MINISTERSTVO DOPRAVY, PÔŠT A TELEKOMUNIKÁCIÍ SR
Sekcia informatizácie spoločnosti
Odbor pre informačnú bezpečnosť a štandardy

Metodický pokyn

k štandardom pre informačné systémy verejnej správy a ich rozdeleniu a náležitostiam, spôsobu ich aktualizácie a oblastiam ich uplatnenia pre informačné systémy verejnej správy

v zmysle Výnosu MDPT SR zo 14. júla 2006 č. 1706/M-2006 o štandardoch pre informačné systémy verejnej správy

Verzia 1.00

Účinnosť od: 1. 10. 2006

Úvod

Metodický pokyn dopĺňa rozdelenie a náležitosti štandardov, spôsob ich aktualizácie a oblasti ich uplatnenia pre informačné systémy verejnej správy, ako nástrojov výkonu informačných činností pri utváraní a prevádzkovaní informačných systémov verejnej správy alebo ich častí.

Štandardy sa nevzťahujú na informačné systémy verejnej správy, ktoré sú poskytované zo strany medzinárodných organizácií ako napr. Organizácia pre hospodársku spoluprácu a rozvoj (OECD), Európska komisia, Organizácia pre bezpečnosť a spoluprácu v Európe (OBSE) atď., ich prevádzkovateľmi sú povinné osoby v Slovenskej republike (napr. Ministerstvo zahraničných vecí SR), ktoré musia dodržiavať pravidlá prevádzky a štandardy daného informačného systému verejnej správy podľa podmienok stanovených správcom a nemôžu ich meniť. Tieto pravidlá závisia napr. od dohody medzinárodného riadiaceho výboru, ktorý má na starosti daný informačný systém.

Táto výnimka sa vzťahuje na prevádzkovateľov iba pokiaľ poskytujú prístup tretím osobám bez ďalších úprav. Pokiaľ zasielajú alebo inak spracovávajú a zverejňujú dokumenty, ktoré sú súčasťou daného informačných systémov verejnej správy, je ich povinnosťou tieto dokumenty upraviť podľa existujúcich štandardov platných v Slovenskej republike.

1. Oblasti štandardizácie

Oblasťami štandardizácie, ktoré sa nachádzajú vo výnose č. 1706 / M -2006 sú:

a) technické štandardy,

b) štandardy prístupnosti,

c) elektronická výmena dát,

d) štandardy pre názvoslovie elektronických služieb,

e) bezpečnostné štandardy.

Tento zoznam nie je uzavretý a do ďalších výnosov sa pripravujú oblasti ako napr. dátové štandardy, štandardy pre priestorovú identifikáciu atď.

2. Metodika popisu štandardov

Štandard obsahuje tieto náležitosti

(1) Názov štandardu obsahuje

(a) jedno alebo viac slov v prirodzenom jazyku určujúce pomenovanie oblasti použitia opisovaného štandardu,

(b) názov štandardu sa začína veľkým písmenom a ukončí sa bez rozdeľovacieho znamienka, bez ohľadu na počet slov.

(2) Povinné požiadavky obsahujú

(a) všetky potrebné a dostačujúce prvky k tomu, aby štandard bol úplne a jednoznačne vymedzený a zrozumiteľný. Táto definícia musí byť teoreticky správna a presná v

príslušných súvislostiach a musí používať pojmy stanovené jednoznačne, prípadne použité pojmy samostatne vymedziť,

(b) popisnú obsahovú stránku štandardu, ktorá obsahuje kategoricky záväzné požiadavky,

(c) ak je to vhodné, vysvetlenie prečo sa daná požiadavka zavádza.

(3) Odporúčané požiadavky obsahujú

(a) všetky potrebné a dostačujúce prvky k tomu, aby štandard bol úplne a jednoznačne vymedzený a zrozumiteľný. Táto definícia musí byť teoreticky správna a presná v príslušných súvislostiach a musí používať pojmy stanovené jednoznačne, prípadne použité pojmy samostatne vymedziť,

(b) popisnú obsahovú stránku štandardu, ktorá obsahuje odporúčané (nie však povinné) požiadavky,

(c) ak je to vhodné, vysvetlenie prečo sa daná požiadavka zavádza.

(4) Odkazy na iné štandardy, číselníky, právne normy a predpisy a iné zdroje uvádzajú

odkazy na medzinárodné, európske a slovenské normy, resp. iné dokumenty, ktoré súvisia so štandardom.

(5) Gestor štandardu udáva

názov štátneho orgánu, ktorý zodpovedá za správnosť a aktuálnosť údajov uvedených v štandarde. Uvádzajú sa názvy štátnych orgánov resp. organizácií v prípade ak je iný ako Ministerstvo v zmysle zákona č. 275 / 2006 o informačných systémoch verejnej správy. Každá organizácia sa píše do samostatného riadku.

3. Stavy štandardov

Stav štandardu môže byť

a) platný, ktorý sa dodržiava v informačných systémoch verejnej správy; za nedodržanie platného štandardu ministerstvo uloží pokutu podľa osobitného predpisu,[1]) uvádza sa vo výnose o štandardoch pre informačné systémy verejnej správy,

b) navrhovaný, ktorý nie je povinný a môže sa používať na účely definovania obsahu budúceho informačného systému verejnej správy pre obstarávateľov informačných systémov verejnej správy; preveruje sa z hľadiska jeho možného zavedenia a po jeho zhodnotení nadobúda stav platného alebo zrušeného štandardu, navrhovaný štandard sa uvádza v metodickom pokyne MDPT SR a je predmetom posúdenia Komisie pre štandardizáciu ISVS (ďalej len „Komisia“),

c) zrušený, ktorý stratil platnosť z dôvodu jeho nahradenia iným štandardom alebo na základe rozhodnutia ministerstva o nevhodnosti jeho používania v informačných systémov verejnej správy, uvádza sa v metodickom pokyne MDPT SR.

Odporúčaná lehota medzi zmenou štandardu zo stavu „navrhovaný“ na stav „platný“ je 1 rok, aby bola zaručená možnosť prispôsobenia sa a dostatočnej informovanosti dodávateľov a správcov ISVS.

[1)] § 10 zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy.

V prípade zrušeného štandardu sa uvádza dátum, od ktorého nadobudol účinnosť a stal sa platným pre informačné systémy verejnej správy ako aj dátum zrušenia jeho platnosti. Dátum sa uvádza v poradí deň, mesiac, rok a jednotlivé časti sa oddeľujú bodkou.

4. Životný cyklus štandardov

Životný cyklus štandardu informačných systémov verejnej správy pozostáva z nasledujúcich krokov:

- Krok 1:
  - Akákoľvek právnická alebo fyzická osoba môže:

    A) navrhnúť nový štandard, ktorý by mohol byť zavedený

    B) navrhnúť existujúci štandard na zrušenie

    C) navrhnúť zmenu niektorej požiadavky pri platnom a zavedenom type štandardu z „povinnej“ na „odporúčanú“ alebo z „odporúčanej“ na „povinnú“, prípadne doplnenie odkazu.
  - Uvedené návrhy sú zasielané na adresu podľa kapitoly č. 6 Gestorstvo a komunikácia s gestormi. Predseda Komisie môže podľa uváženia návrh predložiť na rokovanie Komisie. V prípade nezmyselnosti návrhu nebude tento návrh predložený bez odôvodnenia navrhovateľovi.
- Krok 2:
  - Štandard z kroku 1 môže na základe rozhodnutia Komisie predseda Komisie prideliť konkrétnemu členovi Komisie, podkomisii alebo zadať externému subjektu, aby pripravil relevantný podklad na rokovanie Komisie – predbežné hodnotenie. Podklad musí obsahovať všetky informácie týkajúce sa návrhu tak, aby po oboznámení mohli členovia Komisie prijať záver/uznesenie. Podklady na rokovanie je potrebné distribuovať s dostatočným časovým predstihom, aby členovia Komisie mali dostatočný časový priestor na štúdium a prípadné spracovanie vlastných podkladov.
- Krok 3:
  - návrh z predchádzajúcich bodov (1, 2) Komisia vyhodnotí a príjme záver z predbežného hodnotenia, ak existuje. Komisia môže návrh úplne odmietnuť alebo ho akceptovať a odporučiť na ďalšie hodnotenie.
- Krok 4:
  - v prípade, ak Komisia odmietne návrh už v predbežnom hodnotení, svoje rozhodnutie musí publikovať verejne dostupnou formou tak, aby navrhovateľ získal spätnú väzbu. V prípade, ak je štandard odporúčaný do ďalšieho hodnotenia, Komisia začne proces hodnotenia.
  - Proces hodnotenia pozostáva zo zberu ďalších podkladov a odborných stanovísk jednotlivých členov Komisie. Konkrétnym návrhom sa budú zaoberať všetci členovia Komisie, pričom výsledky svojej práce zosumarizujú na zasadaniach. Počet zasadaní nie je obmedzený a členovia Komisie sa stretávajú a rokujú dovtedy, kým nedôjde k zbliženiu stanovísk. Komisia bude rozhodovať konsenzuálnym princípom. Kým existujú akékoľvek pochybnosti, je potrebné o nich rokovať a snažiť sa o ich odstránenie.
  - Výsledkom hodnotenia môže byť odporúčanie na zrušenie existujúceho štandardu, odporúčanie na zmenu stavu existujúceho štandardu z

„navrhovaného“ na „platný“ alebo naopak, alebo odporúčanie na zmenu niektorej požiadavky štandardu z „povinnej“ na „odporúčanú“ alebo z „odporúčanej“ na „povinnú“, odporúčanie na prijatie nového štandardu a jeho zaradenie do stavu „navrhovaný“ alebo „platný“, prípadne doplnenie ďalších požadovaných údajov. Komisia svoj záver zároveň spracuje do formy návrhu, ktorý bude súčasťou najbližšej aktualizácie výnosu o štandardoch pre informačné systémy verejnej správy.

- Krok 5:
  - Komisia podľa závažnosti návrhov rozhodne o termíne aktualizácie výnosu o štandardoch pre informačné systémy verejnej správy. Aktualizácia výnosu prechádza zaužívaným legislatívnym postupom od vnútrorezortného pripomienkového konania až po rokovanie Legislatívnej rady vlády SR resp. jej príslušnej komisie. Počas medzirezortného pripomienkového konania je možné vyjadriť sa zaužívaným spôsobom.
- Krok 6:
  - Výnos o štandardoch pre informačné systéme verejnej správy je publikovaný v Zbierke zákonov SR a každý nový alebo aktualizovaný štandard nadobúda stav „platný“ alebo „zrušený“ k dátumu účinnosti vydania výnosu alebo stav „navrhovaný“ bez uvedenia dátumu.
  - Pri zmenách a zavedení štandardov je vždy potrebné prihliadať aj na finančné dopady zavedenia alebo zrušenia štandardu a potenciálne finančné alebo aj nefinančné prínosy. Preto pri zavedení resp. zmene platných štandardov sa odporúča vypracovať štúdiu efektívnosti, ktorá bude obsahovať aj finančnú analýzu.

5. Zverejňovanie štandardov

Zoznam štandardov spoločne s prislúchajúcimi metodikami bude verejne vedený na ústrednom portáli verejnej správy a na webovej stránke Ministerstva dopravy, pôšt a telekomunikácií SR.

6. Gestorstvo a komunikácia s gestormi

Každý gestor štandardu má k dispozícii adresu standard@domena.gov.sk kam bude možné zasielať relevantné návrhy a otázky, týkajúce sa štandardov v jeho gescii. Časť „domena“ je platná webová adresa daného gestora (napr. standard@mdptsr.gov.sr).

Návrhy na zmeny podľa kapitoly 4 sa zasielajú na e-mailovú adresu koordinátora procesu štandardizácie, t.j. Ministerstva dopravy, pôšt a telekomunikácií SR - standard@portal.gov.sk.

7. Doplňujúce informácie k jednotlivým kapitolám výnosu

Informácie uvedené v kapitole 7 majú iba rozširujúci a vysvetľujúci charakter, žiadnym spôsobom neupravujú znenie aktuálneho výnosu o štandardoch pre informačné systémy verejnej správy. Za účelom ľahšieho priradenia jednotlivých informácií sa text uvádza vo forme zhodnej s aktuálnym výnosom.

Prvá časť

§ 4
Komunikačné protokoly

Týmto štandardom sa nepostihuje prenos elektronických poštových správ v rámci jedného informačného systému s využitím vnútorných systémov pre elektronické správy. To isté platí aj pre § 5 a § 6.

Štandardy pre integráciu dát

bez uvedenia paragrafu
Výmena štatistických dát a metadát

Odporúčanou požiadavkou je

používanie štandardu Statistical Data and Metadata Exchange, verzia 2.0 (SDMX 2.0) pre výmenu štatistických dát a metadát

Odkazy na iné štandardy, číselníky, právne normy a predpisy a iné zdroje

a) SDMX - ISO/TS 17369:2005

b) iniciatíva SDMX

Stav štandardu

navrhovaný

Druhá časť

Štandardy prístupnosti webových stránok

§ 12
Prístupnosť webových stránok

Štandardy v tejto časti zabezpečujú dostupnosť informačno-komunikačných technológií pre čo najväčší počet ľudí, najmä používateľov s funkčnými zníženiami, starších ľudí a všetkých, ktorí môžu zaostať v rýchlom pokroku technológií vo všetkých oblastiach spoločnosti, a tak napomáha aktívnej účasti a integrácii osôb s postihnutím v spoločnosti.

Používanie týchto štandardov podporuje prístupnosť aj v prípade nedostačujúceho hardvéru alebo softvéru, keď sú obmedzené niektoré vlastnosti (napr. vypnutie zobrazovania obrázkov, čierno-biely displej, vypnutie zvuku atď.).

Splnenie tohto štandardu je bezpodmienečne nutné na to, aby znevýhodneným občanom boli dostupné informácie na webových stránkach.

Splnenie odporúčaných požiadaviek je potrebné na to, aby bola orientácia pre znevýhodnených občanov na webových stránkach čo najpohodlnejšia.

Povinné aj odporúčané požiadavky tohto štandardu odkazujú na pravidlá a zásady z nasledovných dokumentov:

1. „Web Content Accessibility Guidelines 1.0“, ktorý je momentálne dostupný na webovej stránke http://www.w3.org/TR/WCAG10/,

2. „Dokumentácia zásad prístupnosti webových stránok pre používateľov s ťažkým zrakovým postihnutím“ (autor: Radek Pavlíček, preklad do slovenčiny: Jozef Dalnoky a Branislav Mamojka), ktorá je momentálne dostupná na webovej stránke http://www.blindfriendly.sk/download/bfw23_sk.doc.

Ako pomôcku pre prevádzkovateľov ISVS odporúčame použiť nasledovné dokumenty:

1. slovenský preklad „Web Content Accessibility Guidelines 1.0“, ktorý je momentálne dostupný na webovej stránke http://www.telecom.gov.sk/index/open_file.php?file=infospol/bezpecnost/wai_smernice.pdf,

2. „Pravidlá tvorby prístupného webu“ (autor: David Špinar, preklad do slovenčiny: Peter Druska), ktoré sú momentálne dostupné na webovej stránke http://sietook.druskova.sk/?ukaz=archiv&id=2 (originál v češtine je momentálne dostupný na webovej stránke http://pristupnost.nawebu.cz/texty/pravidla-standardy.php?full).

Tretia časť

Štandardy pre jednorazovú elektronickú výmenu dát

Tieto štandardy sa týkajú najmä zasielania súborov alebo zverejňovania na webovej stránke povinnej osoby, či inom informačnom systéme alebo portále v jej gescii.

V prípade, že niektorý typ štandardov pre túto oblasť nie je definovaný, v súčasnosti tento typ nemá povinný štandard (napr. súbory pre prezentáciu alebo súbory pre prácu s tabuľkami).

§ 13
Výmenné formáty pre textové súbory

Formát .doc sa uvádza z dôvodu masového rozšírenia, ale do budúcnosti sa vzhľadom na jeho uzavretý charakter neuvažuje o ďalšom používaní. Microsoft pripravuje nový otvorený formát, ktorý nahradí .doc. Odporúča sa využívať povinný .rtf, ktorý je s .doc prakticky ekvivalentný.

Štvrtá časť

Štandardy pre názvoslovie elektronických služieb

§ 19
Tvar generických e-mailových adries používateľov informačných systémov verejnej správy

V prípadoch, kde je to vhodné resp. ak viac uvádzaných činností podľa § 19 vykonáva ten istý útvar / osoba, je pre existujúcu adresu postačujúci alias. Dôvodom existencie týchto adries je ľahšia orientácia pri komunikácii najmä zo strany občana.

Adresa špecifickej funkcie by zároveň mala plniť funkciu adresy sekretariátu, z tohto dôvodu tam kde je to nutné sa s ohľadom na ochranu osobných údajov prípadne dôležitých informácií odporúča existencia aj oddelenej osobnej adresy (meno.priezvisko@domena.gov.sk).

§ 20
Tvar doménových mien webových stránok inštitúcií štátnej správy

Pre tvar doménových mien je postačujúci aj alias t.j. nie je nutné rušiť aktuálnu existujúcu doménu.

Piata časť

Bezpečnostné štandardy

§ 21
Riadenie informačnej bezpečnosti

Bezpečnostná politika je dôležitým základom pre riadenie a správu informačnej bezpečnosti a zabezpečenie jej kontinuity. Základ bezpečnostnej politiky je ekvivalentný

s bezpečnostným zámerom v zmysle zákona č. 428 / 2002 Z. z. o ochrane osobných údajov, §16 , odsek 4 s rozšíreniami o niektoré presnejšie špecifikácie.

Doplnenie požiadaviek v zmysle výnosu o štandardoch pre informačné systémy verejnej správy a:

- bodu a) podľa uvedeného zákona

Musí existovať systém riadenia kontinuity činnosti. Systém musí byť jasne definovaný v bezpečnostnej politike a musia sa vytvoriť bezpečnostné procedúry pre uvedenú oblasť. Musí byť definované, ktoré aktíva a technické prostriedky je potrebné chrániť a akým spôsobom.

- bodu b) podľa uvedeného zákona – doplnenie o všeobecnú informačnú bezpečnosť

V každej organizácii musí existovať minimálne jedna osoba, ktorá je zodpovedná za informačnú bezpečnosť, táto osoba má na starosti rozvoj a údržbu informačnej bezpečnosti ako takej. Môžu existovať aj ďalšie osoby, ktoré majú na starosti špecifické oblasti alebo systémy.

Riadenie informačnej bezpečnosti musí mať väzbu na riadiacich pracovníkov, nakoľko si vyžaduje znalosť o možných rizikách v prípade jej narušenia a dopadu na organizáciu ako aj prideľovanie adekvátnych finančných prostriedkov na jej funkčnosť.

Organizácia musí zabezpečiť, aby si zamestnanci boli vedomí svojej zodpovednosti a boli pravidelne informovaní alebo školení o aktuálnych trendoch v oblastiach informačnej bezpečnosti, vedeli ako sa majú správať v prípade narušenia niektorého aspektu informačnej bezpečnosti t.j. musia byť jasne definované pravidlá bezpečnej prevádzky systému / systémov. Dôležitou súčasťou je aj vyvodzovanie dôsledkov narušenia bezpečnosti a zodpovednosť relevantných osôb a užívateľov.

- bodu d) podľa uvedeného zákona

Bezpečnostná politika obsahuje rozdelenie údajov podľa citlivosti a z toho vyplývajúce bezpečnostné opatrenia. V rámci ochrany údajov a dát sa vo všeobecnosti zálohujú všetky citlivé údaje, t.j. údaje ktoré môžu spôsobiť hmotnú aj nehmotnú škodu pri ich strate alebo poškodení, prípadne môže ich znehodnotenie narušiť prebiehajúci alebo uzavretý proces (napr. podklady pre vypracovanie stanoviska alebo posudku, registratúrne záznamy v elektronickej podobe atď.).

Prevádzková záloha by mala obsahovať najmä tie údaje, ktoré sa často aktualizujú a zároveň potrebné nastavenia na obnovenie systému v prípade jeho nestability. Archivačná záloha by mala obsahovať všetky citlivé údaje.

§ 23
Riadenie informačnej bezpečnosti

V rámci kontinuity činnosti sa odporúča uskutočňovať aj testovanie bezpečnostných procedúr.

§ 29
Zálohovanie

Za vytvorenie zálohy na dátovom nosiči sa považuje vytvorenie kópie definovaných údajov na DVD, CD, prenosnom hard disku (HD), sieťovom zálohovacom mieste alebo inom médiu.

V zmysle výnosu je nutné, aby súčasne existovali tri zálohy – jedna prevádzková a dve archivačné.

§ 30
Požiadavky na fyzické ukladanie záloh

a) Vzhľadom na časté porušovanie licenčných podmienok je nutné chrániť médiá s licencovaným softvérom pred neoprávneným kopírovaním alebo používaním. Licencovaným softvérom sa myslia napr. inštalačné CD operačných systémoch Windows a podobne.

Ako uzamykateľný priestor je možné použiť napr. plechovú skriňu alebo sklad prístupný iba osobe zodpovednej za správu licencovaného softvéru (systémový administrátor atď.).

b) Dôvodom je, aby pri poškodení budovy resp. miestnosti, kde sa nachádza server alebo iné súčasti informačného systému nenastalo zároveň zničenie oboch archivačných kópií. Je vhodné, aby napr. vzhľadom na ohrozenie požiarom nebola ako objekt uloženia susediaca budova.