ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2014

Vyhlásené: 13. 3. 2014 Časová verzia predpisu účinná od: 1. 5.2020 do: 29. 6.2020

55

VÝNOS

Ministerstva financií Slovenskej republiky

zo 4. marca 2014,

o štandardoch pre informačné systémy verejnej správy

Ministerstvo financií Slovenskej republiky (ďalej len „ministerstvo“) podľa § 13 ods. 1 písm. a) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) ustanovuje:

Základné ustanovenia

§ 1
Štandardy pre informačné systémy verejnej správy

Týmto výnosom sa ustanovujú štandardy pre informačné systémy verejnej správy, ktorými sú

e) bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje, a to

1. štandardy pre architektúru riadenia,
2. štandardy minimálneho technického zabezpečenia.

§ 2
Vymedzenie základných pojmov

Na účely tohto výnosu sa rozumie

a) správcom obsahu povinná osoba zodpovedná za správu obsahu webového sídla a na ňom zverejnené informácie; správca obsahu je zároveň správcom daného informačného systému verejnej správy,

b) technickým prevádzkovateľom prevádzkovateľ informačného systému verejnej správy podľa zákona, ktorý vykonáva činnosti určené správcom obsahu v súvislosti s technickou prevádzkou webového sídla,

c) aktívami programové vybavenie, technické zariadenia, poskytované služby, kvalifikované osoby, dobré meno povinnej osoby a informácie, dokumentácia, zmluvy a iné skutočnosti, ktoré považuje povinná osoba za citlivé,

d) bezpečnostným incidentom akýkoľvek spôsob narušenia bezpečnosti informačných systémov verejnej správy, ako aj akékoľvek porušenie bezpečnostnej politiky povinnej osoby a pravidiel súvisiacich s bezpečnosťou informačných systémov verejnej správy,

e) technickými komponentmi informačného systému verejnej správy tie časti informačného systému verejnej správy a informačno-komunikačné technológie, ktoré nie sú určené na uchovávanie údajov, napríklad štruktúrovaná kabeláž, sieťové karty a zdroje,

f) zariadeniami informačného systému verejnej správy tie časti informačného systému verejnej správy, ktoré môžu uchovávať údaje, napríklad pamäťové médiá a počítače vrátane prenosných počítačov,

g) súborom postupnosť údajov v elektronickej forme, ktorá je označená názvom, informáciou o kapacite údajov a časovou značkou o jej poslednej zmene,

h) dátovým prvkom jednotka údajov, ktorá je jednoznačne a nedeliteľne špecifikovaná prostredníctvom súboru atribútov,

i) gestorom dátového prvku povinná osoba zodpovedná za správnosť a aktuálnosť atribútov dátového prvku; gestor dátového prvku nezodpovedá za obsah prenášaný dátovým prvkom,

j) používateľom služby osoba alebo informačný systém, ktorí používajú alebo požadujú poskytovanie služby verejnej správy,

k) gestorom služby osoba poverená vykonávať riadenie a koordinovanie určitého úseku verejnej správy,

l) projektom jednorazový proces zameraný na dosiahnutie definovaného cieľa, pozostávajúci zo súboru zosúladených, riadených a časovo ohraničených činností, ktorý

   1. je pre danú organizáciu jedinečný, pričom to nie je pravidelná činnosť,
   2. má presne určený začiatok a koniec trvania,
   3. má definované najmenej finančné zdroje a ľudské zdroje, ak sú potrebné,
   4. vyžaduje analýzu súčasného stavu, špecifikáciu cieľového stavu a spôsobu jeho dosiahnutia,

m) malým projektom projekt, ktorého celková cena je najviac 69 999 eur a zmluvná lehota jeho trvania nie je dlhšia ako 180 kalendárnych dní,

n) veľkým projektom projekt, ktorého celková cena je 1 000 000 eur alebo vyššia alebo zmluvná lehota jeho trvania je dlhšia ako 544 kalendárnych dní,

o) stredným projektom projekt, ktorý nespĺňa podmienky podľa písmen m) a n),

p) informačno-technologickým projektom projekt, ktorý súvisí so zavádzaním, správou alebo podporou informačno-komunikačných technológií a týka sa tvorby a úpravy informačných systémov verejnej správy,

q) programom skupina projektov riadených koordinovaným spôsobom za účelom dosiahnutia spoločného cieľa a zvýšených prínosov a umožnenia efektívnej kontroly projektov a efektívneho riadenia projektov, čo nie je možné dosiahnuť, ak by sa projekty riadili samostatne,

r) datasetom ucelená a samostatne použiteľná skupina súvisiacich údajov vytvorených a udržiavaných na určitý účel, uložených spoločne podľa rovnakej schémy a poskytovaných prostredníctvom súboru alebo aplikačného rozhrania,

s) dátovým zdrojom pôvodné miesto evidencie datasetu,

t) referencovateľným identifikátorom identifikátor, ktorý

   1. má formát Uniform Resource Identifier (URI),
   2. je jednoznačný,
   3. je unikátny,
   4. je dlhodobo stabilný,

5. je formátovo a štrukturálne konzistentný,
6. je manažovateľný tak, aby umožňoval logicky rozširovať stanovenú štruktúru,
7. je jasný, stručný a krátky,
8. je pre fyzickú osobu jednoducho čitateľný, pričom časť referencie môže byť reprezentovaná kódovanou informáciou,
9. neobsahuje programátorské kľúčové slová,
10. neobsahuje interpunkciu a iné znaky okrem znakov lomka, pomlčka, bodka, podčiarkovník, zavináč a mriežka, diakritiku a biele znaky ako sú napríklad medzera, tabulátor, nový riadok,
11. neobsahuje reťazec „www“,
12. neobsahuje interpunkciu okrem znakov lomka, pomlčka a bodka, diakritiku a medzery okrem identifikátora fyzickej osoby podľa osobitného predpisu,[1a]) kde je možné použiť interpunkciu a diakritiku,
13. obsahuje iba malé písmená,
14. nahrádza špeciálne znaky, napríklad výkričník, úvodzovky, percento, hviezdička, zátvorka, dolár alebo mriežka, pomlčkami a podčiarkovníkmi,

u) tripletom znalosť vo forme „subjekt predikát objekt“,

v) prepojenými údajmi údaje vyjadrené referencovateľnými identifikátormi, ktoré sú automatizovane spracovateľné tak, že technické zariadenie, ktoré ich spracúva, porozumie ich významu; na opis údajov sa použijú dátové prvky z Centrálneho modelu údajov,

w) metaúdajmi štruktúrované údaje obsahujúce informácie o primárnych údajoch, pričom primárne údaje spravidla reprezentujú určitý hmotný objekt alebo nehmotný objekt; metaúdaje sú určené najmä na vyhľadávanie, katalogizáciu a využívanie primárnych údajov,

x) cloud computingom model umožňujúci jednoduchý samoobslužný sieťový prístup k službám informačných technológií na vyžiadanie, poskytovaným vo virtuálnom prostredí konfigurovateľných výpočtových zdrojov, ktoré môžu byť pridelené alebo uvoľnené s minimálnym úsilím a časovým obmedzením, a to na základe voliteľného škálovania a navyšovania, nezávisle od lokality zdrojov alebo lokality prístupu k nim a bez osobného kontaktu s poskytovateľom cloudovej služby, pričom využitie týchto služieb je merané a hodnotené podľa ich skutočného využitia,

y) cloudovou službou ľubovoľný prostriedok alebo zdroj cloud computingu, poskytovaný vzdialeným prístupom na základe podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb,

z) dohodou o poskytovanej úrovni cloudových služieb zmluvný vzťah upravujúci parametre a kvalitu poskytovaných cloudových služieb, ktorá obsahuje úlohy a povinnosti zmluvných strán, pričom táto dohoda sa obvykle uzatvára medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb alebo sprostredkovateľom cloudových služieb,

aa) odberateľom cloudových služieb osoba, ktorá na základe dohody o poskytovanej úrovni cloudových služieb využíva cloudové služby poskytovateľa cloudových služieb,

ab) poskytovateľom cloudových služieb osoba zodpovedná za správu cloud computingu a poskytovanie cloudových služieb, a to podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb,

ac) prevádzkovateľom cloudových služieb osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb zabezpečuje technické podmienky na prevádzkovanie, prepojenie a prenos cloudových služieb,

ad) sprostredkovateľom cloudových služieb osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb prevádzkuje využívanie, výkon a dodávku cloudových služieb,

ae) audítorom cloudu osoba nezávislá od poskytovateľa cloudových služieb, určujúca na základe poverenia od tohto poskytovateľa kritériá auditu slúžiace na objektívne získavanie dôkazov o dodržiavaní podmienok poskytovania cloudových služieb a vykonávajúca na základe poverenia od tohto poskytovateľa systematický, nezávislý a zdokumentovaný proces ich vyhodnocovania,

af) identifikačnou registráciou osoby proces, počas ktorého je osoba identifikovaná na základe určitých registračných údajov, z ktorých určené registračné údaje môžu byť potvrdzované, pričom výsledkom registrácie je priradenie určitej identity v určenom kontexte tejto osobe,

ag) registračnou autoritou identifikácie poskytovateľ identifikačnej registrácie,

ah) federáciou identít overovanie identít informačných systémov verejnej správy v správe najmenej dvoch povinných osôb, ktoré sa vykonáva u jedného poskytovateľa identít,

ai) priamo podpísaným elektronickým dokumentom podpísaný elektronický dokument, ku ktorému sú elektronický podpis alebo elektronická pečať, ktorými sa podpisuje, pripojené ako jeho súčasť,

aj) externe podpísaným elektronickým dokumentom podpísaný elektronický dokument, ku ktorému sú elektronický podpis alebo elektronická pečať, ktorými sa podpisuje, pripojené prostredníctvom podpisového kontajneru, prostredníctvom formátu podpisu alebo ako samostatné súbory,

ak) číselníkom množina údajov vo forme jednotlivých položiek číselníka, ktoré sú popísané najmenej dvojicou dátových prvkov "kód položky" a "názov položky"; "kódom položky" je textový reťazec, ktorý je v číselníku jedinečný,

al) základným číselníkom číselník vedený centrálne prostredníctvom informačného systému verejnej správy, slúžiaci na určenie prípustných hodnôt príslušných dátových prvkov, ktoré sú vyjadrené jednotným referencovateľným identifikátorom,

am) dereferenciáciou poskytovanie referencovateľného identifikátora ako funkčného priameho odkazu vo forme Uniform Resource Locator (URL) pre informácie o údaji reprezentovanom referencovateľným identifikátorom a o jeho účele,

an) Centrálnym modelom údajov množina ontológií, ktorá sa používa pri opise dátových prvkov verejnej správy, a ktorá je vyjadrením sémantických vzťahov medzi dátovými prvkami, vyjadrenými prostredníctvom jednotných referencovateľných identifikátorov; je zverejnený v centrálnom metainformačnom systéme,

ao) ontológiou množina prvkov opisujúca určitú oblasť prostredníctvom tripletov,

ap) aplikačným rozhraním programovacie rozhranie informačného systému, ktorým je umožnené pre autorizovaného používateľa používať elektronickú službu,

aq) verejne dostupným aplikačným rozhraním aplikačné rozhranie dostupné komukoľvek po splnení ustanovených podmienok, ktoré umožňuje používať elektronickú službu pomocou vlastných softvérových aplikácií alebo aplikácií tretích strán,

ar) validáciou formátu elektronického dokumentu overenie súladu formátu súboru s príslušnou technickou špecifikáciou programovými prostriedkami.

Bezpečnostné štandardy
Štandardy pre architektúru riadenia

§ 29
Riadenie informačnej bezpečnosti

Štandardom pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby, ktorej obsahom je
   1. určenie bezpečnostných cieľov povinnej osoby z hľadiska informačnej bezpečnosti,
   2. určenie spôsobov vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania ich dosahovania, spôsobov priebežného hodnotenia ich adekvátnosti a spôsobov kontroly postupov využívaných na ich dosahovanie,
   3. určenie úlohy vedenia povinnej osoby pri zaisťovaní informačnej bezpečnosti a uvedenie vyhlásenia vedenia povinnej osoby o podpore bezpečnostnej politiky povinnej osoby,
   4. určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti,
   5. určenie povinnosti pre zaistenie nenarušenia informačnej bezpečnosti povinnej osoby,
   6. zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,
   7. určenie požiadaviek na informačné systémy verejnej správy, vyplývajúce zo všeobecne záväzných právnych predpisov, vnútorných predpisov povinnej osoby a jej zmluvných záväzkov a určenie spôsobu vedenia a aktualizácie dokumentácie o informačných systémoch verejnej správy,
   8. určenie rozsahu a úrovne ochrany všetkých informačných systémov verejnej správy vrátane hodnotenia slabých miest a ohrození,
   9. určenie rámca pre manažment rizík u povinnej osoby v súvislosti s aktívami, od ktorých závisí činnosť informačných systémov verejnej správy, alebo ktoré závisia od činnosti informačných systémov verejnej správy; rámec určí, najmä ktoré aktíva sú pre povinnú osobu kritické, čo ich ohrozuje a zásady ich ochrany,
   10. určenie rozsahu a periodicity auditu informačnej bezpečnosti u povinnej osoby a zároveň určenie udalosti v informačných systémoch verejnej správy, o ktorých sa vytvára záznam auditu,
   11. určenie operačných smerníc pre zálohovanie a určenie ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe,
   12. určenie periodicity monitorovania bezpečnosti a aktualizácie softvéru,
   13. určenie dokumentov, ktoré povinná osoba na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam,
   14. určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby,
b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby,
c) určenie osoby alebo osôb zodpovedných za informačnú bezpečnosť povinnej osoby vrátane zodpovednosti za bezpečnosť všetkých informačných systémov verejnej správy,
d) určenie jednotlivých úloh osoby alebo osôb zodpovedných za informačnú bezpečnosť v súlade s bezpečnostnou politikou povinnej osoby,

e) zabezpečenie koordinácie aktivít organizačných zložiek povinnej osoby pri riešení informačnej bezpečnosti,

f) určenie konkrétnej zodpovednosti za jednotlivé aktíva povinnej osoby,

g) určenie privilegovaných používateľských rolí v informačných systémoch verejnej správy, určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a určenie, ktoré používateľské roly nie je možné navzájom zlúčiť; privilegovanými používateľskými roľami sú najmä správca systému, operátor, používateľ, audítor a programátor.

§ 30
Personálna bezpečnosť

Štandardom pre personálnu bezpečnosť je

a) zabezpečenie, aby boli všetci zamestnanci povinnej osoby a osoby, ktoré vykonávajú činnosti pre povinnú osobu vyplývajúce zo zmluvných záväzkov (ďalej len „tretia strana“) poučení o schválenej bezpečnostnej politike povinnej osoby a o povinnostiach z nej vyplývajúcich,

b) zabezpečenie, aby boli zamestnanci povinnej osoby a tretia strana poučení o svojich právach a povinnostiach predtým, ako získajú prístup k informačnému systému verejnej správy; v prípade rozdielnych práv a povinností pre rôzne informačné systémy verejnej správy sa poučenie zopakuje a jeho obsah sa primerane upraví,

c) zabezpečenie, aby povinnosti vyplývajúce z bezpečnostnej politiky povinnej osoby a z pracovného zaradenia zamestnanca boli uvedené v jeho pracovnej zmluve alebo inom dokumente týkajúcom sa jeho právneho vzťahu s povinnou osobou,

d) vypracovanie postupu pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušia bezpečnostnú politiku povinnej osoby alebo niektorý zo súvisiacich predpisov,

e) zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty v súlade s postupmi podľa § 37,

f) vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí

1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,
2. navrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
3. odstránenie informácií povinnej osoby zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
4. zrušenie prístupových práv v informačných systémoch verejnej správy,
5. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

§ 31
Manažment rizík pre oblasť informačnej bezpečnosti

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti je

a) implementácia systému riadenia a monitorovania rizík v súvislosti s informačnými systémami verejnej správy, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami,

b) používanie systému riadenia a monitorovania rizík pri všetkých procesoch riadenia informačnej

bezpečnosti,

c) identifikácia, analýza a hodnotenie rizík spojených s využívaním aktív a informačných systémov verejnej správy mimo priestorov povinnej osoby a zavedenie primeraných postupov a opatrení na redukciu týchto rizík,

d) analyzovanie procesov povinnej osoby, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti na informačných systémoch verejnej správy a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú kritickými procesmi,

e) analyzovanie rizík, vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy; tieto informačné systémy sú kritickými informačnými systémami verejnej správy,

f) vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy,

g) vedenie zoznamu aktív spôsobom určeným orgánom vedenia, a to najmenej v rozsahu zoznamu

1. verejných IPv4 a IPv6 adries,
2. používaných webových sídiel a ich doménových mien,
3. používaných operačných systémov a ich verzií,
4. používaných technológií.

§ 32
Kontrolný mechanizmus riadenia informačnej bezpečnosti

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je

a) dodržiavanie bezpečnostnej politiky povinnej osoby a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti, ktorého periodicita sa určuje v bezpečnostnej politike povinnej osoby,

b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ.

Štandardy minimálneho technického zabezpečenia

§ 33
Ochrana proti škodlivému kódu

Štandardom pre ochranu proti škodlivému kódu je

a) zavedenie ochrany informačných systémov verejnej správy pred škodlivým kódom najmenej v rozsahu

1. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
2. detekcie prítomnosti škodlivého kódu na všetkých používaných zariadeniach informačného systému verejnej správy,
3. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
4. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach povinnej osoby,

b) zavedenie ochrany pred nevyžiadanou elektronickou poštou,

c) používanie len takého softvéru, ktorý je legálny a povolený príslušnými vnútornými predpismi povinnej osoby,

d) určenie pravidiel pre sťahovanie súborov prostredníctvom externých sietí,

e) podpora zabezpečenia autenticity a integrity súborov pomocou kryptografických prostriedkov, ktorým je najmä elektronický podpis,

f) podpora šifrovania elektronických dokumentov.

§ 34
Sieťová bezpečnosť

Štandardom pre sieťovú bezpečnosť je

a) zabezpečenie ochrany vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (firewall) pre informačné systémy verejnej správy,

b) vedenie evidencie o všetkých miestach prepojenia sietí v správe povinnej osoby vrátane prepojení s externými sieťami, ktorými sú všetky prepojenia, ktoré nemá povinná osoba pod svojou správou,

c) zabezpečenie, aby pre každé prepojenie podľa písmena b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami podľa § 41.

§ 35
Fyzická bezpečnosť a bezpečnosť prostredia

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je

a) umiestnenie informačného systému verejnej správy v takom priestore, aby informačný systém verejnej správy alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“),

b) oddelenie zabezpečeného priestoru od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami,

c) zabezpečenie, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť informačný systém verejnej správy umiestnený v tomto zabezpečenom priestore,

d) vypracovanie a implementácia pravidiel pre prácu v zabezpečenom priestore,

e) zabezpečenie ochrany pred výpadkom zdroja elektrickej energie pre tie časti informačného systému verejnej správy, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, aby takýto výpadok nenastal,

f) zabezpečenie, aby boli existujúce záložné kapacity informačného systému verejnej správy, zabezpečujúce funkčnosť alebo náhradu informačného systému verejnej správy, umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru,

g) zabezpečenie, aby bola prevádzka, používanie a manažment informačného systému verejnej správy v súlade s osobitnými predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,

h) vypracovanie, zavedenie a kontrola dodržiavania pravidiel pre

1. údržbu, uchovávanie a evidenciu technických komponentov informačného systému verejnej správy a zariadení informačného systému verejnej správy,
2. používanie zariadení informačného systému verejnej správy na iné účely, na aké boli pôvodne určené,
3. používanie zariadení informačného systému verejnej správy mimo určených priestorov,

4. vymazávanie, vyraďovanie a likvidovanie zariadení informačného systému verejnej správy a všetkých typov relevantných záloh,
5. prenos technických komponentov informačného systému verejnej správy alebo zariadení informačného systému verejnej správy mimo priestorov povinnej osoby,
6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačného systému verejnej správy tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,

i) stanovenie parametrov pre informačné systémy verejnej správy, ktoré definujú maximálnu prípustnú dobu výpadku informačného systému verejnej správy a vytvorenie a zavedenie opatrení, ktoré sú zamerané na riešenie obnovy prevádzky v prípade výpadku informačného systému verejnej správy.

§ 36
Aktualizácia softvéru

Štandardom pre aktualizáciu softvéru je

a) zabezpečenie aktualizácie verzií inštalovaného ochranného softvéru, zabezpečujúceho ochranu podľa § 33 písm. a) a b) a § 34 písm. a), vrátane zabezpečenia všetkých ostatných komponentov a pripájaných prostriedkov,

b) vykonanie aktualizácie minimálne v súlade s bezpečnostnou politikou povinnej osoby.

§ 37
Monitorovanie a manažment bezpečnostných incidentov

Štandardom pre monitorovanie a manažment bezpečnostných incidentov je

a) vykonávanie bezpečnostného monitoringu na aktívne odhaľovanie bezpečnostných incidentov,

b) vypracovanie vnútorného predpisu obsahujúceho
1. postup identifikácie bezpečnostných incidentov,
2. postup hlásenia bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy, najmä na včasné prijatie preventívnych a nápravných opatrení; ak ide o povinné osoby podľa § 3 ods. 3 písm. a) zákona alebo o prevádzkovateľa základnej služby podľa osobitného predpisu,[10a]) tento postup vždy zahŕňa aj hlásenie bezpečnostných incidentov podľa § 22 zákona orgánu vedenia,
3. postup riešenia jednotlivých typov bezpečnostných incidentov a spôsob ich vyhodnotenia,
4. spôsob evidencie bezpečnostných incidentov a použitých riešení,
5. spôsob zaistenia digitálnych stôp bezpečnostného incidentu, ktorý určí a zverejní orgán vedenia,

c) zabezpečenie, aby o postupoch podľa písmena a) boli primeraným spôsobom informovaní všetci používatelia informačného systému verejnej správy, a aby boli tieto postupy dodržiavané,

d) zavedenie evidencie každého výpadku informačného systému verejnej správy a spôsobu jeho riešenia,

e) pre povinné osoby podľa § 3 ods. 3 písm. a) zákona používanie systému na detekciu prienikov, ktorý monitoruje bezpečnosť najmenej v rozsahu Intrusion Detection System (IDS),

f) vytvorenie a prevádzka kontaktného miesta povinnej osoby pre ohlasovanie bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy v správe povinnej osoby a určenie kontaktných osôb vykonávajúcich technické činnosti alebo osôb oprávnených rozhodovať u povinnej osoby,

g) o kontaktnej osobe podľa písmena e) oznamiť jej meno a priezvisko, e-mailovú adresu, telefonický kontakt a jej úlohu u povinnej osoby a každú zmenu v týchto údajoch úradu; ak ide o povinnú osobu podľa § 3 ods. 3 písm. a) zákona, oznámiť aj S/MIME[10b]) alebo OpenPGP[10c]) verejný kľúč každej kontaktnej osoby,

h) ak ide o povinnú osobu, ktorá je prevádzkovateľom ústredného portálu verejnej správy, poskytovať netflow z perimetrových prvkov a externých Domain Name Services (DNS) dotazov z rekurzívnych Domain Name Services (DNS) serverov automatizovaným spôsobom úradu.

§ 38
Periodické hodnotenie zraniteľnosti

Štandardom periodického hodnotenia zraniteľnosti je

a) pravidelné hodnotenie slabých miest a ohrození informačného systému verejnej správy identifikovaných podľa bezpečnostnej politiky povinnej osoby s periodicitou najmenej raz ročne,

b) umožnenie vykonávania neinvazívnych penetračných testov podľa § 22 zákona vo verejne dostupných programových prostriedkoch orgánom vedenia a podľa jeho pokynov na základe ich výsledkov prijímať potrebné opatrenia a informovať orgán vedenia o ich prijatí.

§ 39
Zálohovanie

Štandardom pre zálohovanie je

a) zabezpečenie vytvorenia archivačnej zálohy a prevádzkovej zálohy podľa periodicity určenej v bezpečnostnej politike povinnej osoby, najmenej raz za týždeň, ak ide o prevádzkovú zálohu a najmenej raz za dva mesiace, ak ide o archivačnú zálohu,

b) vyhotovenie archivačnej zálohy v dvoch kópiách,

c) zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a v prípade nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči,

d) zabezpečenie vykonania testu obnovy informačného systému verejnej správy a údajov z prevádzkovej zálohy najmenej raz za jeden rok.

§ 40
Fyzické ukladanie záloh

Štandardom pre fyzické ukladanie záloh je

a) fyzické ukladanie prevádzkových záloh, jednej kópie archivačnej zálohy a dátových nosičov s licencovaným softvérom do uzamykateľného priestoru,

b) fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte ako sa nachádzajú technické prostriedky informačného systému verejnej správy, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.

§ 41
Riadenie prístupu

Štandardom pre riadenie prístupu je

a) zavedenie identifikácie používateľa a následnej autentifikácie pri vstupe do informačného systému verejnej správy,

b) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založenej na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh,

c) určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom,

d) určenie požiadaviek, ktoré majú používatelia v súlade s bezpečnostnou politikou povinnej osoby dodržiavať pri používaní informačného systému verejnej správy,

e) automatické zaznamenávanie zmien v pridelenom prístupe a ich archivácia počas celej doby činnosti informačného systému verejnej správy,

f) určenie bezpečnostných zásad pre mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),

g) zabezpečenie, aby používatelia nepoužívali informačné systémy verejnej správy na nelegálne účely,

h) umožniť fyzickým osobám zodpovedným za správu a prevádzku informačných systémov verejnej správy prístup iba k takým údajom a funkciám v týchto informačných systémoch verejnej správy, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh,

i) automatické zaznamenávanie každého prístupu každého používateľa vrátane administrátora do informačného systému verejnej správy, zamedzenie možnosti zmeny týchto záznamov a zamedzenie možnosti vymazania týchto záznamov bez schválenia zodpovednou osobou určenou podľa § 29 písm. c),

j) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy.

§ 42
Aktualizácia informačno-komunikačných technológií

Štandardom pre aktualizáciu informačno-komunikačných technológií je

a) zavedenie postupov s počiatočným stanovením a zahrnutím bezpečnostných požiadaviek a schvaľovacieho procesu pre

1. zmenu konfigurácie, zavádzanie nových alebo aktualizáciu a rozširovanie funkcionality existujúcich informačných systémov verejnej správy alebo ich častí; v prípade automatizovanej on-line aktualizácie sa schvaľovanie zavádza iba, ak si vyžaduje finančné zdroje alebo je aktualizácia príliš rozsiahla,

2. zavádzanie nových informačno-komunikačných technológií u povinnej osoby najmä s ohľadom na zaistenie kompatibility a zachovanie potrebnej úrovne bezpečnosti,

b) vymenovanie zástupcu správcu alebo prevádzkovateľa informačného systému verejnej správy, zodpovedného za informačnú bezpečnosť a činnosti podľa písmena a),

c) vymenovanie zástupcu dodávateľa, ak je dodávateľom činnosti podľa písmena a) tretia strana, zodpovedného za informačnú bezpečnosť,

d) vykonanie testovania pre činnosti podľa písmena a) a vytvorenie dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch, a to najmenej vykonanie interného používateľského testovania v rozsahu najmenej jedného týždňa pred odovzdaním informačného systému verejnej správy, jeho časti alebo súvisiacej aplikácie dodávateľom a zahrnutie jeho výstupov do dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch,

e) uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy alebo ich častiach, ktorá obsahuje

1. používateľskú dokumentáciu, ktorou je návod na používanie informačného systému verejnej správy,
2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku informačného systému verejnej správy,
3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému verejnej správy alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy.

§ 43
Účasť tretej strany

Štandardom pre účasť tretej strany je

a) analýza rizík v súvislosti s informačnými systémami verejnej správy podľa § 31, vyplývajúcich z činnosti tretích strán v týchto informačných systémoch, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb a zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích strán v informačných systémoch verejnej správy, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

b) zabezpečenie, aby boli v zmluvách s treťou stranou o poskytovaní služieb súvisiacich s informačným systémom verejnej správy uvedené bezpečnostné požiadavky na tieto služby,

c) zamedzenie prístupu tretích strán ku všetkým údajom v informačnom systéme verejnej správy, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom na základe zmluvy tak, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

d) zabezpečenie kontroly plnenia bezpečnostných požiadaviek podľa písmena b),

e) zabezpečenie, aby nesplnenie bezpečnostných požiadaviek podľa písmen b) a c) alebo podľa § 42 písm. a), c) a d) bolo dôvodom na neukončenie príslušnej etapy projektu alebo neschválenie prevzatia vykonávanej činnosti.

§ 44
Federácia identít

Štandardom pre federáciu identít je používanie protokolu Security Assertion Markup Language (SAML) vo verzii 2.0 podľa Organization for the Advancement of Structured Information Standards (OASIS) pri federácii identít informačných systémov verejnej správy, pričom ak je poskytovateľom identít správca ústredného portálu verejnej správy

a) pre protokol Security Assertion Markup Language (SAML) sa používa
   1. profil Web Browser Single Sign-On Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST alebo HTTP-Redirect, alebo
   2. profil Single Logout Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST, HTTP-Redirect alebo Simple Object Access Protocol (SOAP) minimálne vo verzii 1.2,

b) dátová štruktúra Security Assertion Markup Language (SAML) Assertion pre prenos autentifikačných informácií medzi poskytovateľom služby a poskytovateľom identity má atribúty podľa prílohy č. 8.

Záverečné, prechodné a zrušovacie ustanovenia

§ 62
Zrušovacie ustanovenie

Zrušuje sa výnos Ministerstva financií Slovenskej republiky z 9. júna 2010 č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy.

§ 63
Účinnosť

Tento výnos nadobúda účinnosť 15. marca 2014 okrem § 19 písm. c), d), f) a g), § 21, písm h), § 22 písm. d) až g), § 23, § 24 písm. b) až f) a h), § 44, § 47 písm. e) a f), § 48, § 51 ods. 2, § 52, § 53, § 55 až 57, bodov 1.6, 3.1, 5.4, 7.3 a 9.4 prílohy č. 1 a prílohy č. 3 až 10, ktoré nadobúdajú účinnosť 15. marca 2015 a okrem § 3, písm. a) a b), § 19 písm. h) a § 24 písm. g), ktoré nadobúdajú účinnosť 15. marca 2016.

v z. Peter Pellegrini v. r.

Príloha č. 8
k výnosu č. 55/2014 Z. z.

Zoznam atribútov SAML Assertion

Zoznam atribútov SAML Assertion

1.1 Zoznam atribútov SAML Assertion v štruktúre AttributeStatement je uvedený v tejto tabuľke:

Atribút	**Význam**
ActorIDSector	Typ použitého identifikátora v kontexte informačného systému, ktorý je zdrojom a správcom identity použitej v atribúte ActorID pre rolu aktér. Hodnotou je textový reťazec. Pre identity federované z ústredného portálu verejnej správy je hodnotou „SECTOR_UPVS“.
ActorID	Samotný identifikátor identity v roli aktér - používateľ, ktorý akciu vykonal. Hodnotou je identifikátor právnickej osoby alebo identifikátor fyzickej osoby[1)].
SubjectIDSector	Typ použitého identifikátora v kontexte informačného systému, ktorý je zdrojom a správcom identity použitej v atribúte SubjectID pre rolu subjekt. Hodnotou je textový reťazec. Pre identity federované z ústredného portálu verejnej správy je hodnotou„SECTOR_UPVS“.
SubjectID	Samotný identifikátor identity v roli subjekt. Subjektom je konkrétna osoba, v mene ktorej sa vykonáva proces. Hodnotou je identifikátor právnickej osoby alebo identifikátor fyzickej osoby. V prípade, že používateľ koná vo svojom mene, hodnota je totožná s ActorID.
DelegationType	Typ zastupovania: v akom vzťahu je identita SubjectID k identite ActorID. Hodnotou je *0 – generálne zastupovanie podľa všeobecne záväzného právneho predpisu, napríklad konateľ právnickej osoby, alebo súdom určený zástupca nesvojprávnej osoby,* *1 až n – delegované zastupovanie.*
QAAlevel	Úroveň autentifikácie podľa prílohy č. 6 tabuľky č. 8, ktorú použil používateľ pri prihlásení sa do systému. Hodnotou je číslo úrovne autentifikácie elektronických služieb verejnej správy.

1.2 Atribúty podľa bodu 1.1 môžu byť rozšírené o ďalšie atribúty, potrebné pre špecifickú implementáciu.

1) § 10 ods. 11 zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších právnych predpisov.

1a) § 3 písm. j) zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).

2) STN EN 301 549 Požiadavky na prístupnosť produktov a služieb IKT (871549).

3) Napríklad § 5 až 5b zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

4) Napríklad zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov.

4a) RFC 2046: Formát Multipurpose Internet Mail Extensions (MIME). Časť 2: Typy médií, RFC 3629:UTF-8 transformácia UCS (univerzálnej znakovej sady), ISO/IEC 10646 - Informačné technológie. Univerzálna znaková sada (UCS).

4aa) RFC 6838: Špecifikácie typov médií a registračné postupy z dôvodu zjednotenia používaných hodnôt.

4ab) § 31a zákona č. 305/2013 Z. z.

5) ISO/IEC 29500:2012 Formáty súborov Office Open XML.

6) § 4 ods. 3 zákona č. 211/2000 Z. z.

7) ISO/IEC 29500-4:2012 Formáty súborov Office Open XML. Prechodné migračné vlastnosti.

7a) ISO/IEC 15948: Informačné technológie. Počítačová grafika a spracovanie obrázkov. Prenosná sieťová grafika (PNG). Funkčná špecifikácia.

8) ISO/IEC 10918-5:2013 Digitálna kompresia a kódovanie kontinuálne tónovaných statických obrázkov. JPEG File Interchange Format (JFIF).

9) RFC 4180 Spoločný formát a MIME typ pre Comma Separated Values (CSV) súbory.

10) Zákon č. 211/2000 Z. z.

10a) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

10b) RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) verzia 3.2, špecifikácia správ.

10c) RFC 4880: OpenPGP formát správy. RFC 6637: Kryptografia na báze eliptických kriviek (ECC) v OpenPGP.

11) Zákon č. 9/2010 Z. z. o sťažnostiach.

11a) § 31 ods. 1 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z.

11aa) § 54a zákona č. 305/2013 Z. z.

11ab) RFC 7232 - Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests.

11ac) Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

11b) Vykonávacie rozhodnutie Komisie (EÚ) 2015/1506 z 8. septembra 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách, pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9. 9. 2015).

11c) ISO 19005-1, ISO 19005-2.

11ca) § 34 až § 39 zákona č. 305/2013 Z. z.

11e) ETSI TS 102 918 Elektronické podpisy a infraštruktúry (ESI): Formát Associated Signature Containers (ASiC), ETSI TS 103 174 V2.2.1: Elektronické podpisy a infraštruktúry (ESI): Základný profil Associated Signature Containers (ASiC).

11ea) ETSI TS 102 918 Elektronické podpisy a infraštruktúry (ESI): Formát Associated Signature Containers (ASiC), ETSI TS 103 174 V2.2.1: Elektronické podpisy a infraštruktúry (ESI): Základný profil Associated Signature Containers (ASiC).

11eb) ETSI EN 319 162-1.

11ec) § 11 ods. 1 písm. k) zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

11f) Zákon č. 305/2013 Z. z.

11g) Vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky) v znení neskorších predpisov.

11h) § 24 ods. 8 zákona č. 215/2002 Z. z. v znení neskorších predpisov.

11i) STN EN ISO 3166-1 Kódy názvov krajín a ich častí. Časť 1: Kódy krajín (ISO 3166-1: 2013) (01 0190).

11j) ISO 13616 Finančné služby. Medzinárodné bankové číslo účtu (IBAN).

11k) ISO 9362 Bankovníctvo. Bankové telekomunikačné správy. Bankové identifikačné kódy (BIC).

11l) RFC 5646: Značky pre identifikáciu jazykov. STN ISO 639-1 Kódy názvov jazykov. Časť 1: Dvojmiestne abecedné kódy (01 0400). STN ISO 639-2 Kódy názvov jazykov. Časť 2: Trojmiestne abecedné kódy (01 0400).

11m) MessageImprint, kapitola 2.4.1, IETF RFC 3161, X.509 Internet Public Key Infrastructure, Time-Stamp Protocol (TSP).

21) RFC 3061: Menný priestor vo formáte Uniform Resource Name (URN) pre identifikátory objektov.

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.: 02 888 91 131, e-mail: helpdesk@slov-lex.sk.