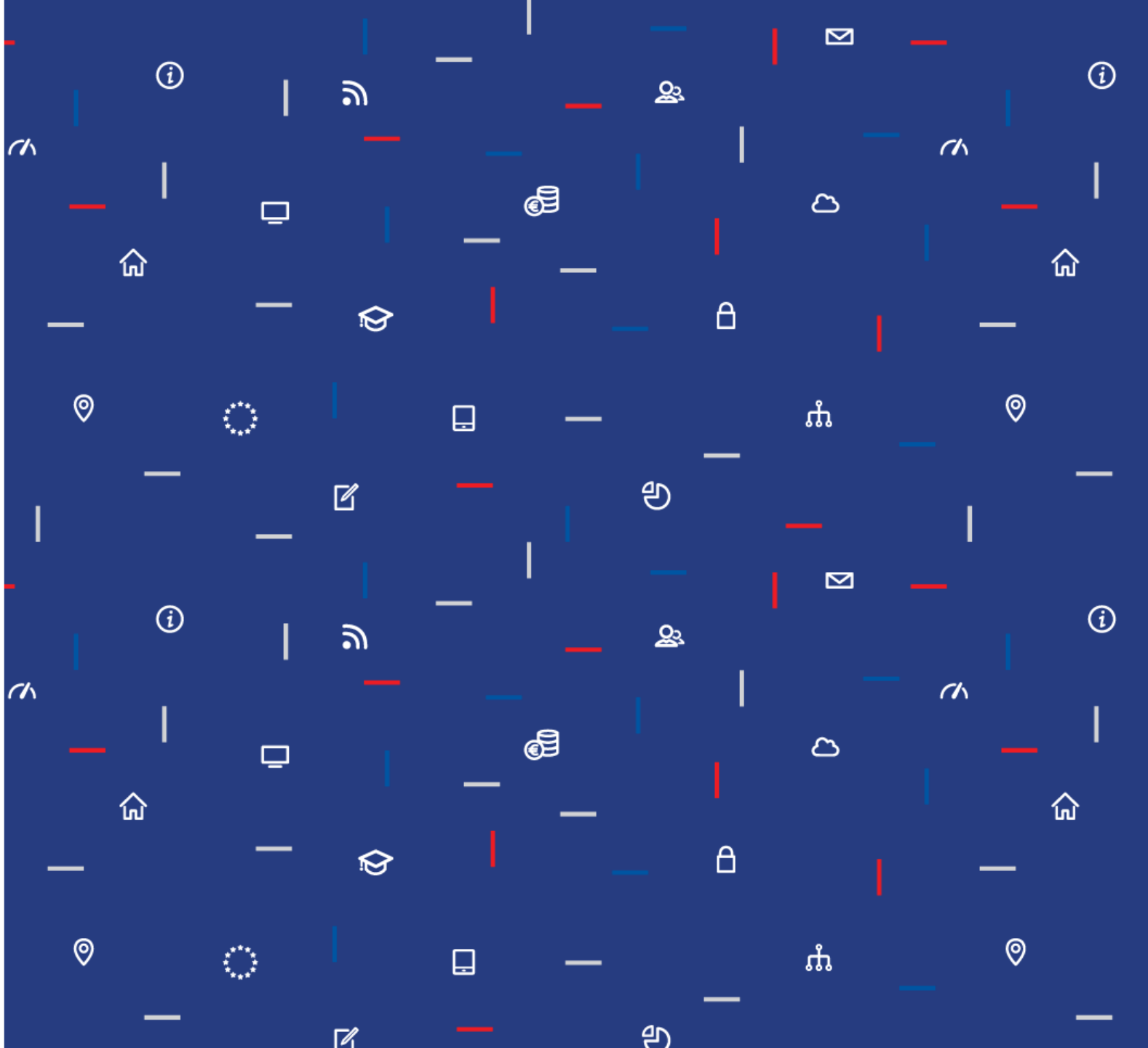
ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

LEGISLATÍVNY RÁMEC K BEZPEČNOSTI

ISVS/ ITVS / Výnos o štandardoch pre ISVS

PhDr.JUDr.Mgr. Ervín Šimko

Odbor Riadenia Informačnej a Kybernetickej Bezpečnosti



Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy

§ 2 písm. d):

ÚPPVII **kontroluje dodržiavanie povinností ustanovených týmto zákonom**; vykonávaním niektorých činností pri kontrole dodržiavania štandardov, s výnimkou kontroly dodržiavania štandardov týkajúcich sa bezpečnosti podľa písmena f), môže ministerstvo poveriť inú fyzickú osobu alebo právnickú osobu, pričom rozsah týchto činností ministerstvo určí v poverení v rámci svojich právomocí ustanovených týmto zákonom,

§ 2 písm. f):

UPPVII **riadi a koordinuje informačnú bezpečnosť** informačných systémov verejnej správy,

§ 6 ods. 1:

Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, **najmä pokiaľ ide o bezpečnosť a integrovateľnosť informačných systémov verejnej správy.** Štandardy musia byť otvorené a technologicky neutrálne.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk
Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 1 ods. 2: pôsobnosť

Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností) a citlivých informácií.

§ 9 ods. 2:

Na postup pri výkone kontroly podľa odseku 1 písm. t) sa použijú základné pravidlá kontrolnej činnosti v štátnej správe.) Vykonávaním niektorých činností pri kontrole dodržiavania štandardov, okrem kontroly dodržiavania podmienok týkajúcich sa bezpečnosti, môže orgán vedenia poveriť inú osobu, pričom rozsah týchto činností orgán vedenia určí v poverení v rozsahu svojej pôsobnosti.

§ 11 ods. 5:

Pri vypracúvaní vnútorných predpisov na účely podľa § 14 až 17 a pri riadení bezpečnosti informačných technológií verejnej správy vychádza orgán riadenia

a) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem, a

b) z metodických usmernení orgánu vedenia.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 12 ods. 1 písm. a):

Orgán riadenia je povinný **zabezpečovať** plynulú, **bezpečnú** a spoľahlivú **prevádzku informačných technológií verejnej správy**, ktorých je správcom, vrátane organizačného, odborného a technického zabezpečenia a zabezpečenia proti zneužitiu, a to v súlade s týmto zákonom, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a národnou koncepciou,

§ 14 ods. 1 písm. i):

Správca je na úseku plánovania a organizácie informačných technológií verejnej správy povinný zabezpečiť riadenie bezpečnosti.

§ 14 ods. 5:

V rámci nastavenia organizačnej štruktúry, procesov a nástrojov, potrebných na riadenie je správca povinný zabezpečiť také organizačné podmienky a procesné podmienky, aby zabezpečil riadny výkon povinností pri riadení informačných technológií verejnej správy a realizoval určené strategické ciele. Organizačnými podmienkami sa rozumie najmä určenie zodpovedných organizačných útvarov a riadiacich pozícií na strategickej, programovej, projektovej a operačnej úrovni riadenia. Procesnými podmienkami sa rozumie najmä určenie postupov riadenia informačných technológií verejnej správy a kontrola dodržiavania všeobecne záväzných právnych predpisov v tejto oblasti, ako aj riadenie kvality, rizík a bezpečnosti informačných technológií verejnej správy. Správca zabezpečuje organizačné podmienky a procesné podmienky, najmä potrebné riadiace pozície, kvalifikačné predpoklady a požiadavky na certifikáciu, v rozsahu a spôsobom v závislosti od veľkosti a od komplexnosti informačných technológií verejnej správy a poskytovaných služieb.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 13 ods. 3 písm. b):

V rámci zabezpečenia správy servisných požiadaviek a prevádzkových incidentov je správca povinný poskytnúť orgánu vedenia na požiadanie, najmenej raz za šesť mesiacov správu o počte a charaktere nahlásených, riešených a uzavretých servisných požiadavkách a prevádzkových incidentoch, okrem informácií, ktorých zverejnenie by bolo rizikové z pohľadu bezpečnosti informačnej technológie verejnej správy, a to v rozsahu a spôsobom podľa dohody s orgánom vedenia

Bezpečnosť informačných technológií verejnej správy:

§ 18

Základné ustanovenia

(1) Povinnosť správcu, ktorý je prevádzkovateľom základnej služby,) prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje osobitný predpis.)

(2) Obsah bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a spôsob a rozsah ich prijímania a realizácie v súlade s osobitným predpisom) ustanovuje tento zákon.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk
Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 19 Bezpečnosť informačných technológii verejnej správy v oblasti plánovania a organizácie

(1) V rámci zabezpečenia riadenia bezpečnosti podľa § 14 ods. 1 písm. i) je správca povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý

a) určí ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti vo forme bezpečnostnej politiky alebo inak zdokumentovaných a schválených mechanizmov riadenia bezpečnosti informačných technológií verejnej správy,

b) zriadi riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené,

c) zabezpečí identifikovanie aktív v informačných technológiách verejnej správy, zraniteľností a relevantných hrozieb a hodnotenie rizík vyplývajúcich z hrozieb, najmä vo forme bezpečnostného projektu podľa § 23 ods. 1 a 2, v nadväznosti na kritickosť aktív v informačných technológiách verejnej správy, ich vývoj a na zmeny všeobecne záväzných právnych predpisov a podmienok v organizácii správcu,

d) zadefinuje mechanizmy rozhodovania o spôsobe riadenia identifikovaných rizík,

e) identifikuje potrebné bezpečnostné opatrenia,

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

f) určí bezpečnostné mechanizmy na procesnej, organizačnej a na technickej úrovni, v nadväznosti na identifikované bezpečnostné opatrenia a rozhodnutia o spôsobe riadenia rizika, a určí opatrenia na ochranu bezpečnosti a integrity informácií vrátane opatrení včasného varovania,

g) určí prostriedky na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení,

h) určí prostriedky kontroly uplatňovania bezpečnostných mechanizmov,

i) určí postupy riešenia bezpečnostných incidentov pri narušení definovaných bezpečnostných cieľov v nadväznosti na mechanizmy riešenia bezpečnostných incidentov.

(2) Správca prostredníctvom riadiacej zložky systému riadenia bezpečnosti zabezpečuje prerokovanie a schválenie

a) koncepčných dokumentov a strategických opatrení týkajúcich sa bezpečnosti informačných technológií verejnej správy,

b) informácií o zaznamenaných bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného výskytu,

c) návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov bezpečnosti informačných technológií verejnej správy.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(3) Správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje

a) vypracovanie a aktualizáciu dokumentov upravujúcich systém riadenia bezpečnosti podľa odseku 1,

b) vyhodnocovanie stavu bezpečnosti informačných technológií verejnej správy najmenej jedenkrát do roka vo forme správy a jej predloženie riadiacej zložke,

c) realizáciu bezpečnostných opatrení,

d) plánovanie, koordináciu a vyhodnocovanie činností súvisiacich s riadením bezpečnostných rizík v oblasti bezpečnosti informačných technológií verejnej správy,

e) koordináciu riešenia bezpečnostných incidentov,

f) organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií verejnej správy.

(4) Správca prostredníctvom kontrolnej zložky systému riadenia bezpečnosti zabezpečuje

a) nezávislú kontrolu dodržiavania povinností v oblasti bezpečnosti informačných technológií verejnej správy,

b) hodnotenie súladu stavu bezpečnosti s požiadavkami všeobecne záväzných právnych predpisov.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(5) Správca pri plánovaní vytvorenia alebo nadobudnutia informačného systému verejnej správy

a) určí kategóriu informačného systému verejnej správy, do ktorej bude z hľadiska klasifikácie informácií a kategorizácie sietí a informačných systémov patriť,

b) vypracuje bezpečnostnú politiku, definuje bezpečnostné problémy, ktoré ochrana informačného systému verejnej správy musí riešiť a navrhne riešenie týchto problémov formou bezpečnostných cieľov,

c) určí osobu zodpovednú za bezpečnosť informačného systému verejnej správy, ktorá

1. rozpracuje bezpečnostné ciele podľa písmena b) do podoby bezpečnostných požiadaviek na vývoj alebo na dodanie informačného systému verejnej správy,

2. vypracuje plán postupu pre naplnenie bezpečnostných požiadaviek podľa prvého bodu a dohliada na ich dodržiavanie,

d) vypracuje analýzu rizík prostredia, v ktorom bude informačný systém verejnej správy prevádzkovaný.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk
Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 20 Bezpečnosť informačných technológii verejnej správy v oblasti obstarávania a implementácie

(1) Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy

a) určí bezpečnostné požiadavky na informačný systém verejnej správy vrátane podmienok jeho vývoja, testovania a dodania, v podmienkach vytvorenia alebo dodania informačného systému verejnej správy,

b) poskytne dodávateľovi informačného systému verejnej správy pseudonymizované kópie údajov alebo fiktívne údaje na testovanie informačného systému verejnej správy a jeho vývoj, ak poskytnutie údajov neznamená pre správcu neprimeranú záťaž s ohľadom na prínos poskytnutia pre testovanie a vývoj,

c) zabezpečí pre tento systém vypracovanie bezpečnostného projektu podľa § 23 ods. 1 a 2.

(2) Dodávateľ informačného systému verejnej správy pre vývoj tohto systému

a) zabezpečí

1. bezpečné vývojové prostredie,
2. dokumentáciu vývoja vrátane používateľskej dokumentácie a administrátorskej dokumentácie.

b) je oprávnený zabezpečiť vytvorenie časti informačného systému verejnej správy treťou osobou len po predchádzajúcom písomnom informovaní správcu,

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

c) je povinný

1. dodržiavať mlčanlivosť o dodávanom informačnom systéme verejnej správy aj po ukončení dodania a zaviazať rovnakou povinnosťou všetky osoby, ktoré sa na dodaní podieľali,

2. dodržiavať vhodné bezpečnostné mechanizmy a preukázať, že ich rozsah a úroveň zodpovedajú bezpečnostným požiadavkám podľa odseku 1 písm. a),

3. identifikovať bezpečnostné požiadavky na informačný systém verejnej správy podľa odseku 1 písm. a), ktoré nie sú pokryté týmto systémom, a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude informačný systém verejnej správy prevádzkovaný,

4. upozorniť správcu na kritické časti alebo na rizikové časti informačného systému verejnej správy, ktoré odhalí pri jeho dodaní a navrhnúť opatrenia na ich riešenie,

5. preukázateľne odstrániť alebo znemožniť používanie funkcie informačného systému verejnej správy, ktoré by jemu alebo tretej strane umožňovali získať neoprávnený prístup do tohto systému a k údajom, ktoré obsahuje.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk
Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 20 Bezpečnosť informačných technológii verejnej správy v oblasti prevádzky, servisu a podpory

(1) V rámci zabezpečenia riadenia služieb bezpečnosti prevádzky podľa § 16 ods. 1 písm. d) správca zabezpečuje

a) zavedenie informačného systému verejnej správy do prevádzky,

b) prevádzku informačného systému verejnej správy,

c) vyradenie informačného systému verejnej správy z prevádzky.

(2) V rámci zabezpečenia zavedenia informačného systému verejnej správy do prevádzky správca

a) overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek pred zavedením do prevádzky a nezavedie do prevádzky informačný systém verejnej správy, ktorý tieto požiadavky nespĺňa,

b) dbá na to, aby pri zavádzaní informačného systému verejnej správy do prevádzky nebol dodávateľovi umožnený prístup k ostatným informačným systémom a údajom, ktoré sa v nich spracúvajú, a ak to nie je možné, zabezpečiť potrebnú kontrolu dodávateľa po celý čas, po ktorý je potrebný prístup k ostatným informačným systémom alebo k údajom, ktoré sa v nich spracúvajú, a zaviazať dodávateľa záväzkom mlčanlivosti vo vzťahu k údajom v informačných systémoch a povinnosťou použiť ich len na účel zavádzania informačného systému do prevádzky.

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(3) V rámci zabezpečenia prevádzky informačného systému verejnej správy správca

a) zabezpečí pre informačný systém verejnej správy

1. určenie a pravidelné aktualizovanie bezpečnostných cieľov,

2. naplnenie bezpečnostných cieľov a eliminovanie negatívnych vplyvov a udalostí na informačný systém verejnej správy pri jeho prevádzkovaní,

b) v závislosti od zaradenia informačného systému verejnej správy z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov

1. aktualizuje bezpečnostný projekt pre tento systém vypracovaný podľa § 20 ods. 1 písm. c),

2. zavedie jednotný systém riadenia informačnej bezpečnosti pre všetky informačné systémy, ktoré sú v jeho správe,

3. zabezpečí riadenie konfigurácie informačného systému verejnej správy a jeho častí,

4. určí bezpečnostne závažné operácie, ktorými sa rozumejú najmä správa prístupov a prístupových údajov, ukladanie záznamov o systémových udalostiach, realizácia bezpečného oddelenia vnútornej časti systému a siete od vonkajšej časti a zavedie dokumentovanie postupov pre tieto operácie,

5. zabezpečí nepretržitý monitoring informačného systému verejnej správy,

6. zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch, určených najmä s ohľadom na dôležitosť informačného systému verejnej správy a na minulé zistenia bezpečnostných auditov a pri zistení závažných bezpečnostných nedostatkov prepracuje bezpečnostný projekt a naň nadväzujúce dokumenty.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(4) V rámci vyradenia informačného systému verejnej správy z prevádzky správca

a) vypracuje plán vyradenia informačného systému verejnej správy z prevádzky, ktorý obsahuje najmä

1. uchovanie kritických informácií vyraďovaného informačného systému verejnej správy, ktoré sú už nepotrebné pre funkčnosť iného informačného systému,

2. spoľahlivé odstránenie informácií z pamäťových médií vyraďovaného informačného systému verejnej správy,

3. postup vyraďovania programových prostriedkov a technických prostriedkov informačného systému verejnej správy,

b) zabezpečí, aby nedošlo ku strate alebo k úniku informácií a k narušeniu práv priemyselného vlastníctva a duševného vlastníctva.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 22 Bezpečnosť informačných technológii verejnej správy v oblasti monitoringu a hodnotenia

V oblasti monitoringu a hodnotenia správca vo vzťahu k informačným technológiám v jeho správe prijíma a vykonáva bezpečnostné opatrenia pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov podľa osobitného predpisu.

§ 23 Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

(1) Bezpečnostný projekt informačného systému verejnej správy je dokument obsahujúci komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek a návrh spôsobu ich efektívneho naplnenia. Bezpečnostný projekt môže byť vypracovaný aj pre viacero informačných systémov verejnej správy, ktoré sú v správe jedného správcu. Vypracovanie bezpečnostného projektu informačného systému verejnej správy zabezpečí správca, vychádzajúc

a) z bezpečnostnej politiky,

b) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem,

c) z metodických usmernení orgánu vedenia.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(2) Správca vypracuje bezpečnostný projekt vždy pre informačný systém verejnej správy, ktorý je z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov v najvyššej kategórii z hľadiska jeho významnosti, funkcie a účelu použitia s ohľadom na potrebu zabezpečenia ochrany dôvernosti a integrity a zabezpečenia dostupnosti a úrovne činností vykonávaných s jeho použitím.

(3) Orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti sú povinní vo vzťahu k informačným technológiám verejnej správy

a) ak sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu,) nahlasovať spôsobom podľa osobitného predpisu) aj kybernetický bezpečnostný incident,) na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu;) ak nie sú do tohto registra zaradení, nahlasujú takýto kybernetický bezpečnostný incident orgánu vedenia ním určeným spôsobom,

b) zasielať automatizovaným spôsobom a najviac v rozsahu ustanovenom v štandardoch orgánu vedenia ním určené systémové informácie z informačných technológií verejnej správy,

c) poskytnúť orgánu vedenia súčinnosť a spoluprácu pri plnení jeho úloh podľa odseku 5,

d) prijať alebo upraviť bezpečnostné opatrenia vrátane vypracovania bezpečnostného projektu, ak bezpečnostný audit alebo hodnotenie zraniteľnosti, vykonané orgánom vedenia zistí riziko) alebo hrozbu) pre informačnú technológiu verejnej správy a oznámiť mu prijaté alebo upravené bezpečnostné opatrenia,

e) zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c),

f) určiť jeden kontaktný bod na nahlasovanie podľa písmena a).

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

(4) Orgán riadenia, neuvedený v odseku 3, je povinný plniť povinnosti podľa odseku 3 písm. a), c), e) a f).

(5) Orgán vedenia vo vzťahu k informačným technológiám verejnej správy

a) môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia kybernetického bezpečnostného incidentu podľa odseku 3 písm. a), jeho predchádzania alebo odstraňovania zistení bezpečnostného auditu alebo hodnotenia zraniteľnosti,

b) zbiera, spracúva a vyhodnocuje systémové informácie na účely predchádzania kybernetickým bezpečnostným incidentom, ich riešenia a obnovenia kybernetickej bezpečnosti,)

c) vykonáva pravidelné, neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií, poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu,

d) môže na žiadosť orgánu riadenia podľa odseku 3 za tento orgán riadenia vykonať bezpečnostný audit alebo pre neho vykonať hodnotenie zraniteľnosti.

§ 29 ods. 1- Správne delikty

Orgán vedenia uloží pokutu od 500 eur do 35 000 eur správcovi, ktorý poruší povinnosť podľa § 6 ods. 1, § 12 ods. 1 písm. a), § 14 ods. 6, § 15 ods. 2 alebo § 16 ods. 3 písm. e) alebo povinnosti na úseku bezpečnosti informačných technológií verejnej správy podľa § 19 až 21 alebo § 23,

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Zákon č. 95/ 2019 o informačných technológiách vo verejnej správe

§ 31 písm. i):

Všeobecne záväzný právny predpis, ktorý sa v Zbierke zákonov Slovenskej republiky vyhlasuje uverejnením úplného znenia a ktorý vydá úrad podpredsedu vlády, ustanoví podrobnosti o bezpečnosti informačných technológií verejnej správy podľa § 18 až 23, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov,

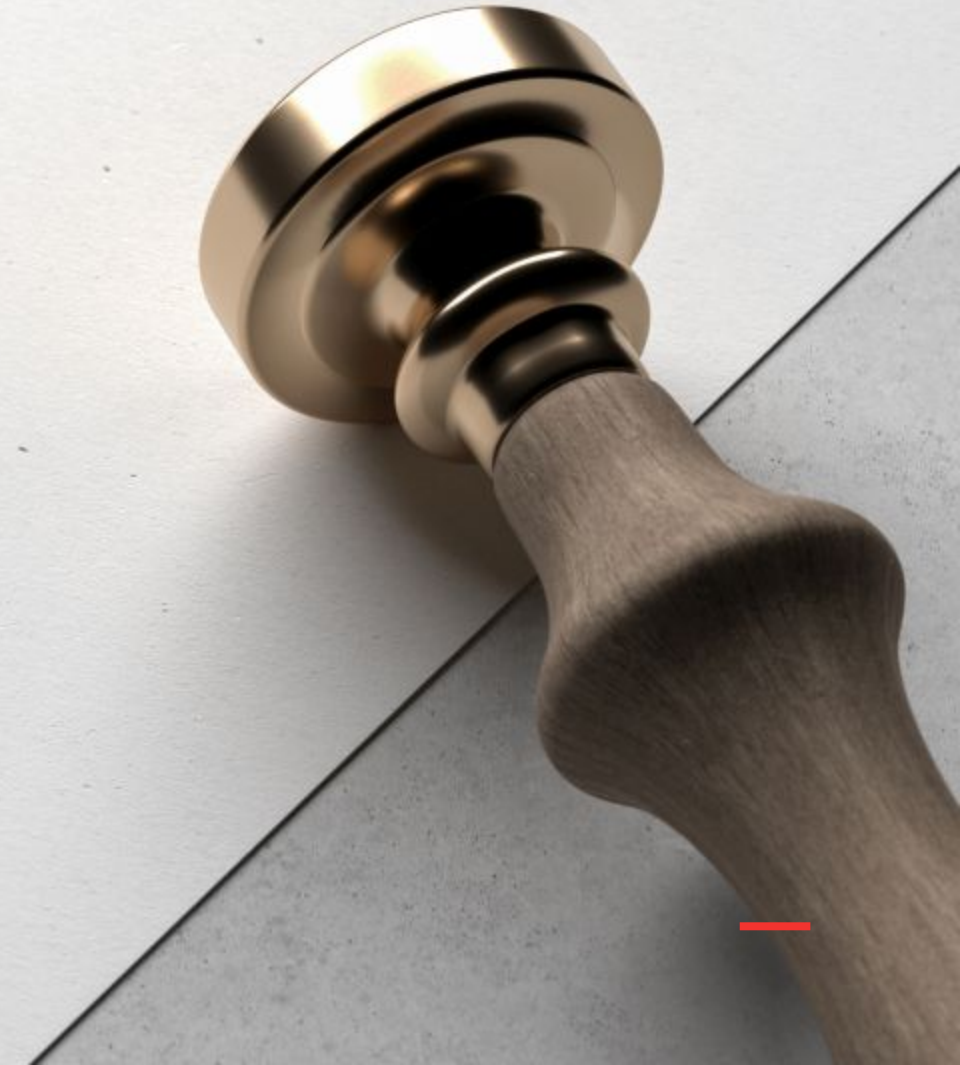
§ 33 ods. 5:

Do uplynutia 30 dní odo dňa zriadenia a uvedenia do prevádzky jednotného informačného systému kybernetickej bezpečnosti) nahlasuje orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, ktorí sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu, kybernetický bezpečnostný incident podľa § 23 ods. 3 písm. a) orgánu vedenia ním určeným spôsobom.

+ 421 2 2092 8xxx
kontakt@vicepremier.gov.sk

Štefánikova 15 - 811 05 Bratislava
www.vicepremier.gov.sk

Ďakujem
za pozornosť



PhDr.JUDr.Mgr.Ervín Šimko