Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Metodika vnútorného auditu informačnej bezpečnosti

Verzia:	0.1
Počet strán / príloh:	18/1
Dátum účinnosti:	01.08.2011
Vypracoval:	ATEMSEC, a.s.

Obsah

Skratky

BP	Bezpečnostná politika
IKT	Informačno-komunikačné technológie
IS	Informačný systém
MF SR	Ministerstvo financií Slovenskej republiky
ISVS	Informačný systém verejnej správy

1 Úvod

Metodika pre interné hodnotenia bezpečnosti poskytuje návod pre hodnotenie bezpečnostných štandardov podľa Výnosu MF SR o bezpečnostných štandardoch pre informačné systémy verejnej správy č. 312/2010 Z.z. (ďalej len „výnos MF SR“), ktorý bol vydaný na základe zákona č. 275/2006 o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

1.1 Cieľ

Cieľom metodického pokynu je umožniť správne pochopenie jednotlivých požiadaviek bezpečnostných štandardov a zároveň dosiahnuť čo možno najpresnejšie odpovede pri ich hodnotení.

2 Proces interného hodnotenia bezpečnosti IS

Proces interného hodnotenia bezpečnosti informačných systémov je definovaný v rámci bezpečnostnej politiky ISVS mesta Malacky. V rámci tohto procesu sú zastúpene role podľa 2.1.

2.1 Role v procese hodnotenia bezpečnosti IS

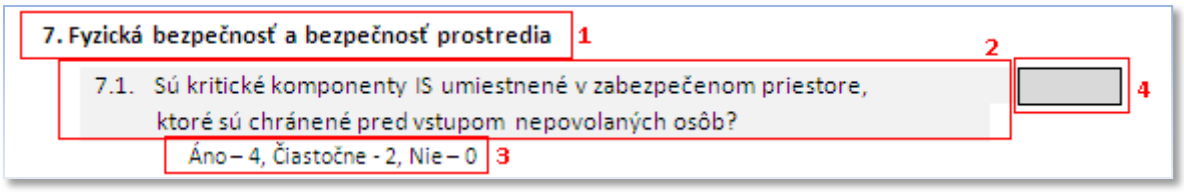
Rola	Rola v BP	Zodpovednosť
Iniciátor procesu	Primátor mesta	Zadáva príkaz na vykonanie interného hodnotenia bezpečnosti IS a zabezpečuje súčinnosť všetkých zúčastnených organizačných jednotiek.
Hodnotiteľ	Audítor informačnej bezpečnosti	Vykonáva hodnotenie, vypracováva dotazník a pripravuje výstup hodnotenia.
Overovateľ	Manažér informačnej bezpečnosti	Overuje výstup hodnotenia.

3 Metodika hodnotenia bezpečnosti IS

3.1 Postup pri hodnotení

Postup hodnotenia bezpečnosti informačných systémov mesta Malacky je založený na zodpovedaní otázok dotazníka, ktorý je postavený tak, aby komplexne zhodnotil implementáciu požadovaných bezpečnostných štandardov.

Hodnotiteľ prechádza dotazník, v ktorom sa nachádzajú rôzne otázky vo forme prezentovanej na Obr. 1 :

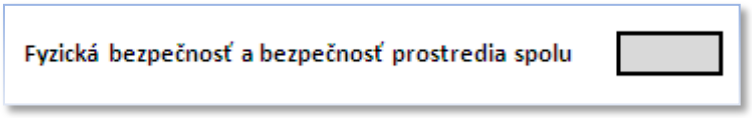


Obr. 1: Otázka v dotazníku hodnotenia bezpečnosti IS

1. Všetky otázky sú zoradené do skupín podľa rôznych aspektov bezpečnosti informačných systémov.
2. Znenie otázky.
3. Alternatívy odpovede na otázku s priradenými bodovými hodnotami.
4. Bodové hodnotenie otázky udelené hodnotiteľom.

Hodnotiteľ prechádza jednotlivými otázkami dotazníka. Po prečítaní otázky sa snaží reflektovať skutočný stav prostredníctvom navrhnutých alternatív odpovedí a priradením prílišného bodového hodnotenia. Toto bodové hodnotenie zapíše do pripraveného priestoru vedľa otázky.

Po zodpovedaní a priradení bodových hodnôt všetkým otázkam v rámci jednej skupiny, hodnotiteľ sčíta bodové hodnotenia a zapíše tento súčet do priestoru na Obr. 2:



Obr. 2: Výsledné hodnotenie skupiny otázok

Množstvo otázok sa vzťahuje k procesom, predpisom a nariadeniam, preto je potrebné mať k dispozícii všetku relevantnú dokumentáciu, a to aj takú, ktorá sa informačnej bezpečnosti týka iba okrajovo. Pri niektorých otázkach je pre overenie odpovede potrebná tiež fyzická kontrola IS alebo IKT, preto je dôležité, aby mal hodnotiteľ zabezpečenú dostatočnú súčinnosť všetkých organizačných zložiek orgánov mesta Malacky, ktoré sa na hodnotení priamo alebo nepriamo zúčastňujú.

Pri internom hodnotení bezpečnosti informačných systémov sa hodnotí splnenie požiadavky formulovanej v príslušnej otázke a danej konkrétnym štandardom, nie však kvalita alebo forma prevedenia. Tieto sa, ak je to potrebné, uvádzajú v poznámke k hodnoteniu, pričom je

možné v prípade nevhodnosti prevedenia odporúčať jej zlepšenie. V prípadoch, kde nie je možné jednoznačne určiť logickú odpoveď áno /nie, sa zvažuje, či bola dodržaná podstata danej požiadavky. Poznámky k hodnoteniu sú súčasťou protokolu o internom hodnotení bezpečnosti informačných systémov (viď. 3.3).

3.2 Výpočet hodnotenia

Na vypracovanie percentuálneho hodnotenia dodržiavania konkrétnych štandardov, ako aj výsledného hodnotenia celej oblasti bezpečnostných štandardov, je zavedený systém váh. Jednotlivé hodnotené skupiny majú určené rôzne váhy podľa dôležitosti kategórie. Hodnotiteľ vypočíta výsledné hodnotenia prostredníctvom postupu na Obr. 3.

	Body	Váha	Výsledná hodnota	Maximálna hodnota	Percent. hodnotenie
	1		2		3
1. Riadenie informačnej bezpečnosti		3		315	%
2. Personálna bezpečnosť		2		56	%
3. Manažment rizík pre oblasť informačnej bezpečnosti		2		72	%
4. Kontrolný mechanizmus riadenia informačnej bezpečnosti		2		24	%
5. Ochrana proti škodlivému kódu		1		36	%
6. Sieťová bezpečnosť		1		16	%
7. Fyzická bezpečnosť a bezpečnosť prostredia		2		128	%
8. Aktualizácia softvéru a IKT		2		88	%
9. Monitorovanie a manažment bezpečnostných incidentov		1		42	%
10. Zálohovanie		1		28	%
11. Riadenie prístupu		2		128	%
12. Účasť tretej strany		2	4	96	5 %
	Spolu			1029	%

Obr. 3: Postup zapisovania výsledku hodnotenia

1. Hodnotiteľ zapíše sumu bodového hodnotenia pre danú skupinu do stĺpca “Body“.
2. Sumu bodového hodnotenia pre danú skupinu vynásobí príslušnou váhou uvedenou v stĺpci „Váha“ a výsledok zapíše do stĺpca „Výsledná hodnota“.
3. Do stĺpca „Percent. Hodnotenie“ hodnotiteľ zapíše výsledok nasledovného vzťahu Výsledná hodnota/Maximálna hodnota *100

4. Po zapísaní výsledkov pre všetky hodnotené kategórie hodnotiteľ zapíše výslednú sumu pre všetky výsledné hodnoty do posledného riadku.
5. Hodnotiteľ vypočíta a zapíše výsledné percentuálne hodnotenie ako hodnotu Výsledná hodnota/Maximálna hodnota *100, kde číselné hodnoty premenných tohto vzťahu dosadí z posledného riadku výsledkovej tabuľky.

Výsledné hodnotenie kontroly vyjadruje percentuálne dodržiavanie bezpečnostných štandardov, ktoré je kategorizované nasledovne:

Výsledné hodnotenie	Slovná kategória
100 %	Dodržiava
99 – 90 %	Významne dodržiava
89 – 70 %	Čiastočne dodržiava
69 – 50 %	Porušuje
49 – 25 %	Vážne porušuje
24 – 10 %	Veľmi vážne porušuje
9 % – 0 %	Nedodržiava (zásadne porušuje)

3.3 Výstup hodnotenia

Výstupom hodnotenia je protokol o hodnotení. Tento protokol musí obsahovať:

1. Meno hodnotiteľa a dátum vypracovania protokolu.
2. Meno overovateľa a dátum overenia.
3. Poznámky k jednotlivým otázkam, kde sa na otázky odkazuje prostredníctvom čísla otázky.
4. Slovné vyjadrenie hodnotiteľa k priebehu a výsledku hodnotenia.
5. Výsledné percentuálne a slovné hodnotenie.
6. Prílohou k protokolu je vypracovaný dotazník a výsledková tabuľka podľa Prílohy č.1 tejto metodiky.
7. Prílohou k protokolu je tiež príkaz na uskutočnenie hodnotenia.
8. Protokol s prílohami je podpísaný hodnotiteľom a overovateľom.

4 Záverečné ustanovenia

Zmeny v tomto predpise môže vykonať iba jeho autor alebo jeho vedúcim určený pracovník.

Tento dokument nadobúda účinnosť dňom:.....

Malacky dňa .....

Primátor mesta Malacky

Príloha č.1: Dotazník hodnotiteľa bezpečnosti informačných systémov

1. Riadenie informačnej bezpečnosti

1.1. Existuje bezpečnostná politika (BP)? Áno – 4, Nie – 0	
1.2. Ak existuje BP, je schválená v rámci procesov organizácie? Áno – 4, Nie – 0, Neexistuje – 0	
1.3. Sú určené bezpečnostné ciele? Áno – 4, Nie – 0	
1.4. Sú určené spôsoby ich vyhodnocovania alebo dosahovania? Áno – 4, Nie – 0	
1.5. Obsahuje BP podporu vedenia (podpis vedúceho pracovníka)? Áno – 4, Nie – 0	
1.6. Sú stanovené pozície pre manažment informačnej bezpečnosti? Áno – 4, Nie – 0	
1.7. Ako je vyhodnotený a zabezpečený súlad BP s ostatnými právnymi dokumentmi? Obsahuje BP vzťah k iným právnym dokumentom? Áno – 4, Nie – 0	
1.8. Ako sa požiadavky, vyplývajúce z právnych dokumentov premietli do správy informačných systémov? Dostatočne – 4, Čiastočne – 2, Nedostatočne – 0	
1.9. Sú stanovené úrovne ochrany IS? Áno – 4, Nie – 0	
1.10. Sú definované aktíva, ktoré súvisia s IS? Áno – 3, Nie – 0	
1.11. Sú definované kritické aktíva? Áno – 1, Nie – 0	
1.12. Stanovuje BP rozsah auditu informačnej bezpečnosti? Áno – 1, Nie – 0	
1.13. Stanovuje BP periodicitu auditu informačnej bezpečnosti? Áno – 1, Nie – 0	
1.14. Sú audity informačnej bezpečnosti vykonávané podľa BP? Áno – 2, Nie – 0	
1.15. Sú vypracované smernice pre zálohovanie? Áno – 2, Nie – 0	
1.16. Ak sú smernice pre zálohovanie vypracované, existuje rozdelenie údajov pre rôzne typy záloh? Áno – 1, Nie – 0	
1.17. Ak sú smernice pre zálohovanie vypracované, určuje BP ako je postihované nedodržiavanie týchto smerníc? Áno – 1, Nie – 0	
1.18. Definuje BP ako často sa vykonáva monitorovanie bezpečnosti softvéru? Áno – 2, Nie – 0	
1.19. Definuje BP ako často sa vykonáva aktualizácia softvéru? Áno – 2, Nie – 0	
1.20. Existuje zoznam dokumentov na zaistenie informačnej bezpečnosti? Áno – 1, Nie – 0	
1.21. Sú dokumenty na zaistenie informačnej bezpečnosti vypracované? Áno – 2, Nie – 0	

1.22. Existuje proces na aktualizáciu dokumentov na zaistenie informačnej bezpečnosti? Áno – 2, Nie – 0	
1.23. Je stanovený postup revízie bezpečnostnej politiky? Áno – 2, Nie – 0	
1.24. Je proces skutočného vykonania revízie BP v súlade s obsahom BP? Áno – 1, Nie – 0	
1.25. Sú stanovené dôvody na mimoriadnu revíziu BP? Áno – 1, Nie – 0	
1.26. Sú stanovené postupy v prípade nedodržiavania bezpečnostnej politiky? Áno – 12, Nie – 0	
1.27. Je stanovená osoba(y) zodpovedná(é) za informačnú bezpečnosť? Áno – 12, Nie – 0	
1.28. Má osoba, zodpovedná za informačnú bezpečnosť definované úlohy? Áno – 8, Nie – 0	
1.29. Existujú smernice/predpisy s definovaním kompetencií, prostredníctvom ktorých je zabezpečená koordinácia aktivít organizačných zložiek pri riešení informačnej bezpečnosti? Áno – 4, Nie – 0	
1.30. Sú určené konkrétne zodpovedné osoby / útvary za jednotlivé aktíva? Áno – 4, Nie – 0	
1.31. Sú určené bezpečnostné pozície / role v jednotlivých IS? Áno – 4, Nie – 0	
Riadenie informačnej bezpečnosti spolu	

2. Personálna bezpečnosť

2.1. Je zabezpečené poučenie o BP a povinnostiach z nej vyplývajúcich? Áno – 2, Nie – 0	
2.2. Existuje tlačivo / dokument o poučení o BP? Áno – 2, Nie – 0	
2.3. Je zabezpečené poučenie o právach a povinnostiach pred vstupom do IS? Áno – 4, Nie – 0	
2.4. Sú povinnosti vyplývajúce z BP uvedené v pracovných zmluvách príslušných zamestnancov? Áno – 4, Nie – 0	
2.5. Existuje vypracovaný postup pre disciplinárne konanie v prípade porušenia BP alebo relevantných predpisov? Áno – 4, Nie – 0	
2.6. Je zabezpečená povinnosť oznamovať bezpečnostné incidenty? Áno – 4, Nie – 0	
2.7. Koľko z nasledovných oblastí pokrývajú postupy pri ukončovaní pracovného pomeru - mlčanlivosť, odovzdanie pridelených zariadení, odstránenie údajov zo zariadení, zrušenie prístupových práv, odovzdanie agendy? Všetky – 8, (4-3) – 6, (2-1) – 4, postupy nie sú vypracované – 0	
Personálna bezpečnosť spolu	

3. Manažment rizík pre oblasť informačnej bezpečnosti

3.1. Existuje zavedenie systému riadenia rizík v relevantnom dokumente?	
Áno – 2, Nie – 0	
3.2. Existuje klasifikácia rizík?	
Áno – 1, Nie – 0	
3.3. Sú zavedené praktické postupy systému riadenia rizík?	
Áno – 1, Nie – 0	
3.4. Existuje implementovaný systém monitorovania rizík?	
Áno – 4, Nie – 0	
3.5. Používa sa systém riadenia rizík a monitorovania?	
Áno – 4, Nie – 0	
3.6. Zohľadňujú riziká aj aktíva a IS mimo priestorov povinnej osoby?	
Áno – 3, Nie – 0	
3.7. Existujú zavedené postupy na redukciu týchto rizík?	
Áno – 1, Nie – 0	
3.8. Existuje analýza závislosti na IS?	
Áno – 4, Nie – 0	
3.9. Existuje analýza kritických procesov?	
Áno – 4, Nie – 0	
3.10. Existuje analýza (zoznam) kritických informačných systémov?	
Áno – 4, Nie – 0	
3.11. Ak áno, sú riziká pre kritické IS špecificky oddelené?	
Áno – 4, Nie – 0	
3.12. Existujú vypracované plány na obnovu?	
Áno – 4, Nie – 0	
Manažment rizík pre oblasť informačnej bezpečnosti spolu	

4. Kontrolný mechanizmus riadenia informačnej bezpečnosti

4.1. Vykonáva sa vnútorná kontrola alebo audit informačnej bezpečnosti?	
Áno – 6, Nie – 0	
4.2. Ak áno, je dodržiavaná periodicita definovaná v BP?	
Áno – 2, Nie – 0	
4.3. Sú auditné správy vyhodnocované?	
Áno – 1, Nie – 0	
4.4. Sú auditné správy chránené?	
Áno – 1, Nie – 0	
4.5. Sú auditné správy archivované?	
Áno – 2, Nie – 0	
Kontrolný mechanizmus riadenia informačnej bezpečnosti spolu	

5. Ochrana proti škodlivému kódu

5.1. Je zavedená ochrana e-mailov pred škodlivým kódom?	
Áno – 4, Nie – 0	
5.2. Je zavedená detekcia škodlivého kódu na zariadeniach IS?	
Áno – 4, Nie – 0	

5.3. Sú kontrolované zasielané a prijímané súbory? Áno – 4, Nie – 0	
5.4. Je zavedená ochrana webových sídiel mesta Malcky a kontrola existencie škodlivého kódu (najmä v používanom CMS)? Áno – 4, Nie – 0	
5.5. Je zavedená ochrana pred nevyžiadanou elektronickou poštou? Áno – 4, Nie – 0	
5.6. Je zavedená kontrola legality softvéru používaného používateľmi? Áno – 2, Nie – 0	
5.7. Existuje vnútorný predpis, ktorý riadi správu inštalácií softvéru? Áno – 2, Nie – 0	
5.8. Existujú pravidlá pre sťahovanie súborov z externých sietí? Áno – 4, Nie – 0	
5.9. Existuje podpora kryptografických prostriedkov autenticity a integrity? Áno – 2, Nie – 0	
5.10. Používa sa v IS mesta Malacky elektronický podpis? Áno – 2, Nie – 0	
5.11. Existuje podpora šifrovania elektronických dokumentov? Áno – 2, Nie – 0	
5.12. Existuje predpis, ktorý upravuje šifrovania elektronických dokumentov? Áno – 2, Nie – 0	
Ochrana proti škodlivému kódu spolu	

6. Sieťová bezpečnosť

6.1. Existuje implementácia firewallov? Áno – 4, Nie – 0	
6.2. Sú nasadené aj personálne firewally? Áno – 4, Nie – 0	
6.3. Je vedená evidencia o všetkých miestach prepojení sietí (tzv. uzly) v správe povinnej osoby? Áno – 2, Nie – 0	
6.5. Ak áno, je táto evidencia aktualizovaná? Áno – 2, Nie – 0	
6.6. Sú vypracované interné akty riadenia prístupu k sieťovým pripojeniam? Áno – 4, Nie – 0	
Sieťová bezpečnosť spolu	

7. Fyzická bezpečnosť a bezpečnosť prostredia

7.1. Sú kritické komponenty IS umiestnené v zabezpečenom priestore, ktoré sú chránené pred vstupom nepovolaných osôb? Áno – 4, Čiastočne - 2, Nie – 0	
7.2. Sú kritické komponenty IS chránené pred haváriami technickej infraštruktúry? Áno – 2, Čiastočne - 1, Nie – 0	
7.3. Sú kritické komponenty IS chránené pred vplyvmi prostredia?	

Áno – 2, Čiastočne - 1, Nie – 0

7.4. Je priestor, v ktorom sú umiestnené kritické komponenty IS zabezpečený fyzickými prostriedkami?
Áno – 8, Čiastočne - 4, Nie – 0

7.5. Je tento priestor umiestnený dostatočne ďaleko, od ohrozenia vodoinštaláciou, horľavinami a pod.?
Áno – 4, Čiastočne - 2, Nie – 0

7.6. Existujú pravidlá pre prácu v zabezpečenom priestore?
Áno – 4, Nie – 0

7.7. Je zabezpečená ochrana serverov pred výpadkom elektriny?
Áno – 6, Čiastočne – 4, Nie – 0

7.8. Je zabezpečená ochrana pracovných staníc pred výpadkom elektriny?
Áno – 2, Čiastočne – 1, Nie – 0

7.9. Existujú záložné kapacity IS (sekundárne, resp. virtualizované servery, ..)?
Áno – 2, Nie – 0

7.10. Ak áno, sú umiestnené v sekundárnom zabezpečenom priestore?
Áno – 2, Nie – 0

7.11. Je prevádzka, používanie a manažment IS v súlade s legislatívou vnútornými predpismi a zmluvami?
Áno – 4, Nie – 0

7.12. Existujú pravidlá pre údržbu, uchovávanie a evidenciu technických a evidenciu technických komponentov IS?
Áno – 4, Nie – 0

7.13. Existujú pravidlá pre používanie zariadení IS na iné účely?
Áno – 2, Nie – 0

7.14. Existujú pravidlá pre prenos a používanie zariadení IS mimo určených priestorov (v rámci orgánov mesta Malacky)?
Áno – 2, Nie – 0

7.15. Existujú pravidlá pre prenos a používanie zariadení IS mimo určených priestorov (mimo priestorov MsP a MsÚ mesta Malacky)?
Áno – 4, Nie – 0

7.16. Existujú pravidlá pre vymazávanie, vyraďovanie a likvidáciu zariadení IS?
Áno – 2, Nie – 0

7.17. Existujú pravidlá pre vymazávanie, vyraďovanie a likvidáciu záloh?
Áno – 2, Nie – 0

7.18. Existujú pravidlá pre narábanie so všetkými informáciami v elektronickej podobe, dokumentáciou systému a pamäťovými médiami?
Áno – 2, Nie – 0

7.19. Je stanovená maximálna prípustná doba výpadku IS?
Áno – 4, Nie – 0

7.20. Sú stanovené opatrenia na riešenie obnovy prevádzky v prípade výpadku?
Áno – 2, Nie – 0

Fyzická bezpečnosť a bezpečnosť prostredia spolu

8. Aktualizácia softvéru a IKT

8.1. Je zabezpečená aktualizácia verzií inštalovaného ochranného softvéru?
Áno – 2, Nie – 0

8.2. Ak áno, je táto aktualizácia v súlade s BP?

Áno – 2, Nie – 0

8.3. Je zavedený schvaľovací proces pre zmeny existujúcich a zavádzanie nových IS a IKT?
Áno – 8, Nie – 0

8.4. Ak áno, zahŕňa tento proces bezpečnostné požiadavky?
Áno – 4, Čiastočne – 2, Nie – 0

8.5. Je zabezpečené menovanie zodpovednej osoby pre činnosti podľa procesu aktualizácie IKT?
Áno – 4, Nie – 0

8.6. Existuje zabezpečenie menovania zástupcu dodávateľa IKT?
Áno – 4, Nie – 0

8.7. Aká je priemerná doba testovania pri zmene existujúceho alebo zavádzaní nového IS?
Viac ako 2 týždne – 6, 1-2 týždne – 4, Menej ako 1 týždeň – 0

8.8. Existuje dokumentácia o testovaní?
Áno – 2, Nie – 0

8.9. Existuje ku každému IS VS používateľská dokumentácia?
Áno – 4, Nie – 0

8.10. Existuje ku každému IS administrátorská dokumentácia (návod na správu a prevádzku)?
Áno – 4, Nie – 0

8.11. Existuje ku každému IS VS prevádzková dokumentácia (architektúra, konfigurácie a väzby)?
Áno – 4, Nie – 0

Aktualizácia softvéru a IKT spolu

9. Monitorovanie a manažment bezpečnostných incidentov

9.1. Je vypracovaný interný akt pre ohlasovanie bezpečnostných incidentov?
Áno – 8, Nie – 0

9.2. Je vypracovaný interný akt pre riešenie a vyhodnocovanie typov bezpečnostných incidentov?
Áno – 4, Nie – 0

9.3. Je vypracovaný interný akt pre spôsob evidencie bezpečnostných incidentov a použitých riešení?
Áno – 4, Nie – 0

9.4. Je zabezpečené informovanie používateľov IS o postupoch pri hlásení bezpečnostných incidentov?
Áno – 2, Nie – 0

9.5. Existuje evidencia všetkých výpadkov?
Áno – 4, Čiastočne – 2, Nie – 0

9.6. Existuje evidencia spôsobu riešenia výpadkov?
Áno – 4, Čiastočne – 2, Nie – 0

9.7. Je zavedený systém na detekciu prienikov (najmenej IDS)?
Áno – 4, Nie – 0

9.8. Existuje kontaktné miesto na ohlasovanie bezpečnostných incidentov a slabých miest?
Áno – 6, Nie – 0

9.9. Je možné ohlásiť aj bezpečnostný incident, identifikovaný externe?

Áno – 2, Nie – 0

9.10. Vykonáva sa periodické hodnotenie slabých miest IS (najmenej raz za rok)?
Áno – 4, Nie – 0

Monitorovanie a manažment bezpečnostných incidentov spolu

10. Zálohovanie

10.1. Existujú archivačné zálohy podľa BP (aspoň raz za 2 mesiace)?
Áno – 4, Nie – 0

10.2. Existujú prevádzkové zálohy podľa BP (aspoň raz za týždeň)?
Áno – 4, Nie – 0

10.3. Má archivačná záloha dve kópie?
Áno – 4, Nie – 0

10.4. Vykonáva sa test funkcionality dátového nosiča jednotlivých záloh?
Áno – 4, Nie – 0

10.5. Vykonáva sa test obnovy systému zo zálohy (najmenej raz za rok)?
Aspoň raz za rok – 3, Menej ako raz za rok – 2, Nie – 0

10.6. Existuje záznam z testu obnovy systému zo zálohy?
Áno – 1, Nie – 0

10.7. Sú zálohy a licencovaný softvér ukladané v uzamykateľnom priestore
Áno – 4, Nie – 0

10.8. Ukladá sa druhá kópia archivačnej zálohy v inom priestore?
Áno – 4, Nie – 0

Zálohovanie spolu

11. Riadenie prístupu

11.1. Je zavedená autentifikácia užívateľov pri vstupe do všetkých IS?
Áno – 8, Čiastočne – 4, Nie – 0

11.2. Je zavedená autorizácia užívateľov pri vstupe do všetkých IS (rozličné prístupové práva diferencované podľa užívateľských rolí)?
Áno – 4, Čiastočne – 2, Nie – 0

11.3. Je vypracovaný interný akt riadenia prístupu k údajom a funkciám IS?
Áno – 8, Nie – 0

11.4. Existuje postup a určená zodpovednosť pre prideľovanie prístupových práv?
Áno – 4, Nie – 0

11.5. Sú určené bezpečnostné požiadavky pre používateľov pri používaní IS?
Áno – 4, Nie – 0

11.6. Sú zmeny prístupu automaticky zaznamenávané a archivované?
Áno – 4, Nie – 0

11.7. Existujú bezpečnostné zásady pre mobilné pripojenie?
Áno – 4, Nie – 0

11.8. Je zavedená kontrola, že používatelia nepoužívajú IS VS na nelegálne účely?
Áno – 4, Nie – 0

11.9. Je zabezpečené, aby administrátori nemali prístup k údajom, ktoré nepotrebujú na vykonávanie svojich úloh?

Áno – 8, Nie – 0

11.10. Existuje automatické zaznamenávanie prístupu všetkých používateľov a správcov IS do systému?
Áno – 6, Nie – 0

11.11. Sú zaznamenávané aj niektoré kategórie činností?
Áno – 2, Nie – 0

11.12. Existuje relevantný postup a implementované riešenie vymazávania záznamov (napr. zasielanie sekundárnej kópie bezp. manažérovi)?
Áno – 4, Nie – 0

11.13. Je zavedená formalizovaná dokumentácia prístupových práv všetkých používateľov IS?
Áno – 4, Nie – 0

Riadenie prístupu spolu

12. Účasť tretej strany

12.1. Je vykonávaná analýza rizík v súvislosti s dodávateľskými prácami na IS?
Áno – 4, Čiastočne – 2, Nie – 0

12.2. Sú v zmluvách s dodávateľmi zahrnuté bezpečnostné požiadavky (súlad s výnosom MF SR a BP, mlčanlivosť, ochrana osobných údajov a pod.)?
Áno – 12, Čiastočne – 6, Nie – 0

12.4. Je zamedzené alebo zmluvne zabezpečené, aby dodávatelia nemali prístup údajom, ktoré sú aktíva podľa BP?
Áno – 12, Čiastočne – 6, Nie – 0

12.5. Sú zmluvne vyžadované bezpečnostné požiadavky kontrolované?
Áno – 8, Nie – 0

12.9. Je zmluvne zabezpečené, aby nedodržanie bezpečnostných požiadaviek zo strany dodávateľa umožnilo neukončiť alebo neprebrať jeho dielo?
Áno – 12, Nie – 0

Účasť tretej strany spolu

Vyhodnotenie dotazníka bezpečnosti informačných systémov

		Body	Váha	Výsledná hodnota	Maximálna hodnota	Percent. hodnotenie
1.	Riadenie informačnej bezpečnosti		3		315	%
2.	Personálna bezpečnosť		2		56	%
3.	Manažment rizík pre oblasť informačnej bezpečnosti		2		72	%
4.	Kontrolný mechanizmus riadenia informačnej bezpečnosti		2		24	%
5.	Ochrana proti škodlivému kódu		1		36	%
6.	Sieťová bezpečnosť		1		16	%
7.	Fyzická bezpečnosť a bezpečnosť prostredia		2		128	%
8.	Aktualizácia softvéru a IKT		2		88	%
9.	Monitorovanie a manažment bezpečnostných incidentov		1		42	%
10.	Zálohovanie		1		28	%
11.	Riadenie prístupu		2		128	%
12.	Účasť tretej strany		2		96	%
		Spolu			**1029**	**%**