.	sa zabráňuje úniku informácií zo zariadení, ktoré sa majú zlikvidovať alebo opätovne použiť; všetky prvky zariadení obsahujúce pamäťové médiá sa kontrolujú, čím sa zabezpečí, že informácie a licencovaný softvér sú bezpečne zmazané alebo prepísané ešte pred vyradením alebo opätovným použitím zariadení		ÁNO	ÁNO
118.	je dostupná dostatočná kapacita podporných aktív, ktorá je priebežne monitorovaná spôsobom v závislosti od typu aktíva		ÁNO	ÁNO
119.	systémový čas príslušných podporných aktív, ktoré spracúvajú informácie alebo podporujú ich spracovanie je synchronizovaný so schválenými zdrojmi času, zohľadňujúcimi časové zóny		ÁNO	ÁNO
120.	používanie systémových programových prostriedkov, ktoré môžu byť schopné obísť systémové a aplikačné opatrenia je obmedzené a kontrolované		ÁNO	ÁNO
121.	sú zavedené postupy a opatrenia na bezpečné riadenie inštalácie programových prostriedkov a informačných systémov do produkčnej prevádzky		ÁNO	ÁNO

122.	zmeny procesov a systémov podliehajú schválenému procesu riadenia zmien		ÁNO	ÁNO
123.	aktualizuje príslušný bezpečnostný projekt pre ISVS pri všetkých významných zmenách implementovaných na úrovni systému.		ÁNO	ÁNO
124.	každý nový prvok ITVS alebo ISVS projekt, nový alebo aktualizovaný ISVS, budú evidované v evidencii aktív a premietnuté do príslušnej bezpečnostnej dokumentácie vedenej podľa tejto vyhlášky		ÁNO	ÁNO
125.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie nástrojov umelej inteligencie a riadená kybernetická bezpečnosť pri používaní umelej inteligencie		ÁNO	ÁNO
126.	je definovaný a zavedený proces riadenia výnimiek zo schválených bezpečnostných opatrení		ÁNO	ÁNO
127.	vedie zoznam všetkých zmenových konaní a podpornej dokumentácie v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre ochranu proti škodlivému kódu a nežiaducemu obsahu prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
128.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia pre aktíva organizácie (servery, koncové zariadenia, mobilné zariadenia) s aktívnym prístupom používateľov alebo publikované do internetu, ktoré prístupujú ku všetkým ISVS a ITVS	ÁNO	ÁNO	ÁNO
129.	je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov	ÁNO	ÁNO	ÁNO
130.	je zavedená pravidelná aktualizácia ITVS a ISVS s cieľom zabezpečiť minimálne narušenie bežnej prevádzky		ÁNO	ÁNO
131.	prístup k externým internetovým zdrojom je riadený s cieľom znížiť vystavenie prvkov ISVS a ITVS škodlivému obsahu		ÁNO	ÁNO

Položka	Bezpečnostné opatrenia pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
132.	je definovaná a zavedená fyzická alebo logická segmentácia a rozdelenie siete organizácie v rámci správy ISVS a ITVS s rovnakým účelom a bezpečnostnými opatreniami	ÁNO	ÁNO	ÁNO
133.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia na ochranu sieťového perimetra organizácie vo všetkých logických lokalitách, v ktorých sú umiestnené všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
134.	sú vypracované a zavedené postupy na prenos informácií v rámci organizácie, ako aj s tretími stranami pre všetky typy technických prostriedkov a médií		ÁNO	ÁNO
135.	na ITVS a ISVS, ktoré spracúvajú, uchovávajú alebo prenášajú chránené informácie podľa klasifikácie informácií, sa aplikujú opatrenia na prevenciu úniku informácií, vrátane zohľadnenia proprietárnych protokolov a dátových tokov; identifikácia vybraných informácií prebieha pomocou klasifikácie informácií		ÁNO	ÁNO
136.	sú určené, zavedené a monitorované bezpečnostné funkcie, úrovne služieb a požiadavky týkajúce sa sieťových služieb		ÁNO	ÁNO
137.	je definovaná a zavedená segmentácia sietí, pričom informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente sú len informačné systémy s podobným účelom		ÁNO	ÁNO
138.	sú prijaté a udržiavané mechanizmy na smerovanie a filtráciu sieťovej prevádzky do a z externých sietí cez sieťový firewall		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre monitorovanie, zaznamenávanie a hlásenie udalostí prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
139.	je definovaný, zavedený a kontrolovaný systém zberu logov a monitorovania kybernetickej a informačnej bezpečnosti organizácie, ktorý obsahuje: - zoznam systémov, v ktorých dochádza ku tvorbe a zberu logov, - typy a obsah zbieraných logov a informácií zo systémov,	ÁNO	ÁNO	ÁNO

	- postupy na sledovanie a uchovávanie logov pri prevádzke všetkých ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie			
140.	uchováva vybrané logy v rámci správy ISVS a ITVS pre potreby spätného dohľadania udalostí	ÁNO	ÁNO	ÁNO
141.	určí, zavedie a používa mechanizmy a nástroje na zber a uchovávanie logov a monitoring pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
142.	sú vytvárané a najmenej 12 mesiacov uchovávané relevantné prevádzkové a bezpečnostné logy, ktoré zachytávajú činnosti, výnimky, poruchy a iné relevantné prevádzkové a bezpečnostné udalosti, pričom bude zabránené zmene ich integrity a neoprávneným prístupom k nim		ÁNO	ÁNO
143.	záznamy o činnostiach obsahujú informáciu o pôvodcovi vykonanej činnosti		ÁNO	ÁNO
144.	siete, informačné systémy, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí		ÁNO	ÁNO
145.	siete, ISVS, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí automatizovaným spôsobom			ÁNO
Položka	Bezpečnostné opatrenia pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
146.	identifikuje a vedie zoznam všetkých lokalít kde sa prevádzkuje alebo používa akýkoľvek prvok ISVS a ITVS	ÁNO	ÁNO	ÁNO
147.	sú definované a zavedené procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre lokality, v ktorých sú fyzicky umiestnené centrálné serverové prvky všetkých ISVS a ITVS	ÁNO	ÁNO	ÁNO

148.	sú definované a zavedené procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre lokality organizácie, v ktorých používatelia prístupujú logicky ku všetkým ISVS a ITVS	ÁNO	ÁNO	ÁNO
149.	sú definované a používané bezpečnostné perimetre na ochranu oblastí, ktoré obsahujú aktíva pre ITVS a ISVS		ÁNO	ÁNO
150.	priestory, v ktorých sa nachádzajú riadiace a serverové súčasti ITVS a ISVS majú definované pravidlá fyzickej bezpečnosti		ÁNO	ÁNO
151.	fyzický prístup k určeným aktívam správcu, ktoré sú významné z hľadiska bezpečnosti a prevádzky ISVS je povolený výhradne autorizovaným osobám		ÁNO	ÁNO
152.	je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení		ÁNO	ÁNO
153.	zabezpečené priestory sú nepretržite monitorované z hľadiska neoprávneného fyzického prístupu		ÁNO	ÁNO
154.	sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu		ÁNO	ÁNO
155.	sú monitorované a vizuálne zaznamenávané všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu			ÁNO
156.	je navrhnutá a zavedená ochrana pred fyzickými hrozbami a environmentálnymi hrozbami ako sú prírodné katastrofy a iné úmyselné alebo neúmyselné ohrozenia ITVS a ISVS		ÁNO	ÁNO
157.	sú vypracované a pravidelne aktualizované zásady bezpečného správania sa pri používaní ISVS a ITVS, ktoré obsahujú súhrn povinností a oprávnení v oblasti kybernetickej a informačnej bezpečnosti pre koncových používateľov	ÁNO	ÁNO	ÁNO
158.	aktíva v zabezpečených priestoroch sú chránené pred poškodením a neoprávneným zásahom zo strany zamestnancov pracujúcich v týchto priestoroch a zo strany nepovolaných osôb		ÁNO	ÁNO

159.	sú definované a primerane presadzované pravidlá čistého stola pre listinné dokumenty a prenosné pamäťové médiá a pravidlá pre čisté obrazovky zariadení na spracovanie informácií		ÁNO	ÁNO
160.	sú riadené riziká vyplývajúce z hrozieb fyzického prostredia a z neoprávneného fyzického prístupu k aktívam		ÁNO	ÁNO
161.	sa prijímajú opatrenia na zabránenie straty, poškodenia, krádeže alebo kompromitácii zariadení používaných, prenášaných a uchovávaných mimo pracoviska a sú definované postupy ak k takejto udalosti dôjde		ÁNO	ÁNO
162.	pamäťové médiá a údaje na nich sú zabezpečené počas ich životného cyklu, t. j. počas ich získavania, používania, prepravy a likvidácie v súlade s klasifikačnou schémou a požiadavkami na manipuláciu s nimi		ÁNO	ÁNO
163.	dáta uložené v koncových zariadeniach používateľov spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich sú chránené		ÁNO	ÁNO
164.	informácie uložené v ITVS a ISVS sú vymazané, ak už nie sú potrebné		ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre ochranu záznamov, súkromia a označovanie informácií prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
165.	je definovaná a zavedená klasifikácia informácií v organizácii a príslušné klasifikačná stupnica. Organizácia správcu klasifikuje informácie spracúvané v ISVS a ITVS na úrovni systémov	ÁNO	ÁNO	ÁNO
166.	informácie sú klasifikované na základe potrieb správcu a na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán		ÁNO	ÁNO
167.	preskúma a reviduje klasifikačné stupne informácií organizácie spracúvaných v ISVS a ITVS najmenej raz ročne a v závislosti od výsledkov vykoná preskúmanie súvisiacich rizík aj revíziu prijatých bezpečnostných opatrení	ÁNO	ÁNO	ÁNO

168.	sú preukázateľne zabezpečené primerané bezpečnostné opatrenia na ochranu informácií v organizácií pre všetky ISVS a ITVS na základne klasifikácie informácií v celom životnom cykle spracúvania informácie	ÁNO	ÁNO	ÁNO
169.	sú vypracované a zavedené postupy na označovanie informácií v súlade s prijatou klasifikačnou schémou		ÁNO	ÁNO
170.	je zabezpečený súlad so všeobecne záväznými právnymi predpismi a zmluvnými požiadavkami týkajúcimi sa práv duševného vlastníctva a používania patentovaných produktov		ÁNO	ÁNO
171.	záznamy sú chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným zverejnením		ÁNO	ÁNO
172.	sú preukázateľne zabezpečené primerané technické a organizačné opatrenia na ochranu osobných údajov v organizácií pre všetky ISVS a ITVS, ktoré spracúvajú osobné údaje	ÁNO	ÁNO	ÁNO
Položka	Bezpečnostné opatrenia pre dodávateľský reťazec prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
173.	identifikuje a vedie zoznam všetkých dodávateľov a tretích strán, ktorí podporujú organizáciu pri vývoji, nákupe, údržbe, prevádzke a riadení kybernetickej a informačnej bezpečnosti pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
174.	počas procesu obstarávania nového dodávateľa alebo tretej strany preskúma identifikované riziká tretej strany vo vzťahu k nákupu, vývoju alebo prevádzke všetkých ISVS a ITVS a uvedie tieto riziká ako súčasť analýzy rizík	ÁNO	ÁNO	ÁNO
175.	je definovaný a zavedený systém určenia kritickosti dodávateľa a tretej strany organizácie správcu, ktorý obsahuje: - metodiku pre určenie kritického dodávateľa a tretej strany podľa tejto vyhlášky, - samotné určenie kritickosti dodávateľa a tretej strany podporujúcej ISVS a ITVS	ÁNO	ÁNO	ÁNO
176.	na základe výsledkov preskúmania rizík dodávateľa prijme primerané procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre celý subdodávateľský	ÁNO	ÁNO	ÁNO

	reťazec. Pre zavedenie povinnosti dodržiavať vybrané bezpečnostné opatrenia treťou stranou sa uzavrie zmluva s dodávateľom (treťou stranou)			
177.	sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán		ÁNO	ÁNO
178.	na riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami je s každou treťou stranou s významným vplyvom uzatvorená zmluva		ÁNO	ÁNO
179.	bezpečnostné opatrenia sú uplatnené v dodávateľskom reťazci produktov a služieb, ktorý priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky ITVS a ISVS správcu		ÁNO	ÁNO
180.	vykoná raz ročne posúdenie rizík dodávateľov s významným vplyvom a účinnosti príslušných bezpečnostných opatrení definovaných v zmluvách s dodávateľmi. V závislosti od výsledkov vykoná organizácia aj aktualizáciu určenia kritickosti dodávateľov a revíziu prijatých bezpečnostných opatrení definovaných v zmluvách	ÁNO	ÁNO	ÁNO
181.	sú pravidelne, najmenej raz za dva roky monitorované, preskúvané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky ITVS a ISVS správcu		ÁNO	ÁNO
182.	sú vypracované, aktualizované a účinné ITVS a ISVS prevádzkové zmluvy (tzv. SLA) s príslušnými bezpečnostnými opatreniami vzťahujúcimi sa na dodávateľov a tretie strany		ÁNO	ÁNO
183.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie cloudových služieb a riadená kybernetická a informačná bezpečnosť pri používaní cloudových služieb		ÁNO	ÁNO

Vysvetlivky:

ITVS - informačnou technológiou verejnej správy

ISVS - je informačný systém verejnej správy

OBSAH A ŠTRUKTÚRA BEZPEČNOSTNÉHO PROJEKTU INFORMAČNÉHO SYSTÉMU VEREJNEJ SPRÁVY

- (1) Pri spracovaní bezpečnostného projektu informačného systému verejnej správy sa prihliada najmä na zložitosť informačného systému verejnej správy, komplexnosť agendy pokrytej informačným systémom verejnej správy a stanovené bezpečnostné požiadavky na informačný systém verejnej správy. Zohľadniť sa musia taktiež bezpečnostné požiadavky na informačný systém verejnej správy vyplývajúce z tejto vyhlášky.
- (2) Bezpečnostný projekt informačného systému verejnej správy pozostáva z dvoch hlavných výstupov: bezpečnostného zámeru a analýzy bezpečnosti. Jednotlivé výstupy sa vypracúvajú v určenom poradí a sú priebežne spracúvané počas celého projektu informačného systému verejnej správy realizovaného v súlade so zákonom.
- (3) Ako prvý výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje dokument bezpečnostný zámer. Bezpečnostný zámer určuje najmä kontext a zameranie bezpečnostného projektu, preto obsahuje najmenej
 - a) formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov správcu, technických noriem a štandardov dobrej praxe,
 - b) zoznam právnych predpisov, ako aj interných riadiacich aktov správcu, aplikovaných v bezpečnostnom projekte,
 - c) rámcový opis metodického prístupu ku kvalitatívnej analýze rizík, ktorá bude v bezpečnostnom projekte vykonaná,
 - d) rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu správcu,
 - e) vymedzenie okolia informačného systému verejnej správy a jeho vzťah k možnému narušeniu bezpečnosti informačného systému verejnej správy vrátane zoznamu integrácií informačného systému verejnej správy,
 - f) vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
 - g) ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo bezpečnostného projektu informačného systému verejnej správy),
 - h) postupy revízie alebo aktualizácie bezpečnostného zámeru.
- (4) Ako hlavný výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje 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 informačného systému verejnej správy a jeho okolia. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so

zákonom a priamo nadväzuje na dokument bezpečnostný zámer. Analýza rizík pozostáva z výkonu týchto činností:

- a) vytvorenie podkladových katalógov určených na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu následkov,
 - b) identifikácia realizovaných existujúcich bezpečnostných opatrení v štruktúre podľa oblastí bezpečnosti ustanovených osobitným predpisom,⁶⁾
 - c) identifikácia rizík a opis analyzovaných scenárov rizík v štruktúre podľa oblastí bezpečnosti ustanovených osobitným predpisom,⁷⁾
 - d) priradenie aktív, hrozieb, zraniteľností a následkov ku každému z identifikovaných scenárov rizík,
 - e) vyhodnotenie rizík kombináciou pravdepodobnosti realizácie scenáru rizika a závažnosti následkov,
 - f) opis navrhovaných bezpečnostných opatrení pre každé identifikované riziko, ktoré nie je akceptovateľné.
- (5) Pri každom scenári rizika sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny následok na aktíva ISVS a správcu. Odhad pravdepodobnosti realizácie scenára rizika je vykonaný kvalitatívnou formou. Pri hodnotení závažnosti výsledného následku sa zohľadňuje celková závažnosť následkov, ktoré môžu byť spôsobené realizáciou rizika. Vyhodnotenie závažnosti následkov pri realizácii scenára rizika je vyjadrené kvalitatívnou formou tak, aby bolo možné následne stanoviť výslednú hodnotu rizika. Úroveň následkov sa určuje osobitne pre každé analyzované riziko a zahŕňa všetky aktíva dotknuté príslušným scenárom rizika. Analyzované riziko môže mať na aktíva správcu viaceré následky, ktoré je potrebné sumárne vyhodnotiť. Výsledná hodnota rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.
- (6) Postup výkonu analýzy rizík musí byť v súlade s technickou normou STN ISO/IEC 27005 a metodikou ministerstva investícií. Výsledné vyhodnotenie rizík podľa použitej metodiky musí byť možné premietnuť do stupnice metodiky podľa § 5 ods. 1 písm. c).
- (7) Cieľom návrhu bezpečnostných opatrení je vytvorenie takého okruhu bezpečnostných opatrení, že po ich implementácii a následnom prehodnotení rizík sú všetky zvyškové riziká akceptovateľné. Pri niektorých typoch opatrení je prípustné sa odkazovať aj na dokumentáciu k informačnému systému verejnej správy v súlade so zákonom. Opis navrhovaných bezpečnostných opatrení zohľadňuje
- a) opatrenia a požiadavky ustanovené touto vyhláškou alebo osobitným predpisom,
 - b) spôsob uplatňovania bezpečnostných opatrení v konkrétnych podmienkach správcu a analyzovaného informačného systému verejnej správy,
 - c) dostupné možnosti prístupu k riadeniu rizika.
- (8) Výstupný dokument analýzy bezpečnosti s výsledkami analýzy rizík obsahuje najmä
- a) ciele a priority analýzy rizík,

⁶⁾ § 20 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

⁷⁾ § 20 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

- b) stručný opis použitej metodiky analýzy rizík,
 - c) opis scenárov rizík založený na identifikácii aktív, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností a na identifikácii následkov zohľadňujúcich stratu dôvernosti, integrity a dostupnosti aktív správcu,
 - d) vyhodnotenie rizík podľa použitej metodiky,
 - e) opis navrhovaných bezpečnostných opatrení pre identifikované riziká v závislosti od ich závažnosti,
 - f) celkové zhrnutie výsledkov analýzy rizík usporiadaných podľa závažnosti,
 - g) postupy revízie alebo aktualizácie analýzy bezpečnosti.
- (9) Štruktúra výstupu analýzy bezpečnosti musí pokryť minimálne oblasti bezpečnosti ustanovené osobitným predpisom.⁸⁾ Finalizácia dokumentácie bezpečnostného projektu informačného systému verejnej správy je realizovaná v etape IMPLEMENTÁCIA A TESTOVANIE v súlade so zákonom.

⁸⁾ § 20 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

**SYSTÉMOVÉ INFORMÁCIE Z INFORMAČNÝCH TECHNOLOGIÍ VEREJNEJ
SPRÁVY ZASIELANÉ ORGÁNU VEDENIA PRE ÚČELY RIADENIA
KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI**

Kategória I

(1) Základné údaje o správcovi

- a) názov organizácie,
- b) meno a priezvisko správcu,
- c) adresa správcu,
- d) kontaktné údaje správcu,
- e) typ správcu.

(2) Kontaktné údaje pre roly

- a) meno a priezvisko kontaktnej osoby,
- b) e-mailový kontakt,
- c) telefónny kontakt,
- d) priradenie roly osoby (manažér kybernetickej bezpečnosti, príjemca hlásení z CSIRT-u, vedúci IT, pracovník IT, štatutár organizácie, iné),
- e) dostupnosť kontaktu (napríklad 8x5, 24x7).

(3) IPv4 adresy

- a) IPv4 adresa alebo rozsah IPv4 adries (adresa siete alebo dĺžka masky),
- b) účel použitia danej adresy (adresy).

(4) IPv6 adresy

- a) IPv6 adresa alebo rozsah IPv6 adries (prefix alebo dĺžka),
- b) účel použitia danej adresy (adresy).

(5) Doménové mená

- a) doménové meno,
- b) priradená IPv4 adresa,
- c) priradená IPv6 adresa,

d) účel použitia doménového mena.

Kategória II a Kategória III

(6) Sieťové služby

- a) názov služby,
- b) doménové meno služby,
- c) IPv4 a IPv6 (ak sa používa) adresa služby,
- d) URL služby (pre služby na báze HTTP(S)),
- e) čísla portov a transportné protokoly,
- f) siete, z ktorých je služba prístupná (napríklad internet, GOVNET),
- g) popis služby,
- h) ID služby alebo príslušného informačného systému v MetaIS,
- i) klasifikácia služby podľa dôvernosti, integrity, dostupnosti (číselníkové položky),

(7) Informácie o softvérovom vybavení správcu

- a) typ softvéru (operačný systém, aplikačný softvér, firmvér hardvéru, systémy umelej inteligencie (AI), modely AI na všeobecné účely,⁹⁾ iné – číselníková položka),
- b) názov softvéru vrátane systému AI, modelu AI na všeobecné účely,
- c) verzia softvéru vrátane systému AI, modelu AI na všeobecné účely (vrátane posledného tréningu alebo verzie, ak je dostupná),
- d) ID softvéru (podľa číselníka softvéru),
- e) počet inštancií softvéru vrátane systému AI, modelu AI na všeobecné účely,
- f) informácia, či je daný softvér vrátane systému AI, modelu AI na všeobecné účely použitý aj na systémoch prístupných z externých sietí,
- g) účel a rozsah použitia systému AI a modelu AI na všeobecné účely (napríklad spracovanie údajov, rozhodovacia podpora, kybernetická bezpečnosť, automatizácia procesov).

(8) Informácie o aktívach správcu

- a) ID aktíva,

⁹⁾ Čl. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, 2024/1689, 12.7.2024).

- b) názov aktíva,
- c) typ aktíva,
- d) popis aktíva,
- e) IP adresa,
- f) MAC adresa (voliteľné),
- g) správca,
- h) prevádzkovateľ.

(9) Parametre a výsledky realizácie

- a) analýzy vplyvov na prevádzkovanie (business impact assessment).
- b) určenie cieľovej doby obnovy a cieľového bodu obnovy

(10) Evidencia kybernetických bezpečnostných incidentov

- a) dátum zistenia, aspoň predpokladaný dátum vzniku, časové údaje priebehu, dĺžka trvania,
- b) geografické rozšírenie,
- c) počet zasiahnutých používateľov,
- d) detailný opis priebehu,
- e) rozsah vzniknutých škôd (aspoň odhad),
- f) zasiahnuté služby, informačné systémy a informačné technológie verejnej správy,
- g) konkrétny popis všetkých zasiahnutých aktív,
- h) popis vplyvu kybernetického bezpečnostného incidentu na stupeň narušenia podľa písmena d) a detailný opis priebehu podľa písmena e),
- i) stav riešenia,
- j) vykonané nápravné opatrenia,
- k) opis následkov,
- l) správa o riešení incidentu,
- m) prijaté bezpečnostné opatrenia kybernetického bezpečnostného incidentu.

(11) Odpovede na otázky v dotazníkoch

- a) identifikácia dotazníka,
- b) identifikácia otázky,

- c) kód odpovede,
- d) hodnota odpovede.“.

KLASIFIKAČNÁ SCHÉMA

Kritériá klasifikácie informácií

Klasifikačné stupne

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktívum“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a vyjadrujú dôležitosť alebo hodnotu týchto aktív pre výkon činností správcu.

1. Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

- a) verejné informačné aktívum určené pre verejnosť, ktoré je získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne zverejnené informácie alebo všeobecne dostupné informácie,
- b) interné informačné aktívum, ktoré je používané a prístupné pre všetkých používateľov v rámci organizácie správcu bez ohľadu na ich rolu; na sprístupnenie týchto aktív tretím stranám alebo verejnosti je potrebné schválenie zo strany vlastníka informácie,
- c) chránené informačné aktívum, ktoré je používané a prístupné len určeným skupinám oprávnených osôb a ktorej neautorizované odhalenie, prezradenie alebo zničenie môže mať pre správcu negatívny vplyv na výkon činností; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,
- d) prísne chránené informačné aktívum, ktoré je používané a prístupné len jednotlivým vybraným zamestnancom správcu a ktorého neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na aktíva a procesy správcu; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilegií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretia strana má k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

Ak nie je informačné aktívum explicitne klasifikované, je považované za interné.

2. Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

- a) nízka zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí výkon činností správcu,

- b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre výkon činností správcu a ktorých chyba alebo nepresnosť môže spôsobiť negatívny vplyv na kontinuitu činností správcu a jeho oblasť pôsobenia,
- c) vysoká zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre výkon činností správcu a ktorých chyba, nepresnosť bezprostredne ohrozuje výkon činností, s ňou spojené aktivity a dobrú povesť správcu.

3. Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

- a) nízka zahŕňa informačné aktíva správcu, ktorých výpadok výrazne neohrozí výkon činností správcu alebo pre ktoré existujú alternatívne postupy,
- b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre výkon činností správcu a ktorých zlyhanie môže mať vplyv na kontinuitu činností správcu a jeho oblasť pôsobenia,
- c) vysoká zahŕňa vybrané informačné aktíva, ktoré sú kritické pre výkon činností správcu a ktorých zlyhanie bezprostredne ohrozuje výkon činností správcu a jeho dobré meno.

Základné pravidlá klasifikácie informácií

- a) každá klasifikovaná informácia má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti,
- b) bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia informačných aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú,
- c) správca môže v rozsahu svojej pôsobnosti jednotlivé informačné aktíva zaradiť do vyššieho stupňa v zmysle definícií stupňov.

