KONTROLA DODRŽIAVANIA BEZPEČNOSTNÝCH ŠTANDARDOV

Povinná osoba:
Dátum kontroly:
Celkový dosiahnutý výsledok:

Zápis z kontroly dodržiavania bezpečnostných štandardov podľa výnosu č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy, vyplývajúce zo zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy.

Jednotlivé percentuálne hodnotenia dodržiavania konkrétnych štandardov, ako aj celkové hodnotenie celej oblasti bezpečnostných štandardov, sa vypočítavajú na základe udelených trestných bodov, a to s použitím váh pre konkrétne požiadavky.

Prvý hodnotiaci stĺpec ("Predbežná kontrola") zahŕňa hodnotenie už s predbežným odpočtom voči úplnému rozsahu bezpečnostných štandardov, ktorých účinnosť sa začne k 1.10.2009, druhý hodnotiaci stĺpec ("Dodržiava [%] + trestné body [n]") predstavuje skutočné hodnotenie ku dňu kontroly.

Informácie poskytnuté v zápise sa považujú za citlivé.

Váha [n]	Číslo	Požiadavka	Záznam kontroly (-)	Dodržiava [%] + trestné body [n]
3		**§ 28 Riadenie informačnej bezpečnosti**		
2	§28a)	1. Existuje bezpečnostná politika (BP)?		
		Ak je to relevantné, je táto politika rezortná alebo iba organizácie?		
		Je schválená v rámci procesov organizácie ?		
		Ak áno, kedy bola schválená?		
		Akým spôsobom (na akej úrovni)?		
1	§28a) 1	2. Sú určené bezpečnostné ciele?		
1	§28a) 2	3. Sú určené spôsoby ich vyhodnocovania alebo dosahovania? Ak áno, ako?		
		Na základe čoho boli určené?		
1	§28a) 3	4. Obsahuje podporu vedenia?		
1	§28a) 4	5. Sú stanovené pozície pre manažment informačnej bezpečnosti?		
1	§28a) 6	6. Ako je vyhodnotený a zabezpečený súlad bezpečnostnej politiky s ostatnými právnymi dokumentmi?		
1	§28a) 7	7. Ako sa požiadavky, vyplývajúce z právnych dokumentov, premietli do správy IS VS?		
1	§28a) 8	8. Sú stanovené úrovne ochrany IS VS?		
		Ako sú definované?		
1	§28a) 9	9. Sú definované aktíva, ktoré súvisia s IS VS?		
		Sú definované kritické aktíva? Ktoré to sú ?		
1	§28a) 10	10. Je stanovený rozsah a periodicita auditu informačnej bezpečnosti?		

		Ako často sa audit vykonáva?		
		Vykonáva sa interne alebo externe?		
1	§27a) 11	11. Sú vypracované smernice pre zálohovanie?		
		Ak áno, existuje rozdelenie údajov pre rôzne typy záloh?		
		Aká periodicita bola zvolená pre prevádzkovú zálohu a aká pre archivačnú?		
		Ako je postihované nedodržiavanie týchto smerníc?		
0,5	§28a) 12	12. Ako často sa vykonáva monitorovanie bezpečnosti softvéru?		
0,5		13. Ako často sa vykonáva aktualizácia softvéru?		
1	§28a) 13	14. Existuje zoznam dokumentov na zaistenie informačnej bezpečnosti?		
		Ktoré dokumenty to sú?		
		Sú tieto dokumenty vypracované?		
		Ak áno, kedy boli vypracované?		
		Boli tieto dokumenty aktualizované?		
		Ak áno, kedy a s akou periodicitou?		
1	§28a) 14	15. Je stanovený postup revízie bezpečnostnej politiky?		
		Ako často sa revízia vykonáva?		
		Aké dôvody boli stanovené na mimoriadnu revíziu?		
3	§28 b)	16. Sú stanovené postupy v prípade nedodržiavania bezpečnostnej politiky?		
		Akým spôsobom?		
3	§28 c)	17. Je stanovená osoba(y) zodpovedná(é) za informačnú bezpečnosť?		
2	§28 d)	18. Aké úlohy má osoba, zodpovedná za informačnú bezpečnosť?		
1	§28 e)	19. Ako je zabezpečená koordinácia aktivít organizačných zložiek pri riešení informačnej bezpečnosti?		
1	§28 f)	20. Sú určené konkrétne zodpovedné osoby / útvary za jednotlivé aktíva?		
1	§28 g)	21. Ako sú určené bezpečnostné pozície v IS VS?		
2		**§ 29 Personálna bezpečnosť**		
1	§29 a)	22. Je zabezpečené poučenie o BP a povinnostiach z nej vyplývajúcich?		
		Ako sa vykonáva poučenie o BP a povinnostiach z nej vyplývajúcich?		
		Ako sa zabezpečuje poučenie osôb, ktoré vykonávajú činnosti na základe zmluvných vzťahov?		
1	§29 b)	23. Ako je zabezpečené poučenie o právach a povinnostiach pred vstupom do IS VS?		
1	§29 c)	24. Sú povinnosti vyplývajúce z BP uvedené v pracovných zmluvách príslušných zamestnancov?		
2	§29 d)	25. Existuje vypracovaný postup pre disciplinárne konanie v prípade porušenia BP alebo relevantných predpisov?		
1	§29 e)	26. Ako je zabezpečená povinnosť oznamovať bezpečnostné incidenty?		

2	§29 f)	27. Sú vypracované postupy pri ukončovaní práce či pracovného pomeru, ktoré zabezpečujú ochranu IKT v správe organizácie?		
		Ktoré oblasti pokrývajú?		
2		**§ 30 Manažment rizík pre oblasť informačnej bezpečnosti**		
1	§30 a)	28. Existuje implementovaný systém riadenia rizík?		
		Ako je implementovaný?		
1		29. Existuje implementovaný systém monitorovania rizík?		
		Ako je implementovaný?		
1	§30 b)	30. Používa sa systém riadenia rizík a monitorovania?		
		Ak nie, kde sa nepoužíva a prečo?		
1	§30 c)	31. Zohľadňujú riziká aj aktíva a IS VS mimo priestorov povinnej osoby?		
		Aké postupy sú zvolené na ich redukciu?		
2	§30 d)	32. Existuje analýza závislosti na IS VS?		
		33. Existuje analýza kritických procesov?		
2	§30 e)	34. Existuje analýza (zoznam) kritických informačných systémov?		
		Sú riziká pre ne špecificky oddelené?		
1	§30 f)	35. Existujú vypracované plány na obnovu?		
		Ktoré plány sú vypracované?		
2		**§ 31 Kontrolný mechanizmus riadenia informačnej bezpečnosti**		
2	§31 a)	36. Vykonáva sa vnútorná kontrola alebo audit informačnej bezpečnosti?		
		Je vykonávaný interne alebo externe?		
1	§31 b)	37. Sú auditné správy archivované? Sú chránené? Sú vyhodnocované?		
2		**§ 32 Ochrana proti škodlivému kódu**		
1	§32a) 1	38. Je zavedená ochrana e-mailov? (škodlivý kód atď.)		
1	§32a) 2	39. Je zavedená detekcia škodlivého kódu na zariadeniach IS VS?		
1	§32a) 3	40. Sú kontrolované zasielané a prijímané súbory?		
1	§32a) 4	41. Je zavedená ochrana webových sídiel a kontrola existencie škodlivého kódu?		
1	§32 b)	42. Je zavedená ochrana pred nevyžiadanou elektronickou poštou?		
		Aký princíp používa?		
1	§32 c)	43. Je zavedená kontrola legality softvéru, používaného používateľmi?		
1	§32 d)	44. Existujú pravidlá pre sťahovanie súborov z externých sietí?		
1	§32 e)	45. Existuje podpora kryptografických prostriedkov autenticity a integrity? Používa sa v IS inštitúcie elektronický podpis?		
		Je povinná (aspoň pre určité prípady nakladania s údajmi)? Ak áno, pre ktoré?		

		Je dodržiavaná?		
1	§32 f)	46. Existuje podpora šifrovania elektronických dokumentov?		
		Je povinná (aspoň pre určité prípady nakladania s údajmi)? Ak áno, pre ktoré?		
		Je dodržiavaná?		
1		**§ 33 Sieťová bezpečnosť**		
2	§33 a)	47. Existuje implementácia firewallov?		
		Sú nasadené iba ochrany vonkajšieho perimetra alebo aj personálne firewally?		
		Ak existujú aj personálne firewally, v akom rozsahu sú nasadené?		
1	§33 b)	48. Je vedená evidencia o všetkých miestach prepojení sietí v správe povinnej osoby (tzv. uzly)?		
		Je aktualizovaná?		
1	§33 c)	49. Je pre každé miesto podľa písm. b) vypracovaný interný akt riadenia prístupu?		
2		**§ 34 Fyzická bezpečnosť a bezpečnosť prostredia**		
2	§34 a)	50. Sú IS VS alebo aspoň ich kritické komponenty umiestnené v zabezpečenom priestore?		
2	§34 b)	51. Je tento priestor zabezpečený fyzickými prostriedkami?		
1	§34 c)	52. Je tento priestor umiestnený dostatočne ďaleko od ohrozenia fyzickými prostriedkami (kanalizácia, vodovod, horľaviny atď.)?		
1	§34 d)	53. Existujú pravidlá pre prácu v zabezpečenom priestore?		
2	§34 e)	54. Je zabezpečená ochrana pred výpadkom elektriny?		
1	§34 f)	55. Existujú záložné kapacity IS VS? Ak áno, aké sú (čo presne je zálohované)?		
		Sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od pôvodného?		
1	§34 g)	56. Je prevádzka, používanie a manažment IS VS v súlade s legislatívou, vnútornými predpismi a zmluvami? Ako je to docielené?		
1	§34h) 1	57. Existujú pravidlá pre údržbu, uchovávanie a evidenciu technických komponentov IS VS?		
0,5	§34h) 2	58. Existujú pravidlá pre používanie zariadení IS VS na iné účely?		
0,5	§34h) 3	59. Existujú pravidlá pre prenos a používanie zariadení IS VS mimo určených priestorov (v rámci organizácie)?		
1	§34h) 4	60. Existujú pravidlá pre vymazávanie, vyraďovanie a likvidáciu zariadení IS VS a záloh?		
1	§34h) 5	61. Existujú pravidlá pre prenos zariadení IS VS mimo priestorov organizácie?		

0,5	§34h) 6	62. Existujú pravidlá pre narábanie so všetkými informáciami v elektronickej podobe (aj pri prevode z a do písomnej podoby), dokumentáciou systému a pamäťovými médiami?		
1	§34 i)	63. Je stanovená maximálna prípustná doba výpadku IS VS?		
		Ak áno, aká doba to je a v ktorom dokumente je stanovená?		
0,5		64. Aké opatrenia sú stanovené na riešenie obnovy prevádzky v prípade výpadku?		
1		**§ 35 Aktualizácia softvéru**		
1	§35 a)	65. Je zabezpečená aktualizácia verzií inštalovaného ochranného softvéru? Ak áno, pre ktoré typy softvéru je zabezpečená?		
1	§35 b)	66. Je táto aktualizácia v súlade s BP?		
1		**§ 36 Monitorovanie a manažment bezpečnostných incidentov**		
2	§36a) 1	67. Je vypracovaný interný akt pre ohlasovanie bezpečnostných incidentov?		
1	§36a) 2	68. Je vypracovaný interný akt pre riešenie a vyhodnocovanie typov bezpečnostných incidentov?		
1	§36a) 3	69. Je vypracovaný interný akt pre spôsob evidencie bezpečnostných incidentov a použitých riešení?		
1	§36 b)	70. Je zabezpečené informovanie používateľov IS VS o postupoch pri hlásení bezpečnostných incidentov?		
		Ak áno, akým spôsobom? Akým spôsobom je zabezpečovaná kontrola dodržiavania týchto postupov?		
2	§36 c)	71. Existuje evidencia každého výpadku a spôsobu jeho riešenia?		
1	§36 d)	72. Je zavedený systém na detekciu prienikov (najmenej IDS)?		
2	§36 e)	73. Existuje kontaktné miesto na ohlasovanie bezpečnostných incidentov a slabých miest?		
		Je možné ohlásiť aj bezpečnostný incident, identifikovaný externe?		
1		**§ 37 Periodické hodnotenie zraniteľnosti**		
1	§37 a)	74. Vykonáva sa periodické hodnotenie slabých miest IS VS (najmenej raz za rok)?		
1		**§ 38 Zálohovanie**		
2	§38 a)	75. Existujú archivačné a prevádzkové zálohy podľa BP (prevádzková aspoň raz za týždeň, archivačná aspoň raz za 2 mesiace)?		
1	§38 b)	76. Má archivačná záloha dve kópie?		

1	§38 c)	77. Vykonáva sa test funkcionality dátového nosiča jednotlivých záloh? *		
1	§38 d)	78. Vykonáva sa test obnovy systému zo zálohy (najmenej raz za rok)?		
1		**§ 39 Fyzické ukladanie záloh**		
1	§39 a)	79. Sú zálohy a licencovaný softvér ukladané v uzamykateľnom priestore?		
1	§39 b)	80. Ukladá sa druhá kópia archivačnej zálohy v inom objekte?		
2		**§ 40 Riadenie prístupu**		
3	§40 a)	81. Je zavedená identifikácia a autentizácia pri vstupe do všetkých IS VS?		
		Aká úroveň sa bežne používa? Existujú pre niektoré systémy aj vyššie úrovne?		
2	§40 b)	82. Je vypracovaný interný akt riadenia prístupu k údajom a funkciám ISVS?		
		Aký princíp používa?		
1	§40 c)	83. Existuje postup a určená zodpovednosť pre prideľovanie prístupových práv?		
1	§40 d)	84. Sú určené bezpečnostné požiadavky pre používateľov pri používaní IS VS?		
1	§40 e)	85. Sú zmeny prístupu automaticky zaznamenávané a archivované?		
1	§40 f)	86. Existujú bezpečnostné zásady pre mobilné pripojenie?		
1	§40 g)	87. Je zavedená kontrola, že používatelia nepoužívajú IS VS na nelegálne účely?		
2	§40 h)	88. Je zabezpečené, aby administrátori nemali prístup k údajom, ktoré nepotrebujú na vykonávanie svojich úloh?		
2	§40 i)	89. Existuje automatické zaznamenávanie prístupu všetkých používateľov a správcov IS VS do systému?		
		Sú zaznamenávané aj činnosti? Ak áno, aké typy a v akom rozsahu?		
1		90. Ako je zamedzené vymazanie záznamov (bez schválenia zodpovednou osobou)?		
1	§40 j)	91. Je zavedená formalizovaná dokumentácia prístupových práv všetkých používateľov IS VS?		
2		**§ 41 Aktualizácia informačno-komunikačných technológií**		
3	§41 a)	92. Je zavedený schvaľovací proces pre zmeny existujúcich a zavádzanie nových ISVS a IKT, ktorý zároveň zahŕňa bezpečnostné požiadavky?		
1	§41 b)	93. Je zabezpečené menovanie zástupcu organizácie pre činnosti podľa predchádzajúceho bodu?		
1	§41 c)	94. Existuje zabezpečenie menovania zástupcu dodávateľa?		
		Ako je zabezpečené?		
2	§41 d)	95. Bolo pri každej zmene existujúceho alebo zavádzaní nového IS VS vykonané testovanie v dostatočnom rozsahu (min. 1 týždeň)?		
1	§41e) 1	96. Existuje ku každému IS VS používateľská dokumentácia (návod na používanie)?		

1	§41e) 2	97. Existuje ku každému IS VS administrátorská dokumentácia (návod na správu a prevádzku)?		
1	§41e) 3	98. Existuje ku každému IS VS prevádzková dokumentácia (architektúra, konfigurácie a väzby)?		
2		**§ 42 Účasť tretej strany**		
1	§42 a)	99. Je vykonávaná analýza rizík v súvislosti s dodávateľskými prácami?		
3	§42 b)	100. Sú v zmluvách s dodávateľmi zahrnuté bezpečnostné požiadavky?		
3	§42 c)	101. Je zamedzené alebo zmluvne zabezpečené, aby dodávatelia nemali prístup k údajom, ktoré sú aktíva podľa BP?		
2	§42 d)	102. Sú zmluvne vyžadované bezpečnostné požiadavky kontrolované? Ak áno, ako?		
3	§42 e)	103. Je zmluvne zabezpečené, aby nedodržanie bezpečnostných požiadaviek zo strany dodávateľa umožnilo neukončiť alebo neprebrať jeho dielo alebo prácu?		

Kategorizácia hodnotení:
100% - dodržiava
99 – 90% - významne dodržiava
89 – 70% - čiastočne dodržiava
69 – 50% - porušuje
49 – 25% - vážne porušuje
24 – 10% - veľmi vážne porušuje
9 – 9% - nedodržiava (zásadne porušuje)