ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2025

Vyhlásené: 28. 8. 2025 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

227

VYHLÁŠKA
Národného bezpečnostného úradu
z 26. augusta 2025
o bezpečnostných opatreniach

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 32 ods. 1 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) ustanovuje:

§ 1

Táto vyhláška ustanovuje obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete a informačné systémy a operačné technológie a obsah a štruktúru bezpečnostnej dokumentácie podľa § 20 zákona.

§ 2

Na účely tejto vyhlášky sa rozumie

a) aktívom hmotný alebo nehmotný komponent informačnej architektúry, ktorý má pre prevádzkovateľa základnej služby hodnotu, najmä služby, procesy, informácie alebo údaje,

b) primárnym aktívom aktívum, ktoré je nevyhnutné na dosiahnutie cieľov prevádzkovateľa základnej služby,

c) podporným aktívom aktívum, na ktorom je závislé jedno alebo viacero primárnych aktív,

d) bezpečnostnou politikou dokumentácia, ktorá určuje smerovanie prevádzkovateľa základnej služby v oblasti kybernetickej bezpečnosti na úrovni riadenia a určuje povinnosti, zodpovednosti, požiadavky, zákazy a zásady správania sa v jednotlivých oblastiach kybernetickej bezpečnosti,

e) bezpečnostným štandardom súbor pravidiel spojených s kybernetickou bezpečnosťou, ktoré jednotne interpretujú požiadavky bezpečnostných politík v konkrétnych situáciách, určujú aktivity, hlavné pravidlá, zodpovednosti a organizáciu riadenia kybernetickej bezpečnosti a ktorých účelom je vytvorenie jednotného prostredia pre dodržiavanie bezpečnostných politík.

§ 3

(1) Bezpečnostné opatrenia tvoria opatrenia podľa § 20 ods. 4 zákona, ktoré sú minimálne bezpečnostné opatrenia a

a) opatrenia pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona, alebo

b) sektorové bezpečnostné opatrenia, ak sú ustanovené.

(2) Rozsah všeobecných bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona je uvedený v prílohe č. 1 a určuje sa na základe analýzy rizík.

§ 4

(1) Bezpečnostná dokumentácia obsahuje

a) schválenú stratégiu kybernetickej bezpečnosti určujúcu ciele, ktoré je potrebné v riadení kybernetickej bezpečnosti dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za systémy manažérstva, riadenie rizík a aktualizáciu bezpečnostnej dokumentácie,

b) schválené bezpečnostné politiky pre jednotlivé oblasti riadenia kybernetickej bezpečnosti vrátane opisu súvisiacej organizačnej štruktúry, procesov a väzieb, pracovných rolí, zodpovednosti a delenia právomocí a opisu rámca riadenia bezpečnostných rizík,

c) vykonanú klasifikáciu informácií podľa prílohy č. 2; ak prevádzkovateľ základnej služby disponuje vlastnou metodikou pre klasifikáciu informácií, vykoná sa mapovanie na klasifikačné stupne v súlade s prílohou č. 2,

d) určenie sietí a informačných systémov a operačných technológií do príslušnej kategórie informačných a komunikačných technológií alebo operačných technológií; v prípade nejednoznačnosti rozhodne o určení kategórie prevádzkovateľ základnej služby,

e) vykonanú analýzu rizík a určenie úrovne identifikovaných rizík, akceptovaných rizík a zvyškových rizík pre aktíva spolu so zoznamom aktív,

f) zadokumentované určenie rozsahu a spôsobu prijatia, dodržiavania a vykonávania bezpečnostných opatrení vrátane odôvodnenia neprijatia bezpečnostného opatrenia podľa § 5 ods. 1 písm. e),

g) poslednú záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti (ďalej len „audit“) podľa § 29 zákona,

h) iné dokumenty, ak to ustanovuje osobitný predpis.[1])

(2) Zadokumentované určenie rozsahu a spôsobu podľa odseku 1 písm. f) obsahuje najmä zoznam prijatých a neprijatých bezpečnostných opatrení a s nimi súvisiace schémy a základné opisy

a) topológie a infraštruktúry operačných technológií,

b) topológie a infraštruktúry informačných a komunikačných technológií,

c) súvisiacej aplikačnej architektúry,

d) súvisiacej bezpečnostnej architektúry.

§ 5

(1) Riadenie rizík obsahuje

a) identifikáciu aktív postupmi podľa § 6,

b) identifikáciu rizík, ktorej súčasťou je aj opis prijatých a vykonávaných bezpečnostných opatrení,

c) analýzu rizík; ak prevádzkovateľ základnej služby disponuje vlastnou bezpečnostnou metodikou, vykoná sa mapovanie na úrovne rizika v súlade so štruktúrou uvedenou v bezpečnostnej metodike zverejnenej na webovom sídle úradu,

d) hodnotenie rizík,

e) prijatie bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú prijaté a ktoré bezpečnostné opatrenia nie sú prijaté spolu s odôvodnením,

f) preskúmavanie identifikovaných rizík najmenej raz ročne a v závislosti od výsledkov aj aktualizáciu rizík a revíziu prijatých bezpečnostných opatrení.

(2) Súčasťou riadenia rizík je analýza funkčného vplyvu, ktorá pozostáva z hodnotenia vplyvu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby alebo spôsobiť ohrozenie alebo narušenie kontinuity jeho služieb. Súčasťou analýzy funkčného vplyvu je určenie cieľovej doby obnovy a cieľového bodu obnovy.

(3) Určenie úrovne identifikovaného rizika sa vykoná vopred nastaveným súborom pravidiel, ktoré umožnia určiť vopred definované úrovne rizika pre najhoršie scenáre. Na určenie úrovne identifikovaného rizika podľa prvej vety sa použijú štandardné a rovnaké metodické postupy.

(4) Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých aktív, kybernetických hrozieb, zraniteľností a ich následkov ako sled alebo kombinácia udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku kybernetického bezpečnostného incidentu.

(5) Pre potreby analýzy rizík sa prvky zoznamov aktív, hrozieb, zraniteľností a následkov môžu združiť do jednotlivých skupín; tieto skupiny je možné použiť univerzálne pre identifikované scenáre.

(6) Analýzou rizík podľa odseku 1 písm. c) sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnymi hrozbami v spojitosti s existujúcimi bezpečnostnými opatreniami. V rámci analýzy rizík sú identifikované následky pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

(7) Výsledky analýzy rizík a návrhy bezpečnostných opatrení v nadväznosti na identifikované riziká preukázateľným spôsobom schvaľuje osoba podľa § 20 ods. 4 písm. h) zákona.

§ 6

(1) Aktívum sa identifikuje a vedie v evidencii aktív. Evidencia aktív sa skladá z identifikovateľných primárnych aktív a podporných aktív.

(2) Aktíva sa identifikujú tak, že sú jednoznačne určené hranice jednotlivých sietí a informačných systémov a rozhrania medzi určenými hranicami.

(3) Evidencia aktív je centralizovane riadená a zodpovedá aktuálnemu stavu.

(4) 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.

(5) Evidencia aktív obsahuje najmä identifikáciu a evidenciu

a) primárnych aktív,

b) podporných aktív,

c) vlastníkov aktív,

d) zodpovedných osôb za identifikáciu a evidenciu aktív.

(6) Podporné aktívum, ktoré súvisí s viacerými primárnymi aktívami, preberá najvyššiu hodnotu zo súvisiacich aktív.

§ 7

(1) Bezpečnostné opatrenia sa navrhujú, prijímajú a vykonávajú tak, aby ošetrili všetky riziká identifikované v rámci vykonanej analýzy rizík, naplnili požiadavky stratégie kybernetickej bezpečnosti, bezpečnostnej politiky a bezpečnostných opatrení podľa § 3 až 6.

(2) Zmluva podľa § 19 ods. 2 zákona obsahuje najmä

a) záväzok dodávateľa na výkon činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“) dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,

b) vyjadrenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,

c) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,

d) ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení.

(3) Vzor bezpečnostnej dokumentácie a vzor zmluvy podľa § 19 ods. 2 zákona sa zverejnia na webovom sídle úradu.

§ 8

Zmluva podľa § 19 ods. 2 zákona uzatvorená do 31. augusta 2025 ostáva v platnosti najneskôr do doby pôvodne v nej dohodnutej; túto dobu nemožno po 31. auguste 2025 predĺžiť, ak už uzatvorená zmluva nie je v súlade s bezpečnostnými opatreniami podľa § 3 až 7. Týmto ustanovením nie je dotknutý § 34b ods. 5 zákona.

§ 9

Zrušuje sa 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 v znení vyhlášky č. 264/2023 Z. z.

§ 10

Touto vyhláškou sa preberajú právne záväzné akty Európskej únie uvedené v prílohe č. 3.

§ 11

Táto vyhláška nadobúda účinnosť 1. septembra 2025.

Roman Konečný v. r.

ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PRE OBLASTI KYBERNETICKEJ BEZPEČNOSTI PODĽA § 20 ODS. 2 ZÁKONA

Položka	Bezpečnostné opatrenia pre organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti podľa § 20 ods. 2 písm. a) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
1.	manažér kybernetickej bezpečnosti predkladá návrhy bezpečnostných opatrení a oznamuje informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
2.	je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému podľa príslušnej bezpečnostnej politiky	ÁNO	ÁNO	ÁNO	ÁNO
3.	je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti vrátane pridelenia úloh, rolí ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie	ÁNO	ÁNO	ÁNO	ÁNO
4.	je zabezpečená primeranosť zdrojov na riadenie kybernetickej bezpečnosti a vzdelávanie v oblasti kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
5.	je definovaný a zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
6.	je uplatnená zásada najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh	ÁNO	ÁNO	ÁNO	ÁNO
7.	je uplatnená zásada oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity	ÁNO	ÁNO	ÁNO	ÁNO
8.	je uplatnená zásada vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností	ÁNO	ÁNO	ÁNO	ÁNO
9.	je uplatnená zásada sprístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré	ÁNO	ÁNO	ÁNO	ÁNO

	z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú				
10.	štatutárny orgán sa preukázateľne zaväzuje dodržiavať povinnosti v oblasti kybernetickej bezpečnosti v súlade so stratégiou kybernetickej bezpečnosti a určenými bezpečnostnými politikami a postupmi	ÁNO	ÁNO	ÁNO	ÁNO
11.	je definovaný, schválený a zavedený vnútorný kontrolný systém pre oblasť kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb podľa § 20 ods. 2 písm. b) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
12.	je zabezpečená informovanosť o identifikovaných kybernetických hrozbách s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie a operačné technológie	ÁNO	ÁNO	ÁNO	ÁNO
13.	sú získavané informácie o zraniteľnostiach používaných informačných systémov vrátane hodnotenia, do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu	ÁNO	ÁNO	ÁNO	ÁNO
14.	je najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností	ÁNO	-	ÁNO	ÁNO
15.	je najmenej raz za 6 mesiacov vykonávané pravidelné posudzovanie zraniteľností	-	ÁNO	-	-
16.	sú určené priority aktualizácií na základe posúdenia rizík a analýzy vplyvov	ÁNO	ÁNO	ÁNO	ÁNO
17.	na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností	-	ÁNO	-	ÁNO
Položka	**Bezpečnostné opatrenia pre správu aktív a riadenie kybernetických hrozieb a rizík podľa § 20 ods. 2 písm. c) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
18.	sú zdokumentované a prijaté pravidlá používania a postupy nakladania s aktívami	ÁNO	ÁNO	ÁNO	ÁNO
19.	zamestnanci prevádzkovateľa základnej služby a zamestnanci tretích strán pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom vracajú prevádzkovateľovi základnej služby všetky aktíva, ktoré mali zverené	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre riadenie udalostí a kybernetických bezpečnostných incidentov podľa § 20 ods. 2 písm. d) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***

20.	je zabezpečené plánovanie a 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	ÁNO	ÁNO
21.	je zabezpečené posúdenie udalostí kybernetickej bezpečnosti a určenie ich priorít	ÁNO	ÁNO	ÁNO	ÁNO
22.	je definovaný systém reakcie na kybernetické bezpečnostné incidenty	ÁNO	ÁNO	ÁNO	ÁNO
23.	poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
24.	sú zavedené a uplatňované postupy na identifikáciu, zhromažďovanie, získavanie a uchovávanie digitálnych stôp súvisiacich s kybernetickými bezpečnostnými incidentmi	ÁNO	ÁNO	ÁNO	ÁNO
25.	v prípade kybernetického bezpečnostného incidentu sú dodržiavané všetky stanovené bezpečnostné opatrenia a postupy	ÁNO	ÁNO	ÁNO	ÁNO
26.	sú definované a pravidelne, aspoň raz ročne testované pravidlá pre izoláciu kritických komponentov sietí, informačných systémov a operačných technológií počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie podľa § 20 ods. 2 písm. e) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
27.	prijíma opatrenia tak, aby bola dostupnosť aktív počas kybernetického bezpečnostného incidentu primerane zabezpečená plánovaním, prijatím, udržiavaním a testovaním na základe cieľov procesu riadenia kontinuity činností a požiadaviek na obnovu prevádzky informačných technológií alebo operačných technológií po kybernetickom bezpečnostnom incidente	ÁNO	ÁNO	ÁNO	ÁNO
28.	sú udržiavané a pravidelne, aspoň raz ročne testované záložné kópie dát, softvéru a konfigurácie sietí, informačných systémov a operačných technológií, o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	ÁNO	ÁNO	ÁNO	ÁNO
29.	infraštruktúra sietí, informačných systémov a operačných technológií je zriadená s dostatočnou redundanciou	ÁNO	ÁNO	ÁNO	ÁNO

30.	komponenty operačných technológií sú schopné prepínať sa na núdzové napájanie a z núdzového napájania bez vplyvu na aktuálny stav zabezpečenia alebo na vopred definovaný obmedzený režim	-	-	ÁNO	ÁNO
31.	je zavedený a dodržiavaný princíp ukladania záloh do logicky, fyzicky a geograficky oddelených priestorov	ÁNO	-	ÁNO	-
32.	je zavedený a dodržiavaný princíp spravovania záložných kópií údajov alebo konfigurácií, ktorý zabezpečuje tri kópie údajov alebo konfigurácií, na dvoch rozličných typoch médií, z ktorých jedna kópia je uložená v logicky, fyzicky a geograficky oddelenom priestore	-	ÁNO	-	ÁNO
33.	zálohy týkajúce sa operačných technológií sú oddelené v samostatnom zálohovacom systéme	-	-	-	ÁNO
34.	pre zálohy týkajúce sa operačných technológií je minimálne raz ročne vykonávaná kontrola funkčnosti záloh aspoň dvoch rôznych systémov; o kontrole funkčnosti záloh sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	-	-	-	ÁNO
Položka	**Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií podľa § 20 ods. 2 písm. f) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
35.	je zabezpečené prepojenie procesov riadenia rizík a projektového riadenia počas celého životného cyklu projektov	ÁNO	ÁNO	ÁNO	ÁNO
36.	sú prijaté opatrenia na zabránenie straty, poškodenia, krádeže alebo kompromitácie aktív a prerušeniu prevádzky	ÁNO	ÁNO	ÁNO	ÁNO
37.	prístup k zdrojovému kódu, vývojovým technológiám a softvérovým knižniciam na čítanie a zápis je riadený	ÁNO	ÁNO	ÁNO	ÁNO
38.	sú prijaté bezpečnostné opatrenia s požadovanými bezpečnostnými nastaveniami tak, aby konfigurácia technických prostriedkov, programových prostriedkov, služieb a sietí nebola zmenená neoprávnenými osobami	ÁNO	ÁNO	ÁNO	ÁNO
39.	sú odinštalované alebo zakázané služby neslúžiace na vykonávanie činností prevádzkovateľa základnej služby na podporných aktívach	-	ÁNO	-	ÁNO
40.	sú určené a aplikované základné parametre pre bezpečné konfigurácie	-	-	ÁNO	ÁNO
41.	komponenty operačných technológií sú konfigurované podľa odporúčaných bezpečnostných nastavení uvedených dodávateľom komponentu operačných technológií	-	-	ÁNO	ÁNO

42.	komponenty operačných technológií poskytujú rozhranie na prístup k aktuálne nasadeným bezpečnostným konfiguračným nastaveniam	-	-	ÁNO	ÁNO
43.	je pravidelne, aspoň raz ročne vykonávaná kontrola a aktualizácia konfigurácie komponentov sietí, informačných systémov a operačných technológií podľa vývoja hrozieb; o kontrole sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	ÁNO	ÁNO	ÁNO	ÁNO
44.	sú určené a uplatnené pravidlá bezpečného vývoja softvéru a informačných systémov	ÁNO	ÁNO	ÁNO	ÁNO
45.	sú pri vývoji alebo získavaní aplikácií identifikované a naplnené relevantné požiadavky na kybernetickú bezpečnosť	ÁNO	ÁNO	-	-
46.	riadiaci systém umožňuje zabráneniu ďalšieho prístupu spustením uzamknutia relácie po konfigurovateľnom čase nečinnosti alebo manuálnym uzamknutím; blokovanie relácie zostáva v platnosti, ak používateľ, ktorý reláciu vlastní, alebo iný oprávnený používateľ neobnoví prístup pomocou schválených identifikačných a autentifikačných postupov – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	ÁNO	ÁNO
47.	je zavedená a dodržiavaná schopnosť chrániť integritu relácií	ÁNO	ÁNO	ÁNO	ÁNO
48.	je automaticky odmietnuté použitie neplatných identifikátorov relácií	ÁNO	ÁNO	ÁNO	ÁNO
49.	je zaručený bezpečný návrh, inštalácia a prevádzka sietí, informačných systémov a operačných technológií v rámci životného cyklu	ÁNO	ÁNO	ÁNO	ÁNO
50.	v rámci životného cyklu vývoja operačných technológií sú návrhy a zmeny vykonané vo vyhradenom vývojovom prostredí	-	-	ÁNO	ÁNO
51.	sú definované a vykonávané procesy súvisiace s bezpečným programovaním softvéru s cieľom znížiť počet potenciálnych zraniteľností v softvéri	ÁNO	ÁNO	ÁNO	ÁNO
52.	sú definované a vykonávané procesy testovania bezpečnosti informačných systémov a operačných technológií	ÁNO	ÁNO	ÁNO	ÁNO
53.	testovanie kybernetickej bezpečnosti je začlenené do životného cyklu vývoja a údržby sietí, informačných systémov a operačných technológií	ÁNO	ÁNO	ÁNO	ÁNO
54.	sú riadené, monitorované a kontrolované činnosti súvisiace s vývojom programových prostriedkov a informačných systémov, ktoré sú dodávané treťou stranou	ÁNO	ÁNO	ÁNO	ÁNO
55.	vývojové, testovacie a produkčné prostredia sú vzájomne oddelené a zabezpečené	ÁNO	ÁNO	ÁNO	ÁNO
56.	dáta používané pre testovanie sú vhodne vyberané, chránené a spravované	ÁNO	ÁNO	ÁNO	ÁNO
Položka		**Relevancia pre IKT***		**Relevancia pre OT***	

	Bezpečnostné opatrenia pre postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti podľa § 20 ods. 2 písm. g) zákona prijíma prevádzkovateľ základnej služby tak, že:	**PZS***	**PKZS***	**PZS***	**PKZS***
57.	je zaručený súlad s požiadavkami vyplývajúcimi zo všeobecne záväzných právnych predpisov, zmluvnými požiadavkami týkajúcimi sa kybernetickej bezpečnosti	ÁNO	ÁNO	-	-
58.	riadenie kybernetickej bezpečnosti je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií	ÁNO	ÁNO	ÁNO	ÁNO
59.	súlad so stratégiou kybernetickej bezpečnosti, bezpečnostnými politikami, bezpečnostnými štandardmi a normami je prehodnocovaný najmenej raz za kalendárny rok v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií	ÁNO	ÁNO	ÁNO	ÁNO
60.	sú definované pravidlá pre výkon auditných činností a kontrolných činností v oblasti kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre kryptografické opatrenia a zásady používania kryptografie podľa § 20 ods. 2 písm. h) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
61.	nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov a sú dodržiavané požiadavky vyplývajúce zo všeobecne záväzných právnych predpisov, požiadavky vyplývajúce zo zmlúv alebo v prípade certifikovaného subjektu normatívne požiadavky týkajúce sa kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
62.	sú definované a zavedené pravidlá efektívneho používania kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov	ÁNO	ÁNO	ÁNO	ÁNO
63.	sú prijaté a aplikované postupy na pravidelné prehodnocovanie odolnosti zavedených kryptografických mechanizmov; prehodnocovanie odolnosti zavedených kryptografických mechanizmov sa vykonáva najmenej raz ročne a vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre bezpečnosť a spôsobilosti ľudských zdrojov podľa § 20 ods. 2 písm. i) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
64.	sú určené pravidlá pre zaradenie osôb do jednotlivých pracovných rolí	ÁNO	ÁNO	ÁNO	ÁNO

65.	v pracovných zmluvách, zmluvách v súvislosti s iným obdobným pracovnoprávnym vzťahom alebo iných súvisiacich dokumentoch sú uvedené zodpovednosti za kybernetickú bezpečnosť	ÁNO	ÁNO	ÁNO	ÁNO
66.	pre všetky pracovné roly je poskytované primerané vzdelávanie, aby štatutárny orgán prevádzkovateľa základnej služby, zamestnanci prevádzkovateľa základnej služby a tretie strany mali primerané povedomie o kybernetickej bezpečnosti v oblasti informačných a operačných technológií; súčasťou školení sú aj praktické simulácie a cvičenia reakcie na kybernetické bezpečnostné incidenty	ÁNO	ÁNO	ÁNO	ÁNO
67.	zamestnanci prevádzkovateľa základnej služby a tretie strany sú preukázateľne oboznámení s bezpečnostnými politikami	ÁNO	ÁNO	ÁNO	ÁNO
68.	aktualizované verzie bezpečnostných politík sú bezodkladne sprístupňované vrcholovému vedeniu prevádzkovateľa základnej služby, manažmentu prevádzkovateľa základnej služby, zamestnancom prevádzkovateľa základnej služby, a v potrebnom rozsahu aj tretej strane alebo ďalším zainteresovaným stranám	ÁNO	ÁNO	ÁNO	ÁNO
69.	sú formalizované disciplinárne procesy voči zamestnancom prevádzkovateľa základnej služby, ktorí sa dopustili porušenia ustanovení bezpečnostných politík prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
70.	zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti, ktoré zostávajú v platnosti aj pri zmene alebo pri ukončení pracovnoprávneho vzťahu alebo zmluvy tretej strany s prevádzkovateľom základnej služby podľa § 19 ods. 2 zákona, sú v rámci zmeny alebo ukončenia pracovnoprávneho vzťahu alebo zmluvy tretej strany s prevádzkovateľom základnej služby podľa § 19 ods. 2 zákona definované, presadzované a oznámené príslušným zamestnancom, tretím stranám alebo iným zainteresovaným stranám s cieľom chrániť záujmy prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
71.	sú určené, zdokumentované a pravidelne, najmenej raz za dva roky, preskúmavané a podpisované dohody o mlčanlivosti, ktoré odrážajú potreby prevádzkovateľa základnej služby pre zachovanie dôvernosti	ÁNO	ÁNO	ÁNO	ÁNO
72.	ak zamestnanci pracujú na diaľku, sú prijaté bezpečnostné opatrenia na ochranu informácií, ku ktorým sa pristupuje, ktoré sa spracúvajú alebo ktoré sa uchovávajú mimo priestorov prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
73.	sa používa viacfaktorové overovanie pre vzdialený prístup	ÁNO	ÁNO	ÁNO	ÁNO

74.	sú prijaté požiadavky na identifikáciu oprávnenosti pristupujúceho technického prostriedku a následne aj používateľa; toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	ÁNO	ÁNO
75.	v prípade prístupu na inžinierske prostredia v rámci prostredia operačných technológií je zaistený prístup a overenie technológiou pre záznam a archiváciu úkonov externej organizácie; toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	-	ÁNO
Položka	**Bezpečnostné opatrenia pre správu identít a prístupov podľa § 20 ods. 2 písm. j) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
76.	pri riadení prístupov k sieťam a informačným systémom 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 údajov a zápis údajov a na zmeny oprávnení a prostredníctvom ktorých sa zaznamenáva použitie prístupových oprávnení	ÁNO	ÁNO	ÁNO	ÁNO
77.	zavedená a využívaná samostatná, oddelená technológia na riadenie prístupov v operačných technológiách	-	-	-	ÁNO
78.	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	ÁNO	ÁNO
79.	každému používateľovi a systémovému účtu je pridelený jednoznačný identifikátor na autentizáciu na prístup do siete a informačného systému	ÁNO	ÁNO	ÁNO	ÁNO
80.	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	ÁNO	ÁNO
81.	je zavedené riadenie prístupov na základe rolí a zásady najnižších oprávnení pre používateľov	-	ÁNO	ÁNO	ÁNO

82.	privilegované prístupové práva sú poskytované len oprávneným používateľom, komponentmi informačných a operačných technológií a službám podľa príslušnej politiky riadenia prístupov a práv	ÁNO	ÁNO	ÁNO	ÁNO
83.	prístup k aktívam je obmedzený v súlade s určenou s definovanou politikou riadenia prístupov	ÁNO	ÁNO	ÁNO	ÁNO
84.	technológie a postupy bezpečnej autentizácie sú zavedené na základe požiadaviek na obmedzenie prístupu k informáciám podľa príslušnej politiky riadenia prístupov a práv	ÁNO	ÁNO	ÁNO	ÁNO
85.	používatelia majú prijaté primerané opatrenia na ochranu a udržiavanie pridelených autentifikačných prostriedkov vrátane nezdieľania autentifikačných prostriedkov s inými osobami	ÁNO	ÁNO	ÁNO	ÁNO
86.	všetky prístupy do sietí, informačných systémov a operačných technológií z nedôveryhodných zdrojov sú riadené a monitorované	-	-	ÁNO	ÁNO
87.	siete, informačné systémy a operačné technológie umožňujú identifikáciu neoprávnených rádiofrekvenčných zariadení	-	ÁNO	-	ÁNO
Položka	**Bezpečnostné opatrenia pre bezpečnosť pri prevádzke sietí a informačných systémov podľa § 20 ods. 2 písm. k) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
88.	prevádzkové postupy pre zariadenia na spracovanie informácií, siete a informačné systémy sú zdokumentované a sprístupnené zamestnancom podľa ich potreby	ÁNO	ÁNO	ÁNO	ÁNO
89.	sa zabraňuje strate, poškodeniu alebo ohrozeniu aktív alebo prerušeniu prevádzky v dôsledku zlyhania a narušenia podporných služieb vrátane dodávky elektrickej energie	ÁNO	ÁNO	ÁNO	ÁNO
90.	sa zabraňuje strate, poškodeniu, krádeži alebo kompromitácii aktív alebo prerušeniu prevádzky v súvislosti s narušením kabeláže elektrického napájania alebo dátových liniek	ÁNO	ÁNO	ÁNO	ÁNO
91.	sa zabraňuje 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	ÁNO	ÁNO
92.	je dostupná kapacita podporných aktív	ÁNO	ÁNO	ÁNO	ÁNO
93.	systémový čas príslušných podporných aktív, ktoré spracúvajú informácie alebo podporujú ich spracovanie, je synchronizovaný so schválenými zdrojmi času, zohľadňujúcimi časové zóny	ÁNO	ÁNO	ÁNO	ÁNO

94.	používanie systémových obslužných programových prostriedkov, ktoré môžu byť schopné obísť systémové a aplikačné opatrenia, je obmedzené a kontrolované	ÁNO	ÁNO	ÁNO	ÁNO
95.	sú zavedené postupy a opatrenia na bezpečné riadenie inštalácie programových prostriedkov a informačných systémov do produkčnej prevádzky	ÁNO	ÁNO	ÁNO	ÁNO
96.	zmeny procesov a systémov podliehajú schválenému procesu riadenia zmien	ÁNO	ÁNO	ÁNO	ÁNO
97.	je definovaný a zavedený proces riadenia výnimiek zo schválených bezpečnostných opatrení	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre ochranu proti škodlivému kódu a nežiaducemu obsahu podľa § 20 ods. 2 písm. l) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
98.	je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov	ÁNO	ÁNO	ÁNO	ÁNO
99.	je zaručená pravidelná aktualizácia sietí, informačných systémov a operačných technológií s cieľom zabezpečiť minimálne narušenie bežnej prevádzky	ÁNO	ÁNO	ÁNO	ÁNO
100.	prístup k externým internetovým zdrojom je riadený s cieľom znížiť vystavenie škodlivému obsahu	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť podľa § 20 ods. 2 písm. m) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
101.	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	ÁNO	ÁNO
102.	je používané šifrovanie na zabezpečenie údajov pri prenose vybraných údajov medzi systémami OT; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií	-	-	ÁNO	ÁNO
103.	je používané šifrovanie na zabezpečenie vybraných údajov pri prenose medzi a v rámci rôznych úrovní systémov OT; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	-	ÁNO
104.	na informačné systémy, siete a technické prostriedky, 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	ÁNO	ÁNO

105.	siete a technické prostriedky sietí sa zabezpečujú, spravujú a kontrolujú s cieľom chrániť informácie v informačných systémoch, programových prostriedkoch a mobilných aplikáciách	ÁNO	ÁNO	ÁNO	ÁNO
106.	sú určené, zavedené a monitorované bezpečnostné funkcie, úrovne služieb a požiadavky týkajúce sa sieťových služieb	ÁNO	ÁNO	ÁNO	ÁNO
107.	sú prijaté a udržiavané systémy detekcie narušenia, ktoré zohľadňujú proprietárne protokoly a dátové toky	-	-	ÁNO	ÁNO
108.	pre komponenty operačných technológií je automaticky ukončovaná vzdialená relácia po stanovenom, konfigurovateľnom čase nečinnosti	-	-	ÁNO	ÁNO
109.	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	ÁNO	ÁNO
110.	sú prijaté a udržiavané mechanizmy na smerovanie a filtráciu sieťovej prevádzky do a z externých sietí cez sieťový firewall	-	-	ÁNO	ÁNO
111.	je definovaná a zavedená logická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami	-	-	ÁNO	ÁNO
112.	je definovaná a zavedená fyzická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami	-	-	-	ÁNO
113.	sú segmentované vybrané siete riadiaceho systému od ostatných sietí operačných technológií – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	ÁNO	ÁNO
114.	sieťový firewall pre operačné technológie je nezávislý od ostatných mechanizmov na smerovanie a filtráciu sieťovej prevádzky	-	-	ÁNO	ÁNO
115.	v sieťach určených pre operačné technológie je blokované odosielanie a prijímanie správ medzi používateľmi	-	-	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre monitorovanie, zaznamenávanie a hlásenie udalostí podľa § 20 ods. 2 písm. n) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
116.	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	ÁNO	ÁNO
117.	záznamy o činnostiach obsahujú informáciu o pôvodcovi vykonanej činnosti	-	ÁNO	-	ÁNO

118.	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	ÁNO	ÁNO
119.	siete, informačné systémy, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí automatizovaným spôsobom	-	ÁNO	-	ÁNO
120.	sú prijaté a udržiavané mechanizmy overovania činností bezpečnostných funkcií a oznamovania nezvyčajného správania počas bežnej prevádzky, testovania a plánovanej údržby	-	-	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení podľa § 20 ods. 2 písm. o) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
121.	sú definované a používané bezpečnostné perimetre na ochranu oblastí, ktoré obsahujú aktíva používané v sieťach, informačných systémoch a operačných technológiách	ÁNO	ÁNO	ÁNO	ÁNO
122.	priestory, v ktorých sa nachádzajú riadiace a serverové súčasti informačných a operačných technológií, majú definované pravidlá fyzickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
123.	fyzický prístup k vybraným aktívam infraštruktúry, ktoré sú klasifikované ako kritické alebo významné z hľadiska bezpečnosti a prevádzky, je povolený výhradne autorizovaným osobám	ÁNO	ÁNO	ÁNO	ÁNO
124.	je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení	ÁNO	ÁNO	ÁNO	ÁNO
125.	zabezpečené priestory sú nepretržite monitorované z hľadiska neoprávneného fyzického prístupu	ÁNO	ÁNO	ÁNO	ÁNO
126.	sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu	ÁNO	ÁNO	ÁNO	ÁNO
127.	sú monitorované a vizuálne zaznamenávané všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu	-	ÁNO	-	ÁNO
128.	je navrhnutá a zavedená ochrana pred fyzickými hrozbami a environmentálnymi hrozbami, ako sú prírodné katastrofy a iné úmyselné alebo neúmyselné ohrozenia informačných a operačných technológií	ÁNO	ÁNO	ÁNO	ÁNO
129.	aktíva v zabezpečených priestoroch sú chránené pred poškodením a neoprávneným zásahom zo strany zamestnancov pracujúcich v týchto priestoroch a nepovolaných osôb	ÁNO	ÁNO	ÁNO	ÁNO

130.	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	ÁNO	ÁNO
131.	sú riadené riziká vyplývajúce z hrozieb fyzického prostredia a z neoprávneného fyzického prístupu k aktívam	ÁNO	ÁNO	ÁNO	ÁNO
132.	sa prijímajú opatrenia na zabránenie strate, poškodeniu, krádeži alebo kompromitácii zariadení používaných, prenášaných a uchovávaných mimo pracoviska a sú definované postupy, ak k takejto udalosti dôjde	ÁNO	ÁNO	ÁNO	ÁNO
133.	je regulované alebo zakázané používanie prenosných zariadení v kritických oblastiach operačných technológií	-	-	ÁNO	ÁNO
134.	je zabezpečené automatické presadzovanie konfigurovateľných obmedzení používania, ktoré zahŕňajú najmä zabránenie používaniu prenosných a mobilných zariadení, vyžadovanie autorizácie špecifickej pre daný kontext, obmedzenie prenosu kódu a údajov do/z prenosných a mobilných zariadení – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	-	ÁNO
135.	je zabezpečené overenie, či prenosné alebo mobilné zariadenia, ktoré sa pokúšajú pripojiť k bezpečnostnej zóne, spĺňajú bezpečnostné požiadavky danej bezpečnostnej zóny	-	-	-	ÁNO
136.	pamäťové médiá sú riadené 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	ÁNO	ÁNO
137.	dáta uložené v koncových zariadeniach používateľov, spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich, sú chránené	ÁNO	ÁNO	ÁNO	ÁNO
138.	informácie uložené v informačných systémoch, zariadeniach alebo na iných pamäťových médiách sú vymazané, ak už nie sú potrebné	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre ochranu záznamov, súkromia a označovanie informácií podľa § 20 ods. 2 písm. p) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
139.	informácie sú klasifikované na základe potrieb prevádzkovateľa základnej služby a na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán	ÁNO	ÁNO	ÁNO	ÁNO

140.	dátové toky medzi jednotlivými bezpečnostnými zónami v rámci topológie systémov OT sú klasifikované na základe potrieb prevádzkovateľa základnej služby a na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán	-	-	ÁNO	ÁNO
141.	sú vypracované a zavedené postupy na označovanie informácií v súlade s prijatou klasifikačnou schémou	ÁNO	ÁNO	ÁNO	ÁNO
142.	je zabezpečený súlad so všeobecne záväznými právnymi predpismi a zmluvnými požiadavkami týkajúcimi sa práv duševného vlastníctva a používania patentovaných produktov	ÁNO	ÁNO	ÁNO	ÁNO
143.	záznamy sú primerane chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným zverejnením	ÁNO	ÁNO	ÁNO	ÁNO
144.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany osobných údajov podľa osobitných predpisov a zmluvných požiadaviek	ÁNO	ÁNO	ÁNO	ÁNO
Položka	**Bezpečnostné opatrenia pre dodávateľský reťazec podľa § 20 ods. 2 písm. q) zákona prijíma prevádzkovateľ základnej služby tak, že:**	**Relevancia pre IKT***		**Relevancia pre OT***	
		PZS*	**PKZS***	**PZS***	**PKZS***
145.	sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán	ÁNO	ÁNO	ÁNO	ÁNO
146.	na riadenie informačnej bezpečnosti a kybernetickej bezpečnosti vo vzťahoch s tretími stranami je s každou treťou stranou s významným vplyvom uzatvorená zmluva podľa § 19 ods. 2 zákona	ÁNO	ÁNO	ÁNO	ÁNO
147.	uzatvoreniu zmluvy podľa § 19 ods. 2 zákona predchádza analýza rizík dodávateľských služieb alebo iných dodávateľských činností	ÁNO	ÁNO	ÁNO	ÁNO
148.	súčasťou zmluvy podľa § 19 ods. 2 zákona sú bezpečnostné požiadavky špecifické pre informačné a komunikačné technológie alebo operačné technológie	ÁNO	ÁNO	ÁNO	ÁNO
149.	bezpečnostné opatrenia sú uplatnené v dodávateľskom reťazci produktov a služieb, ktorý priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
150.	sú pravidelne, najmenej raz za dva roky monitorované, preskúmavané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO

151.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie cloudových služieb a riadená kybernetická bezpečnosť pri používaní cloudových služieb	ÁNO	ÁNO	ÁNO	ÁNO

Vysvetlivky:

***Vrstvami pre operačné technológie** je nasledovné rozdelenie prostredí, ktoré majú vplyv na prevádzkované operačné technológie:
vrstva 5 – celkové prostredie organizácie,
vrstva 4 – prostredie pre centrálnu správu operačných technológií,
vrstva 3 – prostredie pre prevádzku a riadenie výrobného procesu, najmä zálohovací server (historian), riadiace servery,
vrstva 2 – prostredie pre riadenie a automatizáciu procesov, najmä rozhranie človek-stroj (HMI), dispečerské riadenie a zber dát (SCADA),
vrstva 1 – prostredie priameho riadenia, najmä programovateľné logické automaty (PLC),
vrstva 0 – fyzické prostredie, najmä senzory, akčné členy.

***PZS** – prevádzkovateľ základnej služby,
PKZS – prevádzkovateľ kritickej základnej služby,
IKT – informačné a komunikačné technológie,
OT – operačné technológie,
Komponent informačnej architektúry – súčasť/prvok informačného systému, ktorý sa podieľa na jeho fungovaní,
Infraštruktúra operačných technológií – súbor všetkých technických, materiálnych a organizačných prostriedkov, ktoré sú potrebné na zabezpečenie a realizáciu výroby.

Príloha č. 2
k vyhláške č. 227/2025 Z. z.

KLASIFIKAČNÁ SCHÉMA

A. Kritériá klasifikácie informácií

Klasifikačné stupne

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktíva“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

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

   a) verejné informačné aktíva určené pre verejnosť, ktoré sú 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 publikované informácie alebo všeobecne dostupné informácie,

   b) interné informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,

   c) chránené informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; 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 aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ 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 poskytovanú službu,

   b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť vplyv na kontinuitu poskytovanej služby, strategickú oblasť, trhové a operačné riziká,

   c) vysoká zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej

služby.

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

   a) nízka zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,

   b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať vplyv na kontinuitu poskytovanej služby, strategickú oblasť, trhové a operačné riziká,

   c) vysoká zahŕňa vybrané informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.

Základné pravidlá klasifikácie informácií

1. Každá klasifikovaná informácia má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti.
2. Bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.
3. Prevádzkovateľ základnej služby môže v rozsahu svojej pôsobnosti jednotlivé informačné aktíva zaradiť do vyššieho stupňa.

Príloha č. 3
k vyhláške č. 227/2025 Z. z.

ZOZNAM PREBERANÝCH PRÁVNE ZÁVÄZNÝCH AKTOV EURÓPSKEJ ÚNIE

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27. 12. 2022).

1) Napríklad § 6 ods. 2 vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Račianska 71, 813 11 Bratislava,
tel.: +421 2 888 91 864, +421 2 888 91 865, e-mail: helpdesk@slov-lex.sk.