53) skryto

54) skryto

55) skryto

4.2.3 Údržba zařízení

Organizační zásady:

56) skryto

4.2.4 Bezpečnost zařízení mimo prostory justiční složky

Organizační zásady:

57) Před přemístěním zařízení mimo chráněné prostory musí z něho být odstraněny všechny informace (např. vyjmutím veškerých nosičů informací nebo jejich bezpečným výmazem). V opačném případě musí být zařízení pod neustálým dohledem odpovědného pracovníka justiční složky nebo jiné oprávněné smluvní strany.

58) Použití prostředků pro zpracování informací mimo budovy justiční složky, bez ohledu na jejich vlastníka, podléhá schválení odpovědnou osobou.

59) Zařízení používané mimo prostory justiční složky musí být zabezpečeno s přihlédnutím k různým rizikům, která vyplývají z jejich použití mimo justiční složku.

   a) Zařízení ICT a nosiče informací, při cestách mimo justiční složku, nesmí být ponechána bez dozoru (zejména nesmí být ponechána bez dozoru v dopravním prostředku, v autě, ve veřejných prostorách, v konferenčních centrech nebo zasedacích místnostech apod.). Mobilní výpočetní zařízení a sdělovací technika (viz 158)) musí být přepravována jako příruční zavazadla a v rámci možností ukrývána. V případě, kdy uživatel musí nechat mobilní výpočetní zařízení bez dozoru, musí jej ponechat v uzamčených prostorách nebo úložných schránkách s dostatečně omezeným přístupem (z toho je vyjmut automobil, ve kterém nesmí být zařízení ponecháno bez dozoru);

   b) Musí být dodržovány pokyny výrobce týkající se ochrany zařízení, například zajištění ochrany proti působení silného magnetického pole;

   c) Pro práci doma musí být určena vhodná opatření na základě hodnocení rizik.

4.2.5 Bezpečné zničení nebo opakované použití zařízení

Organizační zásady:

60) Všechna zařízení obsahující paměťová média (počítače, velkokapacitní tiskárny, multifunkční zařízení apod.) musí být před jejich zničením nebo opakovaným použitím zkontrolována a musí být zajištěno, že data a licencované programové vybavení jsou odstraněny nebo bezpečně vymazány nebo zničeny (viz 98)).

4.2.6 Přemístění majetku

Organizační zásady:

61) O přemístění zařízení ICT musí být proveden záznam. Tato zásada se vztahuje

   a) na veškerá zařízení umístěná v serverovnách;

   b) na výpočetní zařízení koncových uživatelů, která nejsou mobilními zařízeními (viz 158)), a to v případech, kdy by měla být přemístěna mimo prostory justiční složky resp. organizační jednotky.

5 ŘÍZENÍ KOMUNIKACÍ A ŘÍZENÍ PROVOZU

5.1 Provozní postupy a odpovědnosti

5.1.1 Dokumentace provozních postupů

Organizační zásady:

62) Všechny provozní postupy používané při správě, údržbě a provozu systémů ICT musí být dokumentovány v podobě formálních dokumentů, které podléhají změnovému řízení. Tyto dokumenty musí být dostupné všem pracovníkům, kteří danou činnost provádějí.

63) skryto

64) Součástí popisu postupů musí být i informace o tom, kdo je oprávněn danou operaci provést, resp. kdo odpovídá za její včasné a správné provedení. Podrobnost postupů musí být na takové úrovni, aby umožnila provádět zásahy i osobám znalým použitý produkt bez podrobných znalostí konkrétního systému ICT.

65) Provedení operací, které mění konfigurace HW, SW a jejich nastavení, a události vztahující se k poruchám a nestandardnímu chování systému ICT, musí být zaznamenáno do příslušného provozního deníku systému, pracoviště apod.

5.1.2 Řízení změn

Organizační zásady:

66) Konfigurace systému ICT a nastavení jednotlivých částí musí být dokumentovány. Tato dokumentace musí být vždy aktuální.

67) skryto

68) Veškeré změny v systému ICT musí být testovány před jejich aplikací na cílový systém.

69) Úpravy migračních postupů musí být před aplikací na cílový systém otestovány na reprezentativním vzorku dat.

70) Součástí každé změny systému ICT musí být připravený postup pro návrat do původního stavu před změnou.

5.1.3 Rozdělení povinností

Organizační zásady:

71) skryto

5.1.4 Vzájemné oddělení vývoje, testování a provozu

Organizační zásady:

72) skryto

5.2 Řízení dodávek a služeb třetích stran

Organizační zásady:

73) Služby v oblasti ICT dodávané externími subjekty a třetími stranami musí být realizovány na základě smluvního vztahu (viz 3.1), který zajistí soulad s požadavky na zajištění bezpečnosti informací (zejména dodržování této Politiky BICT a příslušných předpisů justičních složek) a nápravu případných nedostatků.

a) Za zapracování příslušných ustanovení do smlouvy odpovídá zaměstnanec, který je odpovědný za přípravu smluvního vztahu;

b) O připravované smlouvě o dodávce služeb spojených s provozem systému ICT je zaměstnanec odpovědný za přípravu smluvního vztahu povinen informovat vedoucího informatika složky, který je povinen zkontrolovat obsah ustanovení spojených s bezpečností.

5.3 Plánování a přejímání systémů ICT

5.3.1 Řízení kapacit

Organizační zásady:

74) skryto

5.3.2 Přejímání systémů

Organizační zásady:

75) Přejímání nových systémů ICT, jejich aktualizace, zavádění nových verzí včetně vhodného způsobu testování systému v průběhu vývoje a před zavedením do ostrého provozu musí probíhat podle zdokumentovaných postupů (viz kapitola 5.1.2 „Řízení změn").

5.4 Ochrana proti škodlivým programům a mobilním kódům

5.4.1 Opatření na ochranu proti škodlivým programům

Organizační zásady:

76) skryto

77) skryto

78) skryto

Technické zásady:

79) Všechny vstupy nejistého nebo neověřeného původu musí před dalším zpracováním projít kontrolou na přítomnost škodlivých programů.

80) Všechny stanice, ze kterých je přistupováno k systému ICT, musí být vybaveny aktuálním software na detekci škodlivých programů (min. antivirový software), který je používán a pravidelně aktualizován. Toto ustanovení musí být součástí interních předpisů justičních složek a součástí závazné provozní směrnice systému ICT, a musí být také součástí smluv s externími subjekty o přístupu do systému ICT).

81) skryto

5.4.2 Opatření na ochranu proti mobilním kódům

Organizační zásady:

82) Na ochranu proti mobilním kódům nesmí být z centrálních komponent interních systémů ICT justičních složek přistupováno přímo na zdroje v Internetu ani v jiných nedůvěryhodných sítích.

5.5 Zálohování

5.5.1 Zálohování dat a systémů

Organizační zásady:

83) skryto

84) skryto

85) skryto

86) skryto

87) skryto

Technické zásady:

88) skryto

89) skryto

5.6 Správa bezpečnosti sítě a podpůrné infrastruktury

5.6.1 Síťová opatření

Organizační zásady:

90) skryto

91) skryto

Technické zásady:

92) skryto

5.6.2 Bezpečnost síťových služeb

Technické zásady:

93) Veškeré přenosy informací (viz 10)) mezi systémy ICT přes externí sítě musí být chráněny šifrováním spojeným s kontrolou integrity přenášených dat.

94) Veškeré přenosy informací (viz 10)) mezi systémy ICT přes interní sítě, které nejsou pod výhradní kontrolou justičních složek a/nebo jsou vedeny prostředím nebo vyzařují do prostředí mimo jejich kontrolu, musí být chráněny šifrováním spojeným s kontrolou integrity přenášených dat.

95) Veškeré přenosy mezi systémy ICT musí mít zajištěnu integritu přenášených dat.

96) Komunikace mezi primárním a záložním centrem (je-li zřízeno) musí být šifrována.

5.7 Bezpečnost při zacházení s nosiči informací

5.7.1 Správa nosičů informací (počítačových médií)

Organizační zásady:

97) skryto

98) skryto

5.7.2 Zničení záznamů na nosičích informací (počítačových médiích)

Organizační zásady:

99) Nosiče informací, které byly použity v systému ICT (média v počítačích, velkokapacitních tiskárnách a multifunkčních zařízeních) a jsou dále nepotřebné, musí být bezpečně vymazány před tím, než budou zničeny, vyřazeny nebo použity mimo procesy systému ICT.

100) Nosiče informací, které nebyly bezpečně vymazány a jsou dále nepotřebné nebo nefunkční, musí být bezpečně fyzicky zničeny.

101) Nosiče informací, z nichž záznamy nelze bezpečně vymazat programovými prostředky (např. Flash-disky a disky SSD), nesmí být vyjmuty ze systému ICT k opakovanému použití v systému jiné organizace.

102) skryto

Technické zásady:

103) Bezpečný výmaz dat programovými prostředky se provádí přepsáním všech datových sektorů nosiče – jednou zvolenou hodnotou (např. 0x00), potom doplňkem zvolené hodnoty (např. 0xff) a následně náhodným vzorkem).

104) Fyzické zničení nosiče informací se provádí mechanickým zničením. V případě nosičů, na kterých je používán elektromagnetický princip záznamu (HDD, datové pásky apod.), je fyzickým zničením také výmaz v demagnetizátoru (degausseru).

5.7.3 Postupy pro manipulaci s informacemi

Organizační zásady:

105) skryto

106) Před předáním informací uživateli musí být provedeny kontroly oprávněnosti požadavku.

5.7.4 Bezpečnost systémové dokumentace

Organizační zásady:

107) skryto

5.8 Výměna informací

5.8.1 Postupy při výměně informací a programů

Organizační zásady:

108) skryto

5.8.2 Dohody o výměně informací a programů

Organizační zásady:

109) Výměna informací a programového vybavení IS a aplikací s externím subjektem musí probíhat podle definovaného, dokumentovaného a schváleného postupu. Tento postup musí stanovit odpovědnosti vedoucích zaměstnanců za procesy předávání a převzetí informací, nosičů a citlivých předmětů, zaručit

integritu a autenticitu předávaného programového vybavení, a stanovit odpovědnosti a postupy vypořádání bezpečnostních incidentů.

110) Výměna informací a programů (elektronická i manuální) musí být založena na formalizovaných dohodách, z nichž některé mohou mít podobu formálních smluv nebo mohou být součástí podmínek pracovního vztahu.

5.8.3 Bezpečnost nosičů informací při přepravě

Organizační zásady:

111) Nosiče informací obsahující informace (včetně programového vybavení, záloh apod.) musí být při přepravě mimo chráněné prostory justiční složky pod neustálým dohledem pracovníka justiční složky nebo oprávněného smluvního partnera nebo musí být využito služeb spolehlivých kurýrů.

112) V případě použití přepravy nosičů informací kurýrem musí být informace v elektronické podobě na nosičích informací v zašifrované podobě. Pro šifrování musí být použity schválené algoritmy.

113) Zásilka obsahující nosiče informací musí být zabalena tak, aby bylo možno zjistit vzniklé fyzické poškození nebo otevření zásilky při přepravě.

5.8.4 Elektronické zasílání zpráv

Organizační zásady:

114) Informace mohou být přenášeny elektronickou komunikací pouze v případě, že jsou splněny požadavky na ochranu informace (10)). Tento přenos musí být upraven v podobě formálně řízeného dokumentu, který podléhá změnovému řízení.

5.8.5 Veřejně přístupné informace

Organizační zásady:

115) Informace publikované na veřejně přístupných systémech musí být chráněny proti neoprávněné modifikaci.

a) Programy, data a jiné informace zpřístupňované na veřejně dostupných systémech a vyžadující vysoký stupeň integrity, musí být chráněny adekvátními mechanizmy (například digitálním podpisem);

b) Veřejně přístupné systémy by měly být testovány na slabiny a možná selhání předtím, než jsou na ně umístěny informace;

c) Pro zveřejnění informací musí existovat formální schvalovací procesy;

d) Veškeré vstupy poskytnuté zvenku by měly být prověřeny a projít schválením.

5.9 Monitorování

5.9.1 Pořizování auditních záznamů

Organizační zásady:

116) Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události (privilegované operace, systémová varování chyby, neautorizovaný přístup, viry, atd.), musí být uchovány včetně informací o zdroji události, přesném čase atd., za účelem následné kontroly provedených operací a přístupů.

117) skryto

5.9.2 Monitorování používání systému

Organizační zásady:

118) skryto

119) skryto

Technické zásady:

120) Pokud to systém nebo aplikace umožňuje, nebo je vyvíjen speciálně pro použití v justiční složce, musí být napojen na centrální systém kontrolující jeho správnou funkčnost, který na definované události proaktivně informuje odpovědné osoby.

5.9.3 Ochrana vytvořených záznamů

Technické zásady:

121) Auditní záznamy musí být chráněny před modifikací.

5.9.4 Provozní deník

Organizační zásady:

122) skryto

123) skryto

5.9.5 Záznam selhání systému

Organizační zásady:

124) skryto

5.9.6 Synchronizace hodin

Technické zásady:

125) Všechny komponenty kritických systémů ICT a aplikací musí být napojeny na zdroj jednotného času.

6 ŘÍZENÍ PŘÍSTUPU

6.1 Požadavky na řízení přístupu

6.1.1 Politika řízení přístupu

Organizační zásady:

126) skryto

127) skryto

128) Politika řízení přístupu musí zohledňovat následující principy:

- Všechno co není výslovně povoleno, je zakázáno;
- Přístupová práva k datovým úložištím a datovým položkám přistupovaným prostřednictvím aplikací jsou povolena jen v rozsahu, který role resp. zaměstnanec nezbytně potřebuje ke své práci (princip „Need-to-know");
- Práva k užití systémových nástrojů a aplikací jsou povolena jen v rozsahu, který role potřebuje ke své činnosti (princip „Least privilege").

129) skryto

6.2 Řízení přístupu uživatelů

6.2.1 Registrace uživatele

Organizační zásady:

130) skryto

131) skryto

6.2.2 Správa uživatelských hesel

Organizační zásady:

132) skryto

133) skryto

134) skryto

6.2.3 Přezkoumání přístupových práv uživatelů

Organizační zásady:

135) Všechny účty s privilegovaným přístupem (účty administrátorů a správců systémů ICT) musí být evidovány mimo vlastní systém ICT včetně důvodů pro jejich vznik, identifikací osoby, se kterou jsou spojeny a dobou trvání.

136) skryto

6.3 Odpovědnosti uživatelů

6.3.1 Používání hesel

Organizační zásady:

137) Uživatel nesmí pracovat pod jinou, než jemu přidělenou, uživatelskou identitou (nesmí sdílet účet s jinou osobou).

138) Uživatel je povinen udržovat své heslo v tajnosti (zejména je zakázáno sdělovat heslo jiným osobám nebo je zaznamenávat na místech dostupných jiným osobám).

139) skryto

140) skryto

141) skryto

142) skryto

6.3.2 Neobsluhovaná uživatelská zařízení

Organizační zásady:

143) V případě, kdy uživatelé opouští pracoviště, musí zabránit přístupu k účtu / aplikaci.

6.4 Řízení přístupu k síti

6.4.1 Politika užívání síťových služeb

Organizační zásady:

144) skryto

6.4.2 Autentizace uživatele pro externí připojení

Technické zásady:

145) skryto

6.4.3 Princip oddělení v sítích

Technické zásady:

146) Služby systému ICT musí být dostupné pouze z nezbytných sítí a systémů. Zejména nesmí být interní služby systému ICT dostupné z externích sítí. Toto oddělení musí být provedeno na síťové úrovni minimálně pomocí filtrování komunikace pomocí aktivních prvků mezi sítěmi.

6.4.4 Řízení síťových spojení

Technické zásady:

147) Anonymní přístup z externích sítí do systému ICT musí být ukončen ve vyhrazené síti (např. DMZ).

6.5 Řízení přístupu k operačnímu systému

6.5.1 Bezpečné postupy přihlášení

Technické zásady:

148) skryto

149) skryto

6.5.2 Identifikace a autentizace uživatelů

Technické zásady:

150) skryto

151) skryto

152) skryto

153) skryto

6.5.3 Systém správy hesel

Technické zásady:

154) skryto

155) skryto

6.5.4 Časové omezení relace

Technické zásady:

156) skryto

6.6 Řízení přístupu k aplikacím a informacím

6.6.1 Omezení přístupu k informacím

Organizační zásady:

157) Omezení přístupu musí být v souladu s pravidly přístupu stanovenými právními předpisy. Za soulad odpovídá vlastník informací. Zejména musí být prosazeno

a) dodržování povinnosti při zpracování osobních údajů stanovené zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, za použití zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění pozdějších předpisů;

b) dodržování dalších zákonů vyžadujících řízení přístupu.

Technické zásady:

158) skryto

6.7 Mobilní výpočetní zařízení a práce na dálku

6.7.1 Mobilní výpočetní zařízení a sdělovací technika

Technické zásady:

159) skryto

6.7.2 Práce na dálku

Technické zásady:

160) Justiční složka schválí aktivity práce na dálku pouze tehdy, jestliže jsou splněny odpovídající bezpečnostní požadavky a jsou zavedena opatření, jež jsou v souladu s Politikou BICT. Musí být zavedeny postupy pro vzdálený přístup.

161) Na vzdáleném pracovišti musí být zajištěna vhodná ochrana například proti odcizení zařízení a nosičů informací, neautorizovanému vyzrazení informací, neautorizovanému vzdálenému přístupu k vnitřním systémům justiční složky nebo zneužití prostředků. Vzdálený přístup musí být schvalován vedoucími zaměstnanci.

162) Pro vzdálený přístup musí být přijata následující opatření:

a) na zajištění fyzické bezpečnosti pracoviště a práce na dálku včetně fyzického zabezpečení budovy a místního prostředí, viz kapitola 6.7.1;

b) na zajištění komunikační bezpečnosti, zahrnující potřeby vzdáleného přístupu k interním systémům justiční složky, důvěrnost informací, ke kterým je přistupováno a které jsou přenášeny komunikačními linkami, i důležitost a kritičnost interního systému;

c) proti neautorizovanému přístupu k informacím nebo zdrojům ze strany ostatních lidí užívajících místnosti, například rodina a přátelé;

d) proti hrozbám plynoucím z možného používání domácích sítí a požadavky nebo omezení na konfiguraci bezdrátových síťových služeb;

e) na zajištění antivirové ochrany a proti útoku ze sítě;

f) k monitorování a auditu bezpečnosti;

g) ke zrušení oprávnění, přístupových práv a vrácení zařízení při zániku povolení pro vzdálený přístup (viz 24)).

163) Pro vzdálený přístup musí být zváženy, uplatněny a kontrolovány následující požadavky:

a) určení povoleného druhu práce, pracovní doby, informací, které mohou být na zařízení uchovávány, a interních systémů a služeb resortu a justiční složky, ke kterým bude mít daná osoba při práci na dálku přístup;

b) zajištění vhodných metod pro bezpečný vzdálený přístup;

c) zálohovací postupy a postupy zajištění kontinuity činností justiční složky.

7 NÁKUP, VÝVOJ A ÚDRŽBA SYSTÉMŮ ICT

7.1 Bezpečnostní požadavky systémů

7.1.1 Analýza a specifikace bezpečnostních požadavků

Organizační zásady:

164) Součástí zadání vývoje nebo implementace části nebo celého systému ICT, IS a aplikace, musí být relevantní bezpečnostní požadavky uvedené v této politice BICT.

7.2 Správné zpracování v aplikacích

7.2.1 Validace vstupních dat

Technické zásady:

165) Musí být ověřena správnost všech vstupujících dat (pokud je tato kontrola možná).

166) V případě citlivých nebo nevratných operací musí být k jejich provedení vyžádáno speciální potvrzení od uživatele.

167) Maximum informací musí být doplňováno automaticky bez nutnosti zásahu uživatele.

7.2.2 Kontrola vnitřního zpracování

Technické zásady:

168) Pro detekci poškození informací vzniklého chybami při zpracování nebo úmyslnými zásahy do dokumentů, archiválií, databází a dalších úložišť kritických systémů ICT musí existovat a být provozovány nástroje k zajištění integrity. Kontrola integrity musí probíhat v pravidelných intervalech, které musí být kratší než období pokryté pravidelnými zálohami.

7.3 Kryptografická opatření

Kryptografická opatření jsou používána v případech, kdy má být zajištěna důvěrnost (ochrana uložených nebo přenášených důvěrných nebo kritických informací), integrita/autentičnost (digitální podpisy nebo autentizační kódy na ochranu autentičnosti a integrity uložených nebo přenášených důvěrných a kritických informací) a nepopiratelnost (získání důkazu o tom, zda událost nebo činnost nastala).

7.3.1 Politika pro použití kryptografických opatření

Organizační zásady:

169) V systému ICT mohou být použity pouze schválené kryptografické algoritmy se schválenými parametry (např. síla klíče) a doba jejich používání. Schválené algoritmy musí být dokumentovány v podobě formálního řízeného dokumentu, který podléhá změnovému řízení.

170) skryto

171) skryto

Technické zásady:

172) Kryptografické klíče musí být po celou dobu jejich existence chráněny a nikdy nesmí být uloženy nebo přenášeny v otevřeném tvaru. Alternativně mohou být v otevřeném tvaru uloženy v trezoru s řízeným a sledovaným přístupem.

173) skryto

174) Kryptografické klíče (konkrétně soukromé klíče) nesmí být archivovány. Jejich ničení musí probíhat protokolárně včetně zničení všech jejich záloh.

175) V případě neexistence seznamu schválených algoritmů jsou za schválené považovány následující algoritmy (nebo jejich kombinace):

Tab. 1 Schválené kryptografické algoritmy

Algoritmus	Klíče	Doba používání	Poznámka
SHA1		do roku 2012	Pouze pro jednorázové ověření integrity/podpisu (nebude se dlouhodobě ukládat) nebo pro zpracování hesel
SHA-224 SHA-256 SHA-384 SHA-512		do roku 2025	
RC4 Triple DES	max. 2 roky	do roku 2015	
AES	max. 2 roky	do roku 2030	
RSA	max. 2 roky velikost klíče min. 2048 bitů	do roku 2030	U podpisu je nutné zohlednit i vlastnosti hash funkce
ECC	max. 2 roky pro velikost tělesa Fq, musí $q \geq 2^{224}$	do roku 2030	U podpisu je nutné zohlednit i vlastnosti hash funkce

7.3.2 Správa klíčů

Organizační zásady:

176) skryto

177) Postupy pro přístup ke klíčům, stejně jako pro jejich vytvoření, používání a stažení z oběhu nebo zničení musí existovat ve formě formálního řízeného dokumentu, který podléhá změnovému řízení.

Technické zásady:

178) skryto

179) skryto

7.4 Bezpečnost systémových souborů

7.4.1 Správa provozního programového vybavení

Organizační zásady:

180) skryto

7.4.2 Ochrana testovacích údajů

Organizační zásady:

181) skryto

182) skryto

7.5 Bezpečnost procesů vývoje a podpory

Organizační zásady:

183) Musí být zaveden formální postup pro řízení změn, který musí minimálně zajistit:

a) Požadavek na změny bude vznesen pouze oprávněnými uživateli;

b) Bude udržován auditní záznam všech požadavků na změnu;

c) Před zahájením prací dojde k formálnímu odsouhlasení detailního návrhu, zahrnujícího

- určení veškerého programového vybavení, informací, databázových entit a technického vybavení, které vyžadují změny nebo doplnění,
- popis změn všech dotčených komponent,
- popis dopadů změn na bezpečnost a integritu systému;

d) Je zajištěna včasná aktualizace dokumentace, provozních a uživatelských postupů, seznamu testů a kontrol;

e) Je zajištěno vedení archivu změn programového vybavení a dokumentace;

f) Dojde k ověření funkčnosti v testovacím prostředí;

g) Budou existovat záložní postupy pro případ selhání v průběhu realizace změny v provozním prostředí;

h) Bude zajištěna možnost vhodné volby doby realizace, aby nedošlo k narušení provozu;

i) Realizace změny v provozním prostředí bude podmíněna souhlasem vlastníků informací a osob odpovědných za provoz a užití dotčených systémů ICT.

184) V případě změny operačního systému musí být přezkoumány a otestovány kritické aplikace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost informačních systémů.

185) Modifikace programových balíků musí být omezeny pouze na nezbytné změny, veškeré prováděné změny musí být řízeny.

7.6 Řízení technických zranitelností

7.6.1 Řízení, správa a kontrola technických zranitelností

Organizační zásady:

186) Musí být sledovány zranitelnosti systémů ICT a jejich komponent. Zjištěná zranitelnost systému je důvěrnou informací.

187) Zranitelnosti, které mohou být využity hrozbou, musí být opraveny, nebo musí být přijata dodatečná opatření.

188) skryto

189) skryto

8 ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Organizační zásady:

190) skryto

191) skryto

192) Vzniklé bezpečnostní události a zjištěné zranitelnosti systémů ICT musí být evidovány způsobem umožňujícím jejich následné vyhodnocení.

193) Součástí zvládání bezpečnostních událostí musí být i vyšetření příčiny, zaznamenání průběhu události, určení nápravných opatření a určení odpovědnosti za jejich realizaci.

194) skryto

9 ŘÍZENÍ KONTINUITY ČINNOSTÍ

9.1 Řízení kontinuity činností z hlediska bezpečnosti informací v systémech ICT

Organizační zásady:

195) Na základě posouzení rizik musí resort spravedlnosti resp. justiční složka rozhodnout, jestli je potřeba vytvářet plán reakce na havárii a obnovy po havárii. Dále určit, pro které služby a/nebo systémy ICT, musí být plán reakce součástí širšího zajištění kontinuity činností resortu spravedlnosti resp. justiční složky. Rozhodnutí musí být dokumentováno. Pokud budou plány vytvořeny, musí obsahovat

a) účel a předmět plánu,

b) situace pro aktivaci plánu,

c) role a odpovědnosti,

d) úkoly a činnosti v případě vyvolání plánu,

e) způsob a rozsah informování o aktivaci a vykonávání plánu,

f) vlastníka a správce plánu,

g) uložení plánu a jeho kopií tak, aby nebyly zničeny v případě havárie v hlavní lokalitě,

h) aktuální kontakty nutné k vykonávání plánu, včetně kontaktů na dodavatele a servisní organizace.

196) Vytvořené plány pro zvládání událostí s dopadem na činnost justiční složky musí být pravidelně testovány a aktualizovány.

10 SOULAD S POŽADAVKY

10.1 Soulad s právními normami

Organizační zásady:

197) Pro všechny kritické systémy ICT musí být jednoznačně určeny, dokumentovány a udržovány aktuální veškeré relevantní zákonné, regulatorní a smluvní požadavky a způsob, jakým je justiční složka dodržuje.

198) Součástí aktualizace analýzy rizik (viz kapitola 1.1 „Interní organizace") musí být i posouzení revizí zákonů, které mají vztah k provozovanému systému ICT a zejména dopadů, které vyplývají z porušení ustanovení těchto zákonů.

10.2 Soulad s bezpečnostními politikami, normami a technická shoda

10.2.1 Shoda s bezpečnostními politikami a normami

Organizační zásady:

199) Minimálně jedenkrát za rok musí být provedena kontrola technické shody. O provedené kontrole musí být vytvořen písemný záznam obsahující jméno kontrolující osoby, kontrolované skutečnosti a výsledky kontroly.

a) Kontrola technické shody musí ověřit, zda vlastnosti a nastavení systémů ICT jsou v souladu s normami, bezpečnostními politikami a návaznými předpisy;

b) Pro systémy přístupné uživatelům mimo síť justiční složky jiným způsobem, než s využitím VPN, musí být proveden automatizovaný nebo manuální test zranitelností rozhraní.

200) Součástí kontroly technické shody musí být i kontrola odstranění nálezů z minulé kontroly.

201) Záznam o kontrole technické shody je podkladem pro odstranění nalezených nedostatků.

10.3 Hlediska nezávislé kontroly dodržování Politiky BICT

Organizační zásady:

202) skryto

203) skryto

204) skryto

205) skryto

206) skryto

207) skryto

10.4 Výjimky

208) skryto

11 SEZNAM POUŽITÝCH ZKRATEK

Tab. 2 Seznam použitých zkratek

Zkratka	Význam
BICT	Bezpečnost informací v systémech ICT
DMZ	Demilitarized zone - fyzická nebo logická subsíť, která obsahuje a vystavuje externí služby organizace (justiční složky) do vnější nedůvěryhodné sítě, zpravidla do veřejného Internetu.
DVZ	Důvěryhodná výpočetní základna (infrastruktura IT resortu spravedlnosti)
ICT, IT	informační a komunikační technologie, informační technologie (v nejširším slova smyslu zahrnuje hardware, software, automatizované systémy zpracování dat, apod.)
IPS	Intrusion Prevention System, také znám jako Intrusion Detection and Prevention System (IDPS), jsou zařízení pro zajištění síťové bezpečnosti, které monitorují síťové a systémové aktivity a vyhledávají zlomyslné (malicious) aktivity, logují je, pokoušejí se je blokovat/zastavit a hlásí je.
IS	Informační systém - pro účely tohoto dokumentu se „Informačním systémem" rozumí zpracovaný záměr, rozvrh nebo plán budoucího zpracování dat nebo již provozovaného informačního systému. Pod toto označení se zahrnuje také samostatná aplikace, která nebyla (doposud) zařazena do určitého IS.
ISMS	Systém managementu bezpečnosti informací (Information security management systems)
ISVS	informační systémy veřejné správy (viz Zákon č.365/2000 Sb.)
MSp	Česká republika - Ministerstva spravedlnosti
UPS	Nepřerušitelný zdroj energie (Uninterruptible Power Supply/Source) je zařízení nebo systém, který zajišťuje souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta.

12 PŘÍLOHY POLITIKY BEZPEČNOSTI INFORMACÍ V ICT

Příloha č. 1 Seznam právních norem a literatury k bezpečnosti informací v systémech ICT

13 ÚČINNOST POLITIKY BEZPEČNOSTI INFORMACÍ V ICT

Tato politika bezpečnosti informací v ICT nabývá účinnosti dne 1. 1. 2013

V Praze dne 21. 12. 2012

Ing. Petr Koucký
ředitel odboru informatiky

Příloha PS6 – Seznam referencí politiky bezpečnosti ICT

Smlouva o Poskytování datových služeb KIVS v resortu justice

Tento seznam je přílohou dokumentu „Politika bezpečnosti informací v ICT resortu spravedlnosti" (dále jen „Politika BICT") vydaného Odborem informatiky MSp.

Seznam je uspořádán dle roku vydání Sb. a následně dle čísla předpisu.

[1] Zákon č. 563/1991 Sb., o účetnictví, s vyznačením změn s účinností od 1. ledna 2010

[2] Vyhláška č. 37/1992 Sb., o jednacím řádu pro okresní a krajské soudy

[3] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

[4] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[5] Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

[6] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (viz také Nařízení vlády č. 495/2004 Sb.)

[7] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů

[8] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů

[9] Zákon č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích)

[10] Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu

[11] Vyhláška č. 496/2004 Sb., o elektronických podatelnách

[12] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších zákonů (viz také vyhlášky č.645/2004 Sb. a č.191/2009 Sb.)

[13] Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě (k zákonu č. 499/2004 Sb.)

[14] Vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby (k zákonu č. 499/2004 Sb.)

[15] Zákon č. 500/2004 Sb., správní řád

[16] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

[17] Vyhláška č.523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor (k zák. č. 412/2005 Sb.)

[18] Usnesení vlády ČR č.1340 ze dne 19. října 2005, Národní strategie informační bezpečnosti České republiky (NSIB ČR)

[19] Zákon č. 81/2006 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony

[20] Vyhláška č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup

[21] Vyhláška č. 469/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému o datových prvcích a o postupech Ministerstva informatiky a jiných orgánů veřejné správy při vedení, zápisu a vyhlašování datových prvků v informačním systému o datových prvcích (vyhláška o informačním systému o datových prvcích)

[22] Vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy (vyhláška o informačním systému o informačních systémech veřejné správy)

[23] Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

[24] Komentář MVČR k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality ISVS

[25] Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní

[26] Vyhláška č. 53/2007 Sb. o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní) (k zákonu č. 365/2000 Sb.)

[27] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

[28] Zákon č. 40/2009 Sb., trestní zákoník

[29] Vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby

[30] Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů

[31] Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

[32] Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby, VMV částka 76/2009 (část II)

[33] ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, říjen 2006.
(je českou verzí mezinárodní normy ISO/IEC 27001:2005)

[34] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management (původně BS ISO/IEC 17799:2005; RAC 2006 - Překlad a interpretace pro české prostředí)

[35] ČSN BS 25999-1 - Management kontinuity činností organizace - část 1: Soubor zásad

[36] NIST 800-64, Information Security, Security Considerations in the System Development Life Cycle, NIST Special Publication 800-64 Revision 2, October 2008

[37] Zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky

Poznámky:

1.) Pro oblast „Elektronické trestní řízení" (URL=http://www.isvs.cz/?zobraz=kategorie-7) je vyžadováno dodržení požadavků, které stanovuje „Standard ISVS 005/02.01 pro náležitosti životního cyklu informačního systému" a starší normy ČSN ISO/IEC 12207 (369784) Informační technologie - Procesy v životním cyklu softwaru (z roku 1997).

Příloha PS8 – Pověření osoby zastupující Poskytovatele

Smlouva o Poskytování datových služeb KIVS v resortu justice

T-Mobile

POVĚŘENÍ

Společnost T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 149 00, IČ 64949681, (dále jen „Společnost") jednající prostřednictvím představenstva Společnosti tímto **p o v ě ř u j e** níže uvedeného zaměstnance:

[redacted]
nar. [redacted]

aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí se smlouvami o poskytování služeb elektronických komunikací služeb a o prodeji komunikačního zařízení a jejich příslušenství firemním zákazníkům a se smlouvami o zprostředkování anebo spolupráci při uzavírání uvedených smluv; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony, které souvisí se smlouvami, které upravují komplexní řešení ProfiNet, prodej jakýchkoli nehlasových služeb a služeb s přidanou hodnotou; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony, které souvisí se smlouvami o poskytování ICT řešení, jež upravují podmínky pronájmu komunikačních zařízení a souvisejícího vybavení vč. požadované softwarové podpory; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony podle zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky.

Pověřený zaměstnanec v takto vymezeném rozsahu a po dobu pracovního poměru ve Společnosti jedná jménem Společnosti samostatně a je oprávněn v uvedeném rozsahu podepisovat příslušné písemnosti. Zmocněnec není oprávněn zmocnit ani jinak pověřit jinou osobu, aby místo něj jednala za Společnost. Pověřený zaměstnanec dále není oprávněn jakýkoli majetek Společnosti převádět či zatěžovat právy třetích osob.

Podepisování pověřeného zaměstnance se děje tak, že k napsané nebo vytištěné obchodní firmě společnosti či otisku razítka společnosti připojí pověřený zaměstnanec svůj podpis.

V Praze dne 25. března 2011

[redacted]
Dipl. Ing. Roland Mahler
předseda představenstva

[redacted]
Albert Pott
člen představenstva

Toto pověření přijímám:

[redacted]
Ing. Libor Komárek