MINIMÁLNE BEZPEČNOSTNÉ OPATRENIA

Položka	Bezpečnostné opatrenia pre organizáciu a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti prijíma správca tak, že:	Kat. I	Kat. II	Kat. III
1.	je určená osoba zodpovedná za koordináciu a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti, ktorá je nezávislá od štruktúry riadenia prevádzky a vývoja služieb informačných technológií verejnej správy a ktorá 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 prideľovanie 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			ÁNO

	bezpečnosti ustanovených touto vyhláškou; fungovanie výboru upravuje jeho schválený štatút alebo iný interný riadiaci akt správcu			
7.	je zabezpečená primeranosť zdrojov na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti a vzdelávanie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti	ÁNO	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 organizácií 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, ktorý umožňuje splnenie pridelených úloh	ÁNO	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	ÁNO
12.	je uplatnená zásada vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností	ÁNO	ÁNO	ÁNO
13.	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 z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú	ÁNO	ÁNO	ÁNO
14.	je určený štatutárny orgán zodpovedný za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti a za vzdelávanie v týchto oblastiach	ÁNO	ÁNO	ÁNO
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 šesť 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 prijíma správca tak, že:**	**Kat. I**	**Kat. II**	**Kat. III**
24.	identifikuje a vedie 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	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 slúži na určenie primeranosti prijatých bezpečnostných opatrení a obsahuje a) identifikáciu rizík na úrovni celej organizácie a vedenie katalógu týchto rizík, b) metodiku alebo interný postup pre výkon analýzy rizík, c) analýzu rizík s vyhodnotením rizík, d) prijatie bezpečnostných opatrení v závislosti od identifikovaných rizík	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 správcu alebo ním poverený riadiaci pracovník	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 nim určené povinnosti, zodpovednosti a právomoci jednotlivých osôb zastávajúcich 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.	pri prevádzke všetkých ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie je definovaný, zavedený a kontrolovaný systém riadenia bezpečnostných incidentov kybernetickej bezpečnosti a informačnej bezpečnosti organizácie, ktorý obsahuje a) postupy počas celého životného cyklu riadenia bezpečnostných incidentov, b) typy identifikovaných udalostí, ich kombinácie a príslušné bezpečnostné incidenty, c) komunikačné, eskalačné a nahlasovacie povinnosti,	ÁNO	ÁNO	ÁNO

	d) spoluprácu s orgánom vedenia, e) testovanie riešenia bezpečnostných incidentov			
33.	je zabezpečené testovanie riešenia kybernetických bezpečnostných incidentov aspoň raz ročne 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 incidentmi		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 a procesov 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 centrálny metainformačný systém verejnej správy, Vládny informačný systém kybernetickej bezpečnosti a Centrálny portál kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO
39.	je definovaný a zavedený systém určenia kritickosti činností, procesov a služieb organizácie, ktorý obsahuje a) spôsob identifikácie a vedenia všetkých činností, procesov a služieb, b) metodiku pre výkon analýzy vplyvov, c) samotnú analýzu funkčných vplyvov a určenie kritickosti pre ISVS a ITVS,	ÁNO	ÁNO	ÁNO

	d) väzbu na riadenie mimoriadnych a krízových situácií a zmluvných požiadaviek, ak súvisia s prevádzkou ISVS a ITVS			
40.	organizácia preskúma a analyzuje funkčné vplyvy 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.	dostupnosť primárnych aktív počas kybernetického bezpečnostného incidentu je 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 najrýchlejšiu obnovu	ÁNO	ÁNO	ÁNO
45.	je definovaný, nastavený a zavedený systém implementácie a testovania zálohovania biznis dát a systémových alebo 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 určí maximálnu prijateľnú dobu výpadku (RTO) a maximálnu prijateľnú stratu dát (RPO)		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 a) je zabezpečené prepojenie procesov vedenia aktív, riadenia rizík a projektového riadenia počas celého životného cyklu projektov, pričom sú vytvorené požiadavky na bezpečnosť ISVS a ITVS, b) je zabezpečený 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	ÁNO	ÁNO	ÁNO
50.	sú prijaté primerané procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre aplikovanie požiadaviek na bezpečnosť 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.	je zabezpečená integrácia identifikovaných rizík ISVS a ITVS a navrhovaných bezpečnostných opatrení do celkového riadenia rizík v organizácii správcu		ÁNO	ÁNO
52.	sú prijaté opatrenia na zabránenie strate, poškodeniu, krádeži alebo kompromitácii aktív a prerušeniu prevádzky ISVS	ÁNO	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 určí osobu zodpovednú za dohľad nad plnením požiadaviek podľa tejto 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 určí osobu zodpovednú za dohľad nad plnením bezpečnostných požiadaviek určených v katalógu požiadaviek na predmet dodávky ISVS		ÁNO	ÁNO
58.	pre každý projekt ISVS určí 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 stavu bezpečnostných opatrení ISVS, 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.	sú určené požiadavky na bezpečnosť pri integrácii nových ITVS, ISVS alebo služieb do ISVS; tieto požiadavky by mali zahŕňať napríklad kompatibilitu, vhodnú autentifikáciu, šifrovanie dát, ako aj povinnosť zdokumentovať podrobnosti súvisiace s danou integráciou		ÁNO	ÁNO
62.	sú určené bezpečnostné požiadavky na ISVS, ktorý sa ide obstarávať, v súlade s požiadavkami vyplývajúcimi z príslušných všeobecne záväzných právnych predpisov		ÁNO	ÁNO
63.	je zabezpečené zahrnutie konkrétnych bezpečnostných požiadaviek do zmlúv na vývoj alebo rozvoj ISVS alebo do zmlúv o poskytovaní služieb (SLA) s poskytovateľmi IT služieb		ÁNO	ÁNO
64.	je automaticky odmietnuté použitie neplatných identifikátorov relácií		ÁNO	ÁNO
65.	je zabezpečené vypracovanie a implementácia bezpečnostných projektov ISVS podľa špecifikácie uvedenej v prílohe č. 3		ÁNO	ÁNO
66.	je určená povinnosť riadenia rizík identifikovaných v bezpečnostných projektoch vyvíjaných alebo prevádzkovaných ISVS a povinnosť zahrnutia rizík do celkového systému riadenia rizík kybernetickej bezpečnosti		ÁNO	ÁNO

67.	pred nasadením nového ISVS, ktorý má rozhranie s verejnou sieťou internet a ktorý spracúva osobitné kategórie osobných údajov podľa osobitného predpisu[1]) alebo informácie používané a prístupné len určeným skupinám oprávnených osôb, ktorých neoprávnené odhalenie, prezradenie alebo zničenie môže mať negatívny vplyv na poskytovanie služby verejnej správy do produkcie, je zabezpečený výkon penetračného testovania z externého prostredia a odstránenie zistených nedostatkov a následne je realizované penetračné testovanie raz za dva roky		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 vyberané, chránené a spravované		ÁNO	ÁNO
72.	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**
73.	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 bezpečnosti a informačnej bezpečnosti	ÁNO	ÁNO	ÁNO
74.	riadenie kybernetickej bezpečnosti a informačnej bezpečnosti správcu je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií		ÁNO	ÁNO

[1]) Čl. 9 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4. 5. 2016).

75.	súlad kybernetickej bezpečnosti a informačnej bezpečnosti správcu s jeho bezpečnostnou dokumentáciou je prehodnocovaný najmenej raz ročne v plánovaných intervaloch alebo pri významných zmenách procesov, ITVS alebo ISVS		ÁNO	ÁNO
76.	sú definované pravidlá pre výkon auditných činností a kontrolných činností v oblasti kybernetickej bezpečnosti		ÁNO	ÁNO
77.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany osobných údajov podľa osobitných predpisov[2]) a zmluvných požiadaviek, ak sú spracúvané v ISVS a ITVS	ÁNO	ÁNO	ÁNO
78.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany tajomstva podľa osobitných predpisov[3]) a zmluvných požiadaviek, ak sú spracúvané v ISVS a ITVS	ÁNO	ÁNO	ÁNO
79.	je zabezpečené plnenie požiadaviek na ochranu práv duševného vlastníctva a použitia patentových produktov podľa osobitných predpisov[4]) 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**
80.	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
81.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia pre šifrovanie pevných diskov koncových zariadení a prenosných médií používaných v súvislosti s ISVS a ITVS	ÁNO	ÁNO	ÁNO
82.	nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov a sú dodržiavané		ÁNO	ÁNO

[2]) Napríklad nariadenie (EÚ) 2016/679, zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[3]) Napríklad § 91 zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 11 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[4]) Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) č. 1257/2012 zo 17. decembra 2012, ktorým sa vykonáva posilnená spolupráca na účely vytvorenia jednotnej patentovej ochrany (Ú. v. EÚ L 361, 31. 12. 2012), zákon č. 435/2001 Z. z. o patentoch, dodatkových ochranných osvedčeniach a o zmene a doplnení niektorých zákonov (patentový zákon) v znení neskorších predpisov, zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov.

	požiadavky vyplývajúce so všeobecne záväzných právnych predpisov a požiadavky vyplývajúce zo zmlúv			
83.	sú definované a zavedené pravidlá evidencie a používania kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov		ÁNO	ÁNO
84.	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**
85.	organizácia identifikuje a vedie zoznam všetkých zamestnancov, ktorí vykonávajú svoje činnosti v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
86.	sú formalizované procesy súvisiace so zaradením do pozície, zmenou pozície alebo vyradením a odobratím pozície pre používateľov, administrátorov alebo zamestnancov tretích strán zastávajúcich roly	ÁNO	ÁNO	ÁNO
87.	sú určené pravidlá pre zaradenie osôb do jednotlivých rolí		ÁNO	ÁNO
88.	v pracovných zmluvách, zmluvách v súvislosti s iným obdobným pracovnoprávnym vzťahom alebo iných súvisiacich dokumentoch sú uvedené zodpovednosti za kybernetickú bezpečnosť		ÁNO	ÁNO
89.	je definovaný a zavedený systém primeraného úvodného vzdelávania a pravidelného preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti a informačnej bezpečnosti	ÁNO	ÁNO	ÁNO
90.	pre všetky roly je poskytované primerané vzdelávanie, aby štatutárny orgán správcu, zamestnanci správcu 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
91.	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

92.	zamestnanci správcu a tretie strany sú preukázateľne oboznámení s bezpečnostnými politikami	ÁNO	ÁNO	ÁNO
93.	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	ÁNO
94.	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 sa uplatňuje počas výkonu činnosti, ako aj po jej skončení	ÁNO	ÁNO	ÁNO
95.	sú určené, podpísané, zdokumentované a pravidelne, najmenej raz za dva roky preskúmavané dohody o mlčanlivosti, ktoré odrážajú potreby správcu pre zachovanie dôvernosti		ÁNO	ÁNO
96.	ak zamestnanci pracujú na diaľku, sú prijaté bezpečnostné opatrenia na ochranu informácií a služieb, ku ktorým pristupujú, ktoré sa využívajú alebo spracúvajú alebo ktoré sa uchovávajú mimo priestorov správcu	ÁNO	ÁNO	ÁNO
97.	sa používa viacfaktorové overovanie pre vzdialený prístup		ÁNO	ÁNO
98.	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
99.	pre všetky ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie správcu je definovaný, zavedený a kontrolovaný systém riadenia identít a prístupov organizácie správcu, ktorý obsahuje a) zoznam systémov a spôsob riadenia lokálnych identít a centrálne riadených identít používateľov a tretích strán, b) zoznam a jednotlivé typy identít a používateľov, technických účtov a administrátorov naprieč systémami, c) spôsoby identifikácie a autentifikácie používateľov v jednotlivých systémoch	ÁNO	ÁNO	ÁNO
100.	organizácia správcu vedie zoznam všetkých používateľov, ich identifikátorov a autorizácií v rámci správy ISVS a ITVS	ÁNO	ÁNO	ÁNO
101.	organizácia správcu určí, zavedie a používa mechanizmy a nástroje na riadenie identít a prístupov pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
102.	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
103.	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
104.	každému používateľovi a systémovému účtu je pridelený jednoznačný identifikátor na autentizáciu na prístup do siete a ISVS		ÁNO	ÁNO
105.	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		ÁNO	ÁNO

	prístupových účtov; vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej počas obdobia od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia			
106.	je zavedené riadenie prístupov na základe rolí a zásady najnižších oprávnení pre používateľov		ÁNO	ÁNO
107.	privilegované prístupové práva sú poskytované len oprávneným používateľom, komponentom ITVS a ISVS a službám podľa príslušnej politiky riadenia prístupov a práv		ÁNO	ÁNO
108.	prístup k aktívam je obmedzený v súlade s určenou a definovanou politikou riadenia prístupov		ÁNO	ÁNO
109.	technológie a postupy bezpečnej autentizácie sú zavedené na základe požiadaviek na obmedzenie prístupu k informáciám podľa príslušnej politiky riadenia prístupov a práv		ÁNO	ÁNO
110.	používatelia majú prijaté primerané opatrenia na ochranu a udržiavanie pridelených autentifikačných prostriedkov vrátane nezdieľania autentifikačných prostriedkov s inými osobami		ÁNO	ÁNO
111.	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**
112.	sú určené, uplatnené a kontrolované pravidlá bezpečnej prevádzky pre všetky ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie, najmä 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 prevádzkovej dokumentácii ITVS, 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	ÁNO	ÁNO	ÁNO
113.	prevádzkové postupy pre zariadenia na spracovanie informácií, siete a informačné systémy sú zdokumentované a sprístupnené zamestnancom podľa ich potreby		ÁNO	ÁNO

114.	sa zabraňuje 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
115.	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
116.	je dostupná dostatočná kapacita podporných aktív, ktorá je priebežne monitorovaná spôsobom v závislosti od typu aktíva		ÁNO	ÁNO
117.	systémový čas príslušných podporných aktív, ktoré spracúvajú informácie alebo podporujú ich spracovanie, je synchronizovaný so schválenými zdrojmi času, zohľadňujúcimi časové zóny		ÁNO	ÁNO
118.	používanie systémových programových prostriedkov, ktoré môžu byť schopné obísť systémové a aplikačné opatrenia, je obmedzené a kontrolované		ÁNO	ÁNO
119.	sú zavedené postupy a opatrenia na bezpečné riadenie inštalácie programových prostriedkov a informačných systémov do produkčnej prevádzky		ÁNO	ÁNO
120.	zmeny procesov a systémov podliehajú schválenému procesu riadenia zmien		ÁNO	ÁNO
121.	sa aktualizuje príslušný bezpečnostný projekt pre ISVS pri všetkých významných zmenách implementovaných na úrovni systému		ÁNO	ÁNO
122.	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

123.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie systémov AI[5]) a riadená kybernetická bezpečnosť pri používaní umelej inteligencie		ÁNO	ÁNO
124.	je definovaný a zavedený proces riadenia výnimiek zo schválených bezpečnostných opatrení		ÁNO	ÁNO
125.	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**
126.	sú definované a zavedené procesno-organizačné a technické bezpečnostné opatrenia pre aktíva organizácie (servery, koncové zariadenia, mobilné zariadenia) s aktívnym prístupom používateľov alebo prístupné z internetu, ktoré pristupujú ku všetkým ISVS a ITVS	ÁNO	ÁNO	ÁNO
127.	je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov	ÁNO	ÁNO	ÁNO
128.	je zavedená pravidelná aktualizácia ITVS a ISVS s cieľom zabezpečiť minimálne narušenie bežnej prevádzky		ÁNO	ÁNO
129.	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**
130.	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

[5]) Čl. 3 ods. 1 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).

131.	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
132.	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
133.	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
134.	sú určené, zavedené a monitorované bezpečnostné funkcie, úrovne služieb a požiadavky týkajúce sa sieťových služieb		ÁNO	ÁNO
135.	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
136.	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**
137.	pri prevádzke všetkých ISVS a ITVS v súlade s bezpečnostnými cieľmi organizácie je definovaný, zavedený a kontrolovaný systém zberu logov a monitorovania kybernetickej bezpečnosti a informačnej bezpečnosti organizácie, ktorý obsahuje a) zoznam systémov, v ktorých dochádza ku tvorbe a zberu logov, b) typy a obsah zbieraných logov a informácií zo systémov, c) postupy na sledovanie a uchovávanie logov	ÁNO	ÁNO	ÁNO
138.	uchováva vybrané logy v rámci správy ISVS a ITVS pre potreby spätného dohľadania udalostí	ÁNO	ÁNO	ÁNO

139.	sú určené, zavedené a používané mechanizmy a nástroje na zber a uchovávanie logov a monitoring pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
140.	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 je zabránené zmene ich integrity a neoprávneným prístupom k nim		ÁNO	ÁNO
141.	záznamy o činnostiach obsahujú informáciu o pôvodcovi vykonanej činnosti		ÁNO	ÁNO
142.	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
143.	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**
144.	identifikuje a vedie zoznam všetkých lokalít, kde sa prevádzkuje alebo používa akýkoľvek prvok ISVS a ITVS	ÁNO	ÁNO	ÁNO
145.	sú definované a zavedené procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre lokality, v ktorých sú fyzicky umiestnené centrálne serverové prvky všetkých ISVS a ITVS	ÁNO	ÁNO	ÁNO
146.	sú definované a zavedené procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre lokality organizácie, v ktorých používatelia pristupujú logicky ku všetkým ISVS a ITVS	ÁNO	ÁNO	ÁNO
147.	sú definované a používané bezpečnostné perimetre na ochranu oblastí, ktoré obsahujú aktíva pre ITVS a ISVS		ÁNO	ÁNO
148.	priestory, v ktorých sa nachádzajú riadiace a serverové súčasti ITVS a ISVS, majú definované pravidlá fyzickej bezpečnosti		ÁNO	ÁNO

149.	fyzický prístup k určeným aktívam správcu, ktoré sú významné z hľadiska bezpečnosti a prevádzky ISVS, je povolený výhradne autorizovaným osobám		ÁNO	ÁNO
150.	je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení		ÁNO	ÁNO
151.	zabezpečené priestory sú nepretržite monitorované z hľadiska neoprávneného fyzického prístupu		ÁNO	ÁNO
152.	sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu		ÁNO	ÁNO
153.	sú monitorované a vizuálne zaznamenávané všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu			ÁNO
154.	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
155.	sú vypracované a pravidelne aktualizované zásady bezpečného správania sa pri používaní ISVS a ITVS, ktoré obsahujú súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov	ÁNO	ÁNO	ÁNO
156.	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
157.	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
158.	sú riadené riziká vyplývajúce z hrozieb fyzického prostredia a z neoprávneného fyzického prístupu k aktívam		ÁNO	ÁNO
159.	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

160.	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
161.	dáta uložené v koncových zariadeniach používateľov spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich sú chránené		ÁNO	ÁNO
162.	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**
163.	je definovaná a zavedená klasifikácia informácií v organizácii a príslušná klasifikačná stupnica; organizácia správcu klasifikuje informácie spracúvané v ISVS a ITVS na úrovni systémov	ÁNO	ÁNO	ÁNO
164.	informácie sú klasifikované na základe potrieb správcu a na základe požiadaviek na dôvernosť, integritu a dostupnosť a špecifických požiadaviek zainteresovaných strán		ÁNO	ÁNO
165.	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
166.	sú preukázateľne zabezpečené primerané bezpečnostné opatrenia na ochranu informácií v organizácii pre všetky ISVS a ITVS na základe klasifikácie informácií v celom životnom cykle spracúvania informácie	ÁNO	ÁNO	ÁNO
167.	sú vypracované a zavedené postupy na označovanie informácií v súlade s prijatou klasifikačnou schémou		ÁNO	ÁNO
168.	je zabezpečený súlad so všeobecne záväznými právnymi predpismi a zmluvnými požiadavkami týkajúcimi sa práv duševného vlastníctva a používania patentovaných produktov		ÁNO	ÁNO
169.	záznamy sú chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným zverejnením		ÁNO	ÁNO

170.	sú preukázateľne zabezpečené primerané technické a organizačné opatrenia na ochranu osobných údajov v organizácii 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**
171.	identifikuje a vedie zoznam všetkých dodávateľov a tretích strán, ktorí podporujú organizáciu pri vývoji, nákupe, údržbe, prevádzke a riadení kybernetickej bezpečnosti a informačnej bezpečnosti pre všetky ISVS a ITVS	ÁNO	ÁNO	ÁNO
172.	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
173.	je definovaný a zavedený systém určenia kritickosti dodávateľa a tretej strany organizácie správcu, ktorý obsahuje a) postup pre určenie kritického dodávateľa a tretej strany podľa tejto vyhlášky, b) samotné určenie kritickosti dodávateľa a tretej strany podporujúcej ISVS a ITVS	ÁNO	ÁNO	ÁNO
174.	na základe výsledkov preskúmania rizík dodávateľa prijme primerané procesno-organizačné, fyzické a technické bezpečnostné opatrenia pre celý subdodávateľský reťazec; pre zavedenie povinnosti dodržiavať vybrané bezpečnostné opatrenia treťou stranou sa uzavrie zmluva s dodávateľom (treťou stranou)	ÁNO	ÁNO	ÁNO
175.	sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán	ÁNO	ÁNO	ÁNO
176.	na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami je s každou treťou stranou s významným vplyvom uzatvorená zmluva		ÁNO	ÁNO
177.	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
178.	vykoná raz ročne posúdenie rizík dodávateľov s významným vplyvom a účinnosti príslušných bezpečnostných opatrení definovaných v zmluvách s dodávateľmi; v závislosti od výsledkov	ÁNO	ÁNO	ÁNO

	vykoná organizácia aj aktualizáciu určenia kritickosti dodávateľov a revíziu prijatých bezpečnostných opatrení definovaných v zmluvách			
179.	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 ITVS a ISVS správcu		ÁNO	ÁNO
180.	sú vypracované, aktualizované a účinné prevádzkové zmluvy týkajúce sa ITVS a ISVS (tzv. SLA) s príslušnými bezpečnostnými opatreniami vzťahujúcimi sa na dodávateľov a tretie strany		ÁNO	ÁNO
181.	sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky na používanie cloudových služieb a riadená kybernetická bezpečnosť a informačná bezpečnosť pri používaní cloudových služieb		ÁNO	ÁNO

Vysvetlivky:

ITVS – informačná technológia verejnej správy
ISVS – informačný systém verejnej správy