Politika bezpečnosti informací v ICT resortu spravedlnosti

č. j. 142/2012-OI-SP/1

vydaná na základě Instrukce Ministerstva spravedlnosti ze dne 30. 05. 2012, č. j. 24/2012-OI-SP, o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti

0 ÚVOD

Tato „Politika bezpečnosti informací v ICT resortu spravedlnosti“ (dále jen „Politika BICT“) byla vytvořena a schválena Odborem informatiky MSp, publikována a dána na vědomí všem pracovníkům oblasti informatiky a oprávněným třetím stranám na základě Instrukce Ministra spravedlnosti ze dne 30. 05. 2012, č. j. 24/2012-OI-SP, o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti (dále jen „Instrukce BICT).

0.1 Přehled použitých pojmů

Pro účely tohoto dokumentu se rozumí:

Aktivy systémů ICT veškeré informace, procesy, hardware (HW), software (SW), nosiče informací a dokumentace systémů ICT justiční složky a resortu spravedlnosti, které jsou důležité pro provoz těchto systémů, plnění úkolů justiční složky, právní shody a dobrého jména organizace.

Systémy ICT / Systémy informačních a komunikačních technologií resortu spravedlnosti veškeré počítačové sítě resp. informační systémy justičních složek, infrastruktura výpočetní techniky, výpočetní technika včetně mobilních zařízení a přídavných zařízení a nosiče informací. Systémy ICT dále zahrnují správu, bezpečnostní správu a práci uživatele, projektovou a provozní dokumentaci, základní a aplikační software a požadavky na jejich pořízení, instalaci, konfiguraci, provoz, ukončení provozu a zničení aktiv systémů ICT.

Kritické systémy ICT ty systémy, které za pomocí ICT realizují tzv. „**kritické činnosti justičních složek**“. Kritickými jsou ty činnosti, které mají zvýšené požadavky na zajištění bezpečnosti a/nebo mají být justičními složkami plněny i v případě vzniku a trvání havárií a mimořádných událostí. Politika BICT u vybraných bezpečnostních opatření nastavuje kritickým systémům ICT přísnější limity než ostatním systémům ICT.

Formálně řízeným dokumentem dokument, pro který je stanoven subjekt odpovědný za jeho správu, pravidelnou revizi a aktualizaci. Musí být stanovena pravidla pro změnová řízení, schválení aktualizovaného dokumentu a pro jeho distribuci.

Centrálními komponentami systémů ICT aktiva systémů ICT, v nichž jsou soustředěny, výpočetní nebo přenosové kapacity a/nebo informace justiční složky nebo resortu spravedlnosti v takovém množství, že jejich narušení či zničení významně ohrozí plnění cílů bezpečnosti informací v prostředí ICT (§ 2 Instrukce BICT). Není-li v systémové dokumentaci stanoveno jinak, musí být zvýšená opatření na jejich ochranu realizována u kritických systémů od úrovně organizace a u ostatních systémů od úrovně kraje.

Vlastníkem aktiva je osoba (obvykle zaměstnanec) která rozhoduje o používání aktiva (rozsahu, způsobu, postupech…) a odpovídá za to to, že používání aktiva je v souladu s cíli organizace.

Vlastníkem informace je vedoucí odborného útvaru, který má zákonnou, resortní nebo jinou gesci nad obsahem a ochranou údajů. Má působnost na údaje a data, jichž užití je upraveno zákonem, resortním nebo jiným předpisem.

Zaměstnancem všechny osoby v pracovně právním vztahu s ministerstvem spravedlnosti nebo justiční složkou, dále soudci, včetně soudců dočasně přidělených, osoby vykonávající na justiční složce praxi či stáž a osoby činné na justiční složce na základě dohod konaných mimo pracovní poměr a osoby ve služebním poměru ve Vězeňské službě.

Justiční složkou Ministerstvo spravedlnosti České republiky, soudy, státní zastupitelství, Vězeňská služba České republiky, zotavovny Vězeňské služby České republiky, Probační a mediační služba České republiky a dalších organizací řízených ministerstvem.

1 ORGANIZACE BEZPEČNOSTI

1.1 Interní organizace

1) Odpovědnost za dodržování ustanovení této Politiky BICT mají všichni zaměstnanci a smluvní partneři justičních složek.

1.2 Externí subjekty

Organizační zásady:

2) Veškeré způsoby přístupu externích subjektů k systémům ICT a k informacím (včetně vzdáleného přístupu) musí být schváleny.

   - Předtím, než je externím subjektům povolen přístup k systémům ICT a k informacím, musí být identifikována rizika a implementována opatření na jejich pokrytí.

3) Outsourcing provozu systémů ICT, tedy převod odpovědnosti za provoz systémů ICT nebo jejich části a poskytování služeb systémů ICT na jiné osoby než zaměstnance justičních složek, nesmí snížit úroveň bezpečnosti provozu systémů ICT. Bezpečnostní požadavky musí být součástí smlouvy upravující tento vztah.

4) Externí subjekty (třetí strany, smluvní dodavatelé a jejich zaměstnanci) se mohou podílet na zajištění kontinuity provozu systémů ICT při mimořádných událostech a haváriích a na vytváření podmínek pro toto zajištění kontinuity provozu za běžného provozu systémů ICT. Tento vztah musí být upraven písemnou formou, která musí zajistit potřebnou úroveň bezpečnosti systémů ICT, zejména dodržování této Politiky BICT, nadřízených bezpečnostních politik a předpisů justičních složek k zajištění bezpečnosti.

5) Externí subjekty (třetí strany, smluvní dodavatelé a jejich zaměstnanci) se mohou podílet na vývoji a údržbě systémů ICT. Tento vztah musí být upraven písemnou smlouvou, jejíž ustanovení musí zajistit potřebnou úroveň bezpečnosti systémů ICT, zejména dodržování této Politiky BICT, nadřízených bezpečnostních politik a dalších předpisů justičních složek k zajištění bezpečnosti.

6) Odpovědnost za zapracování požadavků Politiky BICT do smlouvy je uvedena v kapitole 5.2 „Řízení dodávek a služeb třetích stran“.

2 ŘÍZENÍ AKTIV

2.1 Odpovědnost za aktiva

Organizační zásady:

7) Aktiva spojená se systémy ICT musí být evidována. Evidence aktiv pomáhá zajistit udržování efektivní ochrany. Proces vytvoření seznamu aktiv je nezbytným předpokladem pro řízení rizik.

8) Veškeré informace a aktiva související se systémy ICT musí mít určeného vlastníka. Vlastnictví se přiděluje na HW komponenty ICT, nosiče informací, procesy, přesně vymezené soubory činností, aplikace, přesně vymezené soubory dat, apod.

   - Běžné úkoly (např. každodenní dohled nad aktivy nebo zpracování dat) mohou být delegovány, odpovědnost však vždy zůstává na vlastníkovi aktiva.

9) Musí existovat formálně řízený dokument, který určuje pravidla a doporučení pro použití aktiv a elektronickou komunikaci (včetně pravidel pro použití elektronické pošty a internetu, doporučení pro použití mobilních zařízení, zejména mimo areál justiční složky, a další). Zaměstnanci, smluvní strany a uživatelé třetích stran (externí subjekty), kteří používají nebo mají přístup k aktivům resortu spravedlnosti nebo justiční složky, musí znát pravidla omezující použití informací, zdrojů, a aktiv souvisejících se systémy ICT. Nesou odpovědnost za použití jakýchkoli zdrojů pro zpracování informací.

2.2 Důvěrnost informací

Organizační zásady:

10) Informace mají být dostupné jen tomu, kdo je „**potřebuje znát ke své práci**“ a je k tomu „**oprávněn**“. Je třeba zajistit přiměřenou úroveň ochrany před neoprávněným přístupem, prozrazením nebo zveřejněním informací. Informace musí být chráněny způsobem přiměřeným jejich významu, zákonným požadavkům na jejich ochranu a požadavkům resortní politiky bezpečnosti informací.

11) Veškeré informace, se kterými přicházejí zaměstnanci při používání informačních a komunikačních technologií rezortu justice do styku, jsou považovány za důvěrné. Povinností zaměstnanců je proto tyto informace chránit před zneužitím, ztrátou nebo poškozením.

    a) Zaměstnanci nesměji pořizovat kopie a zpracovávat jakékoli informace složky resortu spravedlnosti prostředky výpočetní techniky, které nejsou ve vlastnictví složky resortu spravedlnosti. Ve výjimečných a opodstatněných případech může pořizování kopií, zpracování informací a jejich využití povolit přímý nadřízený vedoucí dotčeného zaměstnance. Každá taková výjimka musí být zachycena písemně, podepsaná zaměstnancem i jeho nadřízeným vedoucím zaměstnancem a evidována nejméně po dobu 1 roku.

3 BEZPEČNOST LIDSKÝCH ZDROJŮ

3.1 Před vznikem a před změnou pracovního/smluvního vztahu (pracovního zařazení)

Organizační zásady:

12) Všichni uchazeči o pozici s nadstandardními právy přístupu k systémům ICT a k uloženým datům, zejména administrátoři a správci IS, musí být prověření. Jedná se např. o ověření předchozí pracovní historie.

13) Prověřování externích subjektů (dodavatelů nebo jejich zaměstnanců) s nadstandardními právy musí zajistit úroveň prověření obdobnou úrovni prověřování interních zaměstnanců.

14) Odpovědnost za bezpečnost informací a povinnost mlčenlivosti musí být formálně přijata před umožněním přístupu k IS. Písemný závazek se ukládá a archivuje. Tento závazek se upravuje

    a) ve smlouvě se zaměstnancem nebo

    b) ve smlouvě s externím subjektem nebo

    c) v závazku osoby oprávněné provádět činnost na základě pracovního/smluvního vztahu nespadajícího pod personální odbor/oddělení (externisté, poradci, stážisté).

15) Smlouvy se zaměstnanci musí obsahovat popis kroků (nebo příslušný odkaz), které budou následovat při nedodržení bezpečnostních požadavků.

16) Justiční složka musí stanovit, a to pokud možno určením funkčního zařazení nebo pracovních pozic, které osoby vykonávají následující činnosti:

a) Oznamování termínu přijetí/změny osoby do pracovního vztahu, předpokládaného data ukončení pracovního vztahu a rozsahu práv pro přístup k systémům a aplikacím vyplývající z funkčního zařazení příslušnému informatikovi bez zbytečného odkladu.

b) Oznamování termínu zahájení, změny a ukončení plnění smluvního vztahu s externím subjektem a rozsahu práv pro přístup k systémům a aplikacím vyplývající ze smlouvy příslušnému informatikovi bez zbytečného odkladu.

c) Sledování termínu zahájení/změny pracovní činnosti zaměstnanců a externích subjektů, které jsou oprávněny provádět činnost na základě pracovních a smluvních vztahů nespadajících pod personální odbor/oddělení (externisté, poradci, stážisté), a rozsahu práv pro přístup k systémům ICT, službám, aplikacím a datům.

- Pro každou takovou osobu a externí subjekt musí být určen odpovědný vedoucí zaměstnanec, který odpovídá za stanovení rozsahu jejích přístupových práv.
- Všechny případy, které nejsou nastaveny písemnou smlouvou na dobu neurčitou, musí mít nastavenu dobu exspirace účtu resp. přístupových práv na datum dle smlouvy resp. maximálně na 6 měsíců, není-li datum ukončení stanoveno;
- Přístupy, které mají pokračovat za předem stanovenou dobou exspirace, mohou být prodlouženy pouze postupem dle písmene a), b) a c).

d) Oznamování změn potřebného rozsahu přístupu zaměstnance nebo externího subjektu k aplikacím a datům bez zbytečného odkladu příslušnému informatikovi.

Informatik složky zřizuje účty a rozsah přístupu oprávněných osob k systémům ICT, službám, aplikacím a datům výhradně na základě požadavků oprávněných osob a tyto požadavky eviduje.

3.2 Během pracovního/smluvního vztahu

3.2.1 Odpovědnosti vedoucích zaměstnanců

Organizační zásady:

17) Vedoucí zaměstnanci jsou v rámci své působnosti odpovědní:

a) za zajištění dodržování bezpečnostních opatření stanovených touto Politikou BICT a platnými interními směrnicemi zaměstnanci, smluvními a třetími stranami;

b) za zajištění toho, že zaměstnanci, smluvní a třetí strany jsou dostatečně informovány o svých rolích a odpovědnostech za bezpečnost informací předtím než je jim udělen přístup k informacím, informačním systémům a aplikacím a přístup do prostor chráněných opatřeními fyzické bezpečnosti (viz kapitola 4);

c) za zajištění toho, že zaměstnanci, smluvní a třetí strany obdrží předpisy k provozu a bezpečnosti systémů ICT a/nebo metodické pokyny stanovující bezpečnostní očekávání spojené s rolí, kterou vykonávají.

18) Změny v rozsahu práv pro přístup k systémům ICT, službám, aplikacím a datům mohou být prováděny jen postupem dle kapitoly 3.1.

3.2.2 Informovanost, vzdělávání a školení v oblasti bezpečnosti informací

Organizační zásady:

19) Všem osobám přistupujícím k informacím a informačním systémům justičních složek musí být poskytnuty informace o požadavcích a postupech při zajišťování bezpečnosti informací.

20) Musí existovat předpisy k provozu a bezpečnosti systémů ICT a/nebo metodické pokyny pro práci s aplikacemi pro všechny role přistupující k systému ICT (tedy pro interní uživatele i pro externí uživatele).

21) Musí existovat plán školení práce se systémy ICT v závislosti na čase (nástup uživatele, pravidelné intervaly), komplikovanosti a funkcionalitě rozhraní systému ICT. Školení musí být prováděna podle plánu zohledňujícího následující body:

    a) Všechny osoby přistupující k systémům ICT musí být prokazatelně seznámeny, diferencovaně podle svých rolí při užívání a správě systémů ICT, s předpisy k provozu a bezpečnosti systémů ICT a s metodickými pokyny pro práci s aplikacemi;

    b) Školení resp. seznámení se provádí vždy při nástupu nové osoby do rolí spojených se systémy ICT nebo při jakýchkoliv změnách systémů ovlivňujících bezpečnost, minimálně však jedenkrát za 3 roky;

    c) Školící resp. seznamovací aktivity musí zahrnovat

        - vysvětlení „PROČ“ je nutná spolupráce ze strany uživatelů, „JAKÁ“ spolupráce se očekává a v „JAKÉM“ rozsahu,
        - upozornění na povinnost mlčenlivosti i po ukončení pracovního/smluvního vztahu na jehož základě byl osobě udělen přístup (viz kapitola 3.1),
        - seznámení se sankcemi za nedodržování směrnic a provozní dokumentace systémů ICT (viz kapitola 3.2.3 „Důsledky narušení bezpečnosti“ a kapitola 8 „Zvládání bezpečnostních incidentů“),
        - seznámení s postupy pro provoz a zajištění činnosti systému v době výskytu mimořádné události,
        - seznámení s postupy pro hlášení bezpečnostních incidentů,
        - seznámení s postupy pro obnovu po havárii, zajištění kontinuity činností justiční složky a nácvik reakce na nestandardní situace;

    d) Ze školení je pořízen písemný záznam obsahující osnovu školení, podpisy školitele a účastníků školení. Záznam o školení formou e-learning obsahuje podpis absolventa školení.

22) Odpovědnost za naplnění bezpečnostních požadavků této kapitoly má přímý nadřízený osoby, které se školení týká.

3.2.3 Důsledky narušení bezpečnosti

Organizační zásady:

23) Musí existovat formalizované disciplinární řízení vůči pracovníkům, kteří se dopustili narušení bezpečnosti.

24) Případy narušení bezpečnosti a nápravná opatření musí být po anonymizaci interně prezentována v rámci justiční složky (jako preventivní opatření).

3.3 Ukončení nebo změna pracovního/smluvního vztahu

3.3.1 Odpovědnosti při ukončení pracovního vztahu

Organizační zásady:

25) Musí být zavedeny procesy pro odebrání/změnu práv a navrácení zapůjčených prostředků v případě ukončení nebo změny pracovního/smluvního vztahu; tyto procesy

    a) nesmí být závislé na osobě, které se změna týká;

b) musí být dokumentovány v podobě formálních řízených dokumentů, podléhajících změnovému řízení;

c) musí zahrnovat osoby, veškeré zaměstnanecké a smluvní vztahy, při kterých mohl být účet přidělen (viz kapitola 3.1 odstavec 16).

26) Odpovědnost za ukončení pracovního/smluvního vztahu (změny pozice, pracovního vztahu v rámci justiční složky apod.) v souladu s definovanými procesy, a to včetně provedení všech nezbytných změn, má přímý nadřízený osoby, které se dané ukončení týká.

a) Vedoucí zaměstnanec (přímý nadřízený osoby, které se ukončení týká) je odpovědný

- za oznámení změny pracovního vztahu vedoucímu personálního odboru/oddělení,
- za oznámení změny smluvního vztahu dotčeným zaměstnancům s požadavkem na odebrání/změnu přístupových práv;

b) Vedoucí personálního odboru/oddělení je odpovědný za oznámení požadavku na odebrání/změnu přístupových práv a navrácení zapůjčených prostředků a předání agend vedoucímu informatikovi složky a případným dalším subjektům justiční složky.

3.3.2 Navrácení zapůjčených prostředků a předání agend

Organizační zásady:

27) Musí být zajištěno, aby zaměstnanci, pracovníci smluvních a třetích stran při ukončení pracovního vztahu odevzdali příslušnému subjektu veškeré jim svěřené prostředky, které jsou majetkem justiční složky. Navrácení by mělo zahrnovat poskytnuté programové vybavení (instalační nosiče), dokumenty a vybavení, mobilní výpočetní prostředky, autentizační prostředky (karty pro vzdálený přístup), programová dokumentace a nosiče informací.

28) V případech, kdy zaměstnanci, smluvní nebo třetí strany mají agendy (informace a znalosti) důležité z hlediska stávajícího provozu pracoviště, řešených případů nebo justiční složky, musí být zajištěno jejich dokumentování a předání resp. navrácení.

3.3.3 Odebrání přístupových práv

Organizační zásady:

29) Při ukončení nebo změně pracovního/smluvního vztahu musí být příslušným stranám odejmuta nebo pozměněna přístupová práva k systémům ICT, službám a informacím. Mateřská/rodičovská dovolená se považuje za změnu pracovního zařazení.

30) Při ukončení pracovního/smluvního vztahu uživatele musí být zrušeny e-mailové adresy obsahující příjmení uživatele (a případně jméno) nebo jiný osobní identifikátor. Požadavek na zrušení se nevztahuje na e-maily, které ve svém názvu obsahují jen pracovní pozici, úřední místo nebo jiný neosobní identifikátor.

- Vedoucí personálního odboru/oddělení může uplatnit požadavek na zachování e-mailové adresy na určitou dobu u těch osob, které přestoupily k jiné složce resortu spravedlnosti.

31) O odebrání přístupových práv musí existovat písemný záznam včetně identifikace osoby, která odebrání provedla a osoby, která odebrání inicializovala.

32) Při rozvázání smluvního vztahu s třetí stranou je zaměstnanec odpovědný za tento smluvní vztah odpovědný za inicializaci procesu zrušení veškerých práv k systémům ICT, které tato třetí strana měla.

4 FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

4.1 Zabezpečené oblasti

4.1.1 Serverovny a centrální úložny dat

Technické zásady:

33) Prostory, kde jsou uloženy centrální komponenty systémů ICT, centrální zálohy a archivy (dále jen „centrální aktiva systémů ICT“), musí být:

a) chráněny před hrozbami vnějšího prostředí;

b) ohraničeny uzavřeným a jasně definovaným perimetrem bez existence slabých, snadno proniknutelných míst;

c) vybaveny elektronickým požárním systémem (EPS) a vhodným hasicím zařízením.

34) Pro prostory, kde jsou uložena centrální aktiva systémů ICT, musí být vypracován projekt fyzické bezpečnosti a provozní řád, který je jeho součástí. Součástí provozního řádu nebo obsahem samostatného dokumentu musí být pokyny k ochraně aktiv systémů ICT (dokumentů, nosičů informací, archiválií, technologií apod.) v situacích, kdy bezprostředně hrozí, že dojde k jejich prozrazení, zneužití, poškození nebo zničení.

35) Prostory, kde jsou uložena centrální aktiva systémů ICT, musí být chráněny mechanickými prostředky (bezpečnostní dveře a zámky, mříže) a napojeny na elektronický zabezpečovací systém (EZS) proti neoprávněnému vniknutí. Úroveň opatření musí odpovídat důležitosti informací zde umístěných a požadované úrovni dostupnosti informací a služeb systémů ICT.

Organizační zásady:

36) Přístup do prostor resp. úschovných objektů (trezorů apod.), kde jsou uložena centrální aktiva systémů ICT, smí mít pouze pracovníci v rolích, které potřebují přístup do těchto prostor k plnění svých pracovních povinností.

37) Vstup návštěv (osob bez samostatné možnosti přístupu, včetně pracovníků úklidu, údržby, dodavatelů apod.) do prostor, kde jsou uložena centrální aktiva systémů ICT, je možný pouze po schválení osobou určenou provozním řádem, a to pouze v doprovodu některého z pracovníků, který má povolen přístup podle předchozího odstavce.

38) Datum a čas příchodu a odchodu návštěv do/z prostor, kde jsou uložena centrální aktiva systémů ICT, včetně identifikace účastníků návštěvy a pracovníka, který je doprovázel, musí být zaznamenán a návštěvníci musí být pod stálým dohledem oprávněné osoby. Záznamy o vstupech musí být uchovány minimálně po dobu 1 roku.

39) Musí být určena osoba/role odpovídající za udržování seznamu osob, které mají povolen přístup k centrálním aktivům systémů ICT a mají k dispozici klíče, autentizační předměty, kódy EZS apod., a to včetně historie (již neplatných povolení).

40) Přístupová práva do prostor, kde jsou uložena centrální aktiva systémů ICT, musí být kontrolována minimálně jednou za 6 měsíců. O této kontrole musí být proveden záznam.

41) Prostory, kde jsou uložena centrální aktiva systémů ICT, při nepřítomnosti oprávněných osob, musí být fyzicky uzamčeny a, pokud je to možné, monitorovány EZS.

42) Na pracovištích, kde jsou uložena centrální aktiva systémů ICT, nesmí být ukládány hořlavé nebo jinak nebezpečné materiály (např. prázdné obaly od technického vybavení), je zakázáno zde jíst, pít a kouřit.

4.1.2 Kanceláře

Organizační zásady:

43) Systémy ICT, určené pro zpracování vnitřních agend justiční složky, a jejich části musí být umístěny v prostorách bez volného přístupu veřejnosti.

44) Kritické systémy ICT a jejich další aktiva, zejména evidované nosiče informací, musí být v době mimo přítomnost oprávněných osob umístěny a ukládány v souladu s provozním řádem, který je součástí projektu fyzické bezpečnosti.

4.2 Bezpečnost zařízení

4.2.1 Umístění zařízení a jeho ochrana

Organizační zásady:

45) Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup. Přitom je třeba zvažovat:

   a) minimalizaci nadbytečného přístupu do pracovních prostor;

   b) umístění prostředků pro zpracování a ukládání dat tak, aby bylo sníženo riziko možného odezírání informací;

   c) izolování aktiv, která vyžadují zvláštní ochranu, s cílem snížit rozsah požadované celkové ochrany;

   d) pravidla omezující jídlo, pití a kouření v blízkosti zařízení ICT;

   e) monitorování působení vnějšího prostředí (jako např. teploty a vlhkosti).

46) Všechny centrální komponenty systémů ICT musí být chráněny před selháním napájení.

47) V periodě stanovené provozní dokumentací systému ICT, nejdéle však jednou za 6 měsíců, musí být překontrolována zařízení napojená na generátor náhradního napájení nebo na UPS a zkontrolováno, zda je výkon generátoru a příkon UPS dostatečný (s ohledem na nárůst způsobený nově připojenými technologiemi).

Technické zásady:

48) Ve všech serverovnách systémů ICT musí být nasazena ochrana proti blesku na elektrickém vedení.

49) V prostorách s umístěnými komponentami kritických systému ICT musí být kontinuálně monitorována teplota; výstupy monitorování musí být pravidelně (min. 1x za 30 minut) sledovány.

50) Všechny centrální komponenty systémů ICT musí být

   - buď napojeny na UPS a generátor náhradního napájení s dobou náběhu menší než je doba provozu UPS. Generátor musí být pravidelně kontrolován a v případě delšího používání musí být zajištěno zásobování pohonnou hmotou
   - nebo napojeny na UPS a musí být nastaven řízený shutdown všech serverů.

51) Veškeré podpůrné služby jako elektřina, topení/ventilace a klimatizace musí být přiměřené systému, který podporují. Klimatizace musí být napojena na generátor náhradního napájení, pokud je použit.

4.2.2 Bezpečnost kabelových rozvodů

Technické zásady:

52) Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat a podporu informačních služeb, musí být chráněny před poškozením či odposlechem.

53) Kabely i zařízení centrálních komponent systémů ICT musí být zřetelně označeny a musí být udržován seznam propojení.

54) U kritických systémů ICT musí být zvážena další opatření:

   a) instalace pancéřového potrubí a zamčených místností nebo skříní;

   b) použití alternativního směrování nebo alternativních přenosových cest poskytujících přiměřenou bezpečnost;

   c) použití optických kabelů;

   d) použití stínění kabelů na ochranu před elektromagnetickým vyzařováním.

55) Aktivní prvky zajišťující komunikaci mezi centrálními komponentami systému ICT a koncovými zařízeními musí být umístěny v prostorách pod kontrolou justičních složek.

4.2.3 Údržba zařízení

Organizační zásady:

56) Komponenty systému ICT (zařízení) musí být v intervalech předepsaných výrobcem/dodavatelem kontrolovány pro zajištění jejich stálé dostupnosti a integrity (prováděna profylaxe).

   a) Zařízení musí být udržována a provozována v souladu s doporučeními dodavatele;

   b) Opravy a servis zařízení smí provádět pouze oprávněné osoby;

   c) O všech závadách nebo podezřelých chybách, o preventivních prohlídkách a opravách musí být pořízeny záznamy;

   d) V případech, kdy je údržba prováděna bez dohledu oprávněné osoby, musí být ze zařízení odstraněny veškeré informace.

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 6.7) 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 5.7.2).

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 6.7), 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) Provozní postupy musí být pravidelně kontrolovány, zda odpovídají aktuálnímu stavu systému ICT. Vyhodnocení vlivu změn na provozní postupy musí být také součástí (dílčích) změnových řízení systému ICT.

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) Musí existovat formální proces řízení změn systémů ICT v podobě formálního dokumentu, který podléhá změnovému řízení.

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) Pro role s privilegovaným přístupem ke kritickým systémům ICT musí být vhodně oddělen přístup. To znamená, že osoba v jedné privilegované roli nesmí zastávat jinou privilegovanou roli ve stejném systému ICT.

a) **„Rozdělení povinností"** resp. **„rozdělení funkcí"** minimalizuje riziko úmyslného nebo nedbalostního zneužití systému;

b) Provozní dokumentace informačního systému určí role, které je nutno oddělit, a rozsah jejich práv;

c) V případech, kdy nemůže být rozdělení povinností resp. rozdělení funkcí použito, měla by být zvážena jiná opatření, jako monitorování činností, auditní záznamy a dohled nadřízených zaměstnanců.

5.1.4 Vzájemné oddělení vývoje, testování a provozu

Organizační zásady:

72) Pro snížení rizika neoprávněného přístupu k provoznímu systému anebo jeho změně musí být vzájemně odděleny prostředky vývoje, testování a provozu.

- Projektová dokumentace kritických systémů ICT stanoví, zda posunutí procesu mezi stavy vývoj, testování a provoz musí být schváleno gestorem systému, a případné podmínky pro posunutí procesu.

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) V pravidelných intervalech (u kritických systémů ICT min. jednou týdně) musí být zkontrolovány kapacitní možnosti jednotlivých komponent systémů ICT (diskové prostory, operační paměť, výkon komponent, …). Tato kontrola může probíhat i v rámci automatizovaného systému na sledování stavu systému ICT. V případě nedostatku kapacit musí být tato informace eskalována odpovědnému pracovníkovi.

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) V systémech ICT, kde je to vhodné nebo nutné s ohledem na hrozby, aplikovat zvláštní opatření pro předcházení (prevenci) a detekování škodlivých programů a nepovolených mobilních kódů (například počítačových virů, síťových červů a trojských koňů) a zavést postupy pro jejich odstranění.

77) Na centrální komponenty systému ICT nesmí být přenášena žádná data (z CD/DVD, USB, přes síť apod.), která neprošla kontrolou na přítomnost škodlivých programů (např. antivirová kontrola na stanici uživatele).

78) Musí být zajištěna přiměřená úroveň bezpečnostního povědomí uživatelů a správců ve všech rolích o hrozbách od škodlivých programů.

Technické zásady:

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

- U kritických systémů by měly být zváženy zvýšené požadavky (např. kontrolu provádět jednou ihned po příjmu a podruhé po době min. 14 dnů; kontrolu provádět dvěma nezávislými antivirovými produkty; apod.).

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).

- Pokud politika justiční složky povolí přistupovat z privátního zařízení k přesně určeným službám systémů ICT justiční složky (např. e-mail), je uživatel odpovědný za zajištění politikou požadované úrovně bezpečnosti privátního zařízení.

81) Centrální komponenty systému ICT vystavené vyššímu riziku uplatnění škodlivých programů musí být vybaveny software na detekci škodlivých programů, který je pravidelně aktualizován a používán.

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.

- Mobilní kód je programový kód, který se přenáší z jednoho počítače na druhý a poté se automaticky spustí a vykoná specifickou funkci za minimální nebo žádné součinnosti s uživatelem. Mobilní kódy jsou součástí řady middleware služeb (např. zajišťujících propojení jednotlivých aplikací).
- Kromě ověření toho, že neobsahuje škodlivý kód, je kontrola mobilních kódů důležitá z důvodu vyhnutí se neoprávněnému použití nebo narušení systému, sítě nebo aplikačních zdrojů a jiným narušením bezpečnosti.

5.5 Zálohování

5.5.1 Zálohování dat a systémů

Organizační zásady:

83) Musí existovat plán zálohování a zálohování musí probíhat podle tohoto plánu. Plán zálohování musí obsahovat tvorbu záloh uživatelských dat a systémových dat (operačních systémů, aplikací a jejich konfigurací). Plán zálohování musí být dokumentován v podobě formálně řízeného dokumentu, který podléhá změnovému řízení. V případě neexistence plánu platí pro zálohování následující minimální pravidla:

a) Denní cyklus – každý pracovní den je provedena záloha uživatelských dat. Zálohy jsou uchovávány po dobu 1 týdne. Záloha denního cyklu se neprovádí v den pořizování záloh týdenního cyklu;

b) Týdenní cyklus – 1x za týden je provedena záloha uživatelských dat a systémových dat. Zálohy jsou uchovávány po dobu 2 týdnů. Záloha týdenního cyklu se neprovádí v den pořizování záloh měsíčního cyklu;

c) Měsíční cyklus – 1x za měsíc je provedena úplná záloha uživatelských dat a systémových dat. Zálohy jsou uchovávány po dobu 3 měsíců.

84) Musí probíhat pravidelná kontrola čitelnosti záloh. Tato kontrola musí probíhat jednou měsíčně nad částí nosičů záloh tak, aby každý nosič byl alespoň jednou ročně zkontrolován. V případě, že bude zjištěna chyba při čtení, musí být přijata příslušná opatření snižující riziko a tato opatření musí být dokumentována.

85) Nosič záloh nesmí být používán vícekrát, než je výrobcem definovaný maximální počet cyklů použití média.

86) Musí být prováděny pravidelné testy obnovy dat (systémů) ze záloh.

a) Pravidelný test obnovy ze záloh musí být prováděn ve frekvenci stanovené dokumentací resp. plánem zálohování systému ICT;

b) Není-li frekvence testování obnovy ze záloh stanovena dokumentací ani plánem zálohování systému ICT, musí být test obnovy prováděn minimálně jedenkrát za rok.

c) Výběr komponent systému ICT k obnově musí být proveden tak, aby jednou ročně byla vyzkoušena obnova každé komponenty systému ICT.

87) Jednou za 3 měsíce musí proběhnout kontrola přenosu dat mezi primárním a záložním centrem (je-li zřízeno) včetně úplnosti datového obsahu záložní lokality. V případě nedostatku jiných nástrojů může tato kontrola proběhnout ve formě kontroly náhodného vzorku dat, přenesených mezi primární a záložní lokalitou v době (blízké) vzniku zaznamenaných bezpečnostních incidentů nebo odstávky systémů.

Technické zásady:

88) Zařízení centrálních komponent a kritických systémů ICT musí být provozována v redundantní konfiguraci (hot–standby / cluster, warm–standby) nebo musí být uzavřeny servisní smlouvy garantující požadovanou dobu pro opětovné zprovoznění zařízení.

- Nestanoví-li provozní dokumentace systému ICT jinak, pak zařízení kritických systémů ICT musí být uvedeno do opětovného provozu v pracovní dny do 24 hodin od vzniku výpadku resp. bezpečnostního incidentu.

89) Disky centrálních komponent a kritických systémů ICT a další nosiče informací obsahující data musí být provozovány v redundantní konfiguraci, která zajistí uchování informací i v případě výpadku min. 1 komponenty (RAID1, …).

5.6 Správa bezpečnosti sítě a podpůrné infrastruktury

5.6.1 Síťová opatření

Organizační zásady:

90) Musí existovat formálně řízený dokument, který určuje pravidla a doporučení pro použití sítí a podpůrné infrastruktury resortu a justičních složek.

a) Počítačové sítě justičních složek musí být začleněny do „Důvěryhodné výpočetní základny“ (DVZ), která poskytuje bezpečnou infrastrukturu systémů ICT resortu spravedlnosti;

b) Správa DVZ musí být upravena v podobě formálně řízeného dokumentu, který podléhá změnovému řízení;

c) Musí být stanovena odpovědnost za provoz a bezpečnost

- centrálních částí DVZ a DVZ jako celku,
- lokálních částí DVZ provozovaných v justičních složkách.

91) Pro bezpečný provoz sítí a infrastruktury systémů ICT resortu a justičních složek musí být

a) stanoveny odpovědnosti a postupy pro správu vzdálených zařízení;

b) zavedena zvláštní opatření, která zajišťují důvěrnost a integritu dat přenášených veřejnými nebo bezdrátovými sítěmi a ochranu připojených systémů a aplikací (viz 6.4 a 7.3);

c) vytvořeny a zavedeny vhodné postupy zaznamenávání a monitorování událostí souvisejících s bezpečností;

d) koordinovány činnosti související se správou počítačů a sítí, a to jak z hlediska optimalizace služeb pro justiční složku, tak pro zajištění jejich konzistence v rámci celé DVZ.

Technické zásady:

92) Přístup ke službám přístupným z externí sítě musí být chráněn bezpečným rozhraním (např. firewallem a IPS) s možností rekonfigurace za účelem zabránění útoku.

- Systémy EZS, kamerové systémy a další systémy fyzické bezpečnosti jsou v oddělených sítích a provozovány dle certifikátů těchto systémů. Nejsou žádným způsobem propojeny s důvěryhodnou výpočetní základnou (DVZ) ani se systémy ICT resortu spravedlnosti.
  Pokud přesto má být prostřednictvím DVZ realizován přenos mezi komponentami EZS, kamerového nebo jiného systému, musí být realizován v oddělených segmentech DVZ bez možnosti propojení s IT systémy resortu spravedlnosti a jejich realizace musí být řádně zdokumentována.

5.6.2 Bezpečnost síťových služeb

Technické zásady:

93) Veškeré přenosy informací (viz 2.2) mezi systémy ICT přes externí sítě musí být chráněny šifrováním spojeným s kontrolou integrity přenášených dat.

94) Veškeré přenosy informací (viz 2.2) 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) Evidované nosiče informací (počítačová média) zahrnují

a) pevné disky centrálních technologií a počítačů včetně uživatelských, výměnné (opakovaně použitelné) nosiče informací pro centrální pořizování záloh a archivů a další média spojená se systémy ICT.

98) Správa evidovaných nosičů informací musí zajišťovat:

a) nosiče informací musí být evidovány a o jejich vyřazení musí být veden záznam pro potřeby auditu;

b) nosiče informací musí být ukládány

- v souladu s technickými specifikacemi výrobce,
- v prostředí zabezpečeném v souladu s významem pro zajištění dostupnosti dat a služeb systému;

c) pokud již nejsou nosiče informací potřebné, musí být jejich obsah vymazán předtím, než jsou uvolněny z okruhu osob oprávněných k seznámení se s informacemi na nich uložených a než jsou odstraněny z justiční složky (viz 4.2.3 „Údržba zařízení“, 4.2.4 „Bezpečnost zařízení mimo prostory justiční složky“ a 5.7.2 „Zničení záznamů na nosičích informací (počítačových médiích)“);

d) záznam na nosičích informací musí být obnovován v případech, kdy požadavek na dostupnost informací přesahuje životnost záznamu nebo média.

- záznam musí být přemístěn, pokud má dojít k dosažení životnosti média (podle specifikací výrobce) nebo médium vykazuje chyby,
- záznam musí být na médiu obnoven (např. kopírováním), pokud má dojít k dosažení limitu kvality záznamu (podle specifikací výrobce média);

e) při pořizování hardware musí být součástí smlouvy nebo objednávky ustanovení, že justiční složka je oprávněna v případě oprav a reklamací nepředat dodavateli pevný disk (tzv. „keep your hard drive“).

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) Na nosičích informací, které jsou přemísťovány v rámci téhož systému ICT ale uživatelům nebo správcům s jinými přístupovými právy, musí být přepsána data.

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) Pro zabránění neautorizovanému přístupu nebo zneužití informací musí být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání:

   a) omezení vstupu neoprávněným osobám do prostor se zařízeními a médii, které umožňují přístup k informacím;

   b) zachovávání záznamu o oprávněných příjemcích dat;

   c) ochrana tiskových dat čekajících na výstup;

   d) omezení distribuce informací na odůvodněné případy;

   e) zřetelné označování všech kopií dat pro všechny autorizované příjemce;

   f) kontrola dat čekajících na odesílání;

   g) kontrola rozdělovníku a seznamu autorizovaných příjemců v pravidelných intervalech.

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

5.7.4 Bezpečnost systémové dokumentace

Organizační zásady:

107) Systémová dokumentace ICT musí být chráněna před neoprávněným přístupem.

   a) systémová dokumentace musí být bezpečně uložena a chráněna před zneužitím a proti zničení;

   b) seznam oprávněných osob pro přístup k systémové dokumentaci by měl být omezen na minimum (administrátoři, správci IS a další osoby, které ji potřebují k výkonu své pracovní činnosti) a v případě kritických systémů ICT by měl být autorizován vlastníkem systému/aplikace;

c) systémová dokumentace, která je uložena na síti nebo je jejím prostřednictvím poskytována, by měla být odpovídajícím způsobem chráněna.

5.8 Výměna informací

5.8.1 Postupy při výměně informací a programů

Organizační zásady:

108) Opatření na ochranu informací při jejich výměně pro všechny typy používaných komunikačních zařízení musí být upravena v podobě formálně řízeného dokumentu, který podléhá změnovému řízení. Při vytváření postupů a zavádění opatření musí být zváženo následující:

a) postupy určené na ochranu informací před jejich zachycením, odposlechem, zkopírováním, modifikací, chybným směrováním a zničením;

b) postupy detekce a ochrany před škodlivými kódy (viz také 5.4.1);

c) postupy na ochranu informací přenášených elektronickou poštou a v jejich přílohách;

d) postupy upravující použití zařízení pro elektronickou komunikaci (viz 2.1, odst. 9);

e) postupy pro použití bezdrátové komunikace s ohledem na související specifická rizika;

f) odpovědnost zaměstnanců, smluvních a třetích stran za to, že nezkompromitují justiční složku, například odesláním hanlivých zpráv, použitím elektronické pošty k obtěžování či neautorizovaným nákupům, atd.;

g) použití kryptografických technik pro zajištění důvěrnosti, integrity a autentičnosti přenášených informací (viz 7.3);

h) vytvoření pravidel pro uchování a likvidaci veškeré obchodní korespondence, včetně elektronické pošty v souladu s legislativou a předpisy justiční složky;

i) nenechávat informace volně ležet v tiskárnách, kopírovacích zařízeních a faxech, kde mohou být volně přístupné neautorizovaným osobám;

j) zavedení opatření a omezení souvisejících s přesměrováním elektronické komunikace, např. automatické přeposílání elektronické pošty na externí emailovou adresu;

k) poučení zaměstnanců, že:

- mají dodržovat adekvátní opatrnost, například neprobírat informace, které by mohly být při telefonování zaslechnuty či odposlechnuty;
- nemají nechávat zprávy na záznamníku, protože tyto zprávy mohou být přehrány neautorizovanou osobou, uloženy do veřejné sítě nebo uloženy jako výsledek chybného telefonátu;
- s použitím faxů jsou spojeny hrozby prozrazení informace;
- při registraci programového vybavení nesmí zadávat své osobní údaje, které pak mohou být použity neoprávněným způsobem;
- moderní faxová zařízení a kopírky používají vyrovnávací paměť, ve které je uložen obsah tištěných stránek, pro případ, že v zásobníku dojde papír nebo nastane chyba při přenosu dat.

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 (2.2). 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.

a) Auditní záznamy nemusí být pořizovány při použití cvičné anonymizované databáze.

b) Auditní záznamy nemusí být pořizovány při použití provozních dat pro testování obnovy systému po havárii a v případech takových testů, při kterých není přistupováno k záznamům databáze. Provedení testů musí být zapsáno v provozním deníku.

117) Projektová dokumentace kritických systémů ICT určí, které auditní záznamy a po jakou dobu musí být uchovány.

a) U systémů zpracování osobních údajů, účetnictví a dalších agend upravených legislativou, je doba, po kterou musí být uchovány auditní záznamy aplikačních logů, odvozena od požadavků příslušného právního předpisu;

b) Nestanoví-li projektová dokumentace dobu uchování logů, musí být logy uchovány minimálně po dobu 6 měsíců za provozu systému a 6 měsíců po skončení provozu systému.

c) Projektová dokumentace systému ICT může pro určité komponenty nebo celý systém stanovit způsob a podmínky odfiltrování záznamů standardních událostí resp. kumulace vyhodnocených záznamů standardních událostí.

5.9.2 Monitorování používání systému

Organizační zásady:

118) Požadovanou úroveň monitorování stanoví projektová dokumentace systému ICT na základě hodnocení rizik. Aktivity související s monitorováním událostí musí být v souladu se zákonnými požadavky.

119) Vytvořené auditní záznamy musí být pravidelně analyzovány.

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) O provedených administrátorských zásazích v systému ICT, přemístění zařízení apod., musí být prováděny záznamy. Záznamy musí obsahovat čas zásahu, jméno zaznamenávající osoby a popis události.

123) Provozní deník musí být uchováván po celou dobu provozu systému a po skončení provozu systému po dobu stanovenou provozní dokumentací systému.

5.9.5 Záznam selhání systému

Organizační zásady:

124) Chyby komponent systému ICT zaznamenané v auditních záznamech musí být prozkoumávány a musí být podniknuta příslušná opatření. O příslušném prozkoumání a závěrech (navržených opatřeních) musí existovat záznam.

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) Musí existovat jednotná politika přístupu definující skupiny uživatelů, příslušné role a příslušná přístupová práva v rámci jednotlivých systémů ICT a aplikací. Politika přístupu musí být založena na rolích a musí být dokumentovaná v podobě formálně řízeného dokumentu.

127) Politika řízení přístupu musí být přezkoumána každé 2 roky nebo po každé větší změně systému ICT (zavedení nové služby, změna architektury apod.).

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) Politika řízení přístupu musí zohledňovat požadavky na vzájemné oddělení povinností definované v této Politice BICT.

6.2 Řízení přístupu uživatelů

6.2.1 Registrace uživatele

Organizační zásady:

130) Pro jednotlivé skupiny uživatelů (role), definované v politice řízení přístupu, musí existovat postupy pro registraci/zavedení uživatele do systému ICT a pro zrušení uživatele v systému ICT, a to včetně identifikace rolí, které tuto registraci a zrušení schvalují. Tyto postupy musí být dokumentovány v podobě formálních řízených dokumentů, které podléhají změnovému řízení (viz 3 „Bezpečnost lidských zdrojů“).

131) O každé registraci/zrušení účtu uživatele musí být proveden záznam včetně jmen osob podílejících se na procesu registrace/zrušení. Tento záznam musí být uchován po dobu platnosti účtu a následně po zablokování/zrušení účtu uživatele

a) u kritických systémů ICT minimálně po dobu 3 let a

b) u ostatních systémů ICT po dobu 1 roku.

6.2.2 Správa uživatelských hesel

Organizační zásady:

132) Při registraci nebo opětovném nastavení musí uživatelé dostat jednorázové heslo, které budou nuceni při prvním přihlášení změnit. Pokud není možné vynutit změnu hesla technickým mechanismem, musí uživatel dostat unikátní heslo.

133) Musí být zavedeny postupy pro ověření identity uživatele žádajícího o přidělení nového, náhradního anebo dočasného hesla poskytující dostatečnou záruku identity uživatele. Tyto postupy musí být dokumentovány v podobě formálních řízených dokumentů, které podléhají změnovému řízení.

134) Předávaná hesla nesmí být posílána emailem (nebo jinak přenášena) v nechráněné podobě a nesmí být sdělována třetím osobám.

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) Pro všechny účty s privilegovaným přístupem musí být minimálně jednou za 6 měsíců provedena jejich kontrola zahrnující jejich výpis ze systému a porovnání s evidencí.

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) Uživatel má povinnost změnit své nově přidělené heslo ihned po prvním přihlášení.

140) Heslo uživatele musí být těžko uhodnutelné. Musí být

a) minimálně 8 znaků dlouhé,

b) složeno ze znaků alespoň ze tří skupin (malé znaky; velké znaky; číslice; jiné znaky),

c) měněno minimálně jednou za rok a maximálně jednou za 1 den,

d) bez vazby na uživatele nebo jeho okolí (např. nesmí obsahovat jméno blízké osoby, datum narození, telefonní číslo),

e) odlišné minimálně od předchozích pěti hesel.

141) Hesla systémových účtů a procesů systému ICT musí mít definované vlastnosti (min. 14 znaků, složeno z kombinace znaků alespoň ze tří skupin, bez vazby na justiční složky).

142) Hesla pro přístup k tokenu (např. PIN k čipové kartě) musí mít minimálně 4 znaky a musí být měněna jednou za rok.

6.3.2 Neobsluhovaná uživatelská zařízení

Organizační zásady:

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

a) Opouští-li pracoviště na krátkou dobu v průběhu pracovní doby, musí svůj účet uzamknout;

b) Opouští-li pracoviště na delší či neurčitou dobu nebo na konci pracovní doby, musí ukončit aplikace a odhlásit účet. Tato povinnost může být vynucena systémově.

6.4 Řízení přístupu k síti

6.4.1 Politika užívání síťových služeb

Organizační zásady:

144) Musí existovat politika síťových služeb respektující bezpečnostní opatření této Politiky BICT. Politika síťových služeb musí být dokumentována v podobě formálního řízeného dokumentu, který podléhá změnovému řízení. Nastavení síťových služeb musí zohledňovat tuto politiku síťových služeb.

6.4.2 Autentizace uživatele pro externí připojení

Technické zásady:

145) Neanonymní uživatel přistupující z externí sítě do systému ICT musí být autentizován před přístupem do vnitřní sítě justiční složky. Příchozí spojení musí být ukončena ve vyhrazené síti (např. DMZ).

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) U mechanizmů identifikace a autentizace musí být použity následující zásady:

a) neposkytovat nápovědu během přihlašovacího postupu, která by pomohla neoprávněnému uživateli;

b) zkontrolovat platnost přihlašovacích informací jen v případě, že jsou vstupní data kompletní s tím, že v případě chyby nesmí systém ICT indikovat, která část dat je správná nebo chybná;

c) při dokončení úspěšného přihlášení zobrazit informace o čase posledního přihlášení a podrobnosti o posledních neúspěšných pokusech o přihlášení, pokud to systém umožňuje;

d) zaznamenávat úspěšné i neúspěšné pokusy o přihlášení.

149) V případě autentizace jménem a heslem musí být dále použity následující zásady:

a) omezit počet povolených neúspěšných přihlašovacích pokusů (max. 5 pokusů) a další pokusy o přihlášení povolit až po uplynutí definované doby (min. 30 min.), nebo po odblokování správcem;

b) zaznamenávat překročení maximálního počtu pokusů o přihlášení;

c) nezobrazovat heslo při jeho zadávání;

d) hesla musí být ukládána a přes síť posílána v chráněné podobě (zašifrovaná nebo jinak upravená, např. hash kód hesla).

6.5.2 Identifikace a autentizace uživatelů

Technické zásady:

150) Každý uživatel (každá kombinace uživatele, procesu a role) musí mít jednoznačný uživatelský identifikátor, který nesmí být sdílen mezi více uživateli.

151) Uživatelé i procesy musí být před přístupem k službám a datům systému ICT identifikováni a autentizováni.

152) Autentizace uživatelů musí být zajištěna buď kombinací jméno a heslo nebo prostředky dvoufaktorové autentizace (např. čipovou kartou ve spojení s PIN).

153) Projektová dokumentace kritických systémů ICT, u kterých to požadují výsledky analýzy rizik, stanoví požadavek, aby autentizace uživatelů s privilegovaným přístupem, právem zapisovat a měnit, byla zajištěna prostředky dvoufaktorové autentizace (např. čipovou kartou ve spojení s PIN).

6.5.3 Systém správy hesel

Technické zásady:

154) Uživatel musí mít možnost změnit své heslo.

155) Systém ICT musí vynucovat kvalitu autentizačního prostředku (např. dobu změny hesla a jeho složitost), pokud to systém umožňuje.

6.5.4 Časové omezení relace

Technické zásady:

156) Autentizované spojení uživatele, které není aktivní déle než 30 minut, musí být přerušeno anebo musí být vyžádána nová autentizace.

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) Práva jednotlivých uživatelů a skupin uživatelů aplikačních systémů, včetně pracovníků podpory, musí být maximálně omezena v souladu s jejich potřebou znát a v souladu s politikou řízení přístupu (viz 6.1.1). Pro omezení přístupu k informacím využívat následující opatření:

a) přidělení přístupu uživatelů jen k aplikacím, které potřebují v souladu s potřebou znát;

b) v rámci aplikace omezení přístupu uživatelů jen k funkcím a datovým položkám, které potřebují v souladu s potřebou znát;

c) omezení přístupových oprávnění uživatelů na nezbytný minimální rozsah (čtení, zápis, vymazání, vykonání/spuštění);

d) zajištění toho, aby výstupy z aplikací, které nakládají s informacemi,

- obsahovaly relevantní informace,
- byly posílány pouze oprávněným terminálům a do oprávněných lokalit,
- byly pravidelné kontrolovány, aby nepublikovaly nadbytečné údaje.

6.7 Mobilní výpočetní zařízení a práce na dálku

6.7.1 Mobilní výpočetní zařízení a sdělovací technika

Technické zásady:

159) Při použití mobilních výpočetních prostředků musí být věnována zvláštní pozornost tomu, aby nebyly vyzrazeny informace chráněné justičními složkami. Proto musí být přijata taková formální pravidla a opatření na ochranu proti hrozbám, která zohlední rizika používání mobilního výpočetního zařízení zejména v nezabezpečeném prostředí.

a) Musí být zajištěny požadavky pro bezpečné připojování mobilních výpočetních zařízení k sítím a návod k použití těchto prostředků na veřejných místech, v zasedacích místnostech a jiných nechráněných místech mimo prostor justiční složky;

b) Musí být k dispozici ochrana proti neautorizovanému přístupu a vyzrazení informací uložených a zpracovávaných těmito prostředky, například použitím kryptografických technik (viz 7.3);

c) Při použití těchto zařízení na veřejných místech se uživatelé musí vyhnout riziku odpozorování neautorizovanými osobami;

d) Měly by být použity prostředky proti škodlivým programům a tyto prostředky by měly být aktualizovány (viz 5.4);

e) V pravidelných intervalech by měly být vytvářeny zálohy všech v zařízení uložených kritických informací justičních složek. Zálohy musí být odpovídajícím způsobem chráněny proti zneužití, krádeži nebo ztrátě informací;

f) Vzdálený přístup k informacím justiční složky prostřednictvím veřejných sítí by měl být umožněn pouze po úspěšné identifikaci a autentizaci, a to s nasazením vhodných mechanizmů řízení přístupu (viz 6.4);

g) Musí být zajištěna bezpečnost zařízení mimo prostory justiční složky (viz 4.2.4). Krádež nebo ztrátu mobilního zařízení musí uživatel bezodkladně nahlásit správci systému, jehož je zařízení součástí;

h) Zaměstnanci používající mobilní zařízení musí být seznámeni s formálními pravidly a k dosažení povědomí o dalších rizicích tohoto způsobu práce a stanovených opatřeních.

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 3.3).

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) Jednou ročně musí být seznam schválených algoritmů zkontrolován, musí být vyhodnocena síla uvedených algoritmů vzhledem k časovému horizontu 5–10 let a následně seznam upraven.

171) V případě vyřazení algoritmu ze seznamu schválených algoritmů musí být prověřeno jeho použití v systémech ICT a podniknuta opatření k nápravě stavu.

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) Pokud to charakter použití tajných nebo soukromých klíčů nevyžaduje, nesmí být tyto klíče zálohovány.

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) Přístup ke kryptografickým klíčům musí být omezen výhradně na osoby s pracovní potřebou mít k těmto klíčům přístup (správci systému ICT nebo osoby odpovědné za provádění obnovy systémů po havárii).

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) Soukromé klíče resortních certifikačních autorit musí být generovány i uloženy v čipových kartách nebo ve specializovaném hardware (HSM – Hardware Security Module).

179) Tajné nebo soukromé klíče musí být distribuovány bezpečným způsobem (v zašifrovaném tvaru nebo na specializovaném hardware), přičemž tajemství pro přístup ke klíči (k jejich aktivaci) musí být distribuováno nezávislým kanálem.

7.4 Bezpečnost systémových souborů

7.4.1 Správa provozního programového vybavení

Organizační zásady:

180) Pravidelně musí být prováděna kontrola správné funkčnosti operačních systémů a aplikací na provozních systémech.

7.4.2 Ochrana testovacích údajů

Organizační zásady:

181) Pro účely testování a školení mohou být používána jen anonymizována data (zejména nesmí být použity kopie dat z provozních databází).

182) Použití skutečných provozních dat a databází pro účely testování, školení apod. musí být schváleno stejně jako jiné výjimky z této Politiky BICT resortu spravedlnosti (viz 10.4). Přitom budou obvykle stanoveny podmínky jako zachování identifikace a autentizace uživatele, přístupových práv a synchronizace času ekvivalentních s provozním systémem, vytváření auditních záznamů (viz 5.9.1) atd.

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) Minimálně jedenkrát za 3 roky, při podstatných změnách technologií nebo při výskytu závažných hrozeb, musí být ověřena bezpečnost veškerých rozhraní systému ICT otevřených do externí sítě, a to formou ověření bezpečnosti rozhraní buď provedením skenu automatizovaným nástrojem (při nízkých rizicích) nebo provedením penetračních testů. Na základě zprávy o provedení skenu resp. testů musí být odstraněny nalezené zranitelnosti.

189) Minimálně jednou za 2 roky musí být provedeny penetrační testy na centrální resortní komponenty systému ICT otevřená do interní sítě (kromě sítí vyhrazených pro provoz centrálních komponent systému ICT). Na základě zprávy o provedení testu musí být odstraněny nalezené zranitelnosti.

8 ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Organizační zásady:

190) Musí existovat jednotný závazný postup pro hlášení bezpečnostních událostí (incidentů) a zranitelností systémů ICT. Tento postup musí obsahovat příklady jednotlivých událostí, aktuální kontaktní údaje a musí být dostupný všem zaměstnancům a smluvním partnerům justiční složky. Uživatelé a správci musí být s tímto postupem seznámeni.

191) Musí existovat předem připravený plán (postup) zvládání bezpečnostních událostí nebo zjištěných zranitelností kritických systémů ICT. Plán musí obsahovat odpovědnosti, kontaktní údaje a jednotlivé kroky pro definované skupiny událostí včetně hlášení (notifikace) a případné eskalace. Zainteresovaní pracovníci musí být s plánem prokazatelně seznámeni.

a) Porušení bezpečnostních opatření je chápáno jako bezpečnostní incident a řešeno jako porušení pracovních povinností, resp. porušení právních předpisů;

b) Justiční složka je odpovědná za vyšetřování a hlášení bezpečnostních incidentů v systémech ICT v rozsahu své působnosti. Dále je odpovědná za stanovení nápravných opatření a kontrolu jejich realizace;

c) Každý uživatel systému ICT a/nebo vlastník informací, je povinen hlásit zjištěná porušení ustanovení bezpečnostních směrnic systémů ICT, zjištěné bezpečnostní incidenty nebo podezření na ně svému nadřízenému a vedoucímu informatikovi složky. Porušení zákona hlásí jejich cestou nebo i sám příslušnému správnímu orgánu.

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) U kritických systémů ICT musí být minimálně jedenkrát ročně vyhodnoceny záznamy o zjištěných bezpečnostních událostech a navržena potřebná opatření k odstranění nejvíce frekventovaných nebo závažných incidentů.

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) Odbor informatiky MSp zpracovává plán kontrol dodržování této Politiky BICT. Jednotlivé složky resortu spravedlnosti provádí kontroly dodržování této Politiky BICT dle vlastních potřeb.

203) V pravidelných intervalech musí být prováděna kontrola systémů ICT zahrnující mimo jiné i kontrolu účinnosti bezpečnostních opatření, činností uživatelů, provedených záznamů a oprávněnosti této činnosti.

204) Rozsah kontroly musí být schválen. Přístup k programům a datům by měl být omezen pouze pro čtení. Jiný typ přístupu než „pouze pro čtení“ by měl být povolen jen na samostatných kopiích souborů systému, které by po ukončení kontroly měly být smazány anebo, pokud je to vyžadováno, řádným způsobem chráněny; Přístup k nástrojům určeným pro kontrolu by měl být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.

205) Kontrolu musí provádět interní nebo externí pracovník, v každém případě však osoba, která se nepodílí na provozu systému ICT a ani není součástí organizační složky odpovídající za provoz systému ICT. Kontroly dodržování Politiky BICT dle plánu kontrol odboru

informatiky MSp provádí pracovník odboru informatiky MSp nebo osoba určená odborem informatiky MSp.

206) O provedení kontroly musí být vytvořena kontrolní zpráva, která bude uložena v úložišti kontrolních zpráv resortu spravedlnosti (podle speciálního předpisu).

207) S obsahem kontrolní zprávy musí být seznámen vedoucí justiční složky a vedoucí informatik složky.

10.4 Výjimky

208) Výjimky z Politiky BICT resortu spravedlnosti a výjimky z interních prováděcích předpisů k Politice BICT resortu spravedlnosti schvaluje ředitel odboru informatiky MSp. Výjimky musí být časově omezeny. Platnost výjimky může být prodloužena na základě výsledků přezkoumání nebo na základě nové žádosti.

a) O výjimku pro justiční složku žádá vedoucí justiční složky;

b) Ředitel odboru informatiky MSp může vydat také obecnou výjimku pro resort spravedlnosti nebo pro více justičních složek

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

Digitálně podepsal Ing. Petr Koucký
DN: c=CZ, o=Česká republika - Ministerstvo spravedlnosti [IČ 00025429], ou=Odbor informatiky, ou=473, cn=Ing. Petr Koucký, serialNumber=P124071, title=ředitel odboru
Datum: 2012.12.21 11:17:28 +01'00'

Ing. Petr Koucký
ředitel odboru informatiky

Seznam právních norem a literatury k bezpečnosti informací v systémech ICT

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)

Příloha 1 - Seznam právních norem a literatury

[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).