GENERICKÁ SYSTÉMOVÁ BEZPEČNOSTNÍ POLITIKA ICT

KÓD	MP-3/2015
VERZE	3.2
TYP	Metodický pokyn
ČÍSLO JEDNACÍ	ČP/13715/2021/CKA/02
NAHRAZUJE VNITŘNÍ PŘEDPIS	MP-3/2015 – verze 3.1
KLASIFIKACE	Interní
PLATNOST OD	8. 3. 2021
ÚČINNOST OD	15. 3. 2021
GARANT	Ing. Jaroslav Hloušek ředitel úseku ICT a eGovernment podepsáno elektronicky dne 8. 3. 2021
SCHVALOVATEL	schváleno garantem – technická revize

Obsah dokumentu

1. Úvodní ustanovení

1.1. Účel

(1) Generická systémová bezpečnostní politika ICT (dále jen Politika) je vnitřním předpisem České pošty, s.p. (dále jen ČP) a je součástí komplexních opatření bezpečnostního systému ČP. Svým určením a obsahem Politika rozpracovává směrnici SM-1/2015 Bezpečnostní politiku ICT (dále jen „směrnice Bezpečnostní politika ICT“) do generických systémových opatření k zajištění bezpečnosti ICT ČP a stanovuje zásady bezpečnosti informací v oblasti ICT ČP.

(2) Předmětem Politiky není ochrana utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací.

1.2. Působnost

Politika je závazná pro všechny zaměstnance ČP a externí subjekty, kteří se podílí na procesech návrhu, vývoje, realizace, bezpečnosti a provozu systémů ICT ČP. Seznámení externích subjektů s touto Politikou zajistí prokazatelným způsobem garant externí identity.

1.3. Cíle

(1) Základním cílem Politiky je stanovit požadavky a postupy pro vymezení, zavedení, udržování a zlepšování systémů bezpečnosti informací v oblasti systému ICT ČP.

(2) Jedná se zejména o:

- definování systému řízení bezpečnosti ICT ČP,
- stanovení požadavků na ochranu systémů ICT ČP, identifikaci aktiv a pravidel pro jejich používání a ochranu, určení pravidel pro zálohování v rámci systémů ICT ČP, monitoring, pořizování a vyhodnocování záznamů o událostech, které mohou ovlivnit bezpečnost, zajištění antivirové ochrany, definování pravidel pro oblast řízení kontinuity (plány obnovy ICT) a zvládání bezpečnostních incidentů, jejich hlášení, vyhodnocování a přijímání opatření, atd.

1.4. Přehled změn proti předchozí verzi

Oproti verzi 3.1 došlo k následujícím změnám:

Změna v příloze č. 1 Schválené šifrovací algoritmy.
Příloha č. 1 označena jako samostatná příloha dostupná na IntraNetu ČP.
Formální úpravy.

1.5. Zkratky a pojmy

Politika využívá základní pojmy a názvosloví uvedené ve směrnici Bezpečnostní politika ICT (kapitola 1.4).

ZKRATKY	
ICTV	útvar ICT vývoj
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
Specializovaný útvar ICTB	specializovaný útvar ICT bezpečnost

POJMY	
Bezpečnostní manažer ICT	Vedoucí specializovaného útvaru ICT bezpečnost, který je pověřen Gestorem bezpečnosti ICT řízením bezpečnosti ICT ČP, tj. implementací a prosazováním bezpečnosti ICT v rámci ČP, zpracováním a aktualizací bezpečnostní dokumentace, zajištěním a rozvojem bezpečnostního monitoringu, koordinací sledováním a vyhodnocováním bezpečnostních incidentů a prováděním bezpečnostních kontrol shody ICT ČP. Řídí bezpečnostní architekty a bezpečnostní administrátory. Zastává jmenovanou bezpečnostní roli manažera kybernetické bezpečnosti dle § 6 odst. 3 písm. a) vyhlášky 82/2018 Sb., o kybernetické bezpečnosti.
Politika	Generická systémová bezpečnostní politika ICT
Garant externí identity	Vedoucí věcně příslušné organizační jednotky, v jehož gesci je externí subjekt smluvně vázán

2. Organizace systémové bezpečnosti informací

2.1. Dokumentace

(1) Za přezkoumání a aktualizaci Politiky odpovídá Bezpečnostní manažer ICT. Přezkoumání a aktualizaci provádí minimálně jedenkrát ročně.

(2) Návrh na aktualizaci Politiky předkládá Bezpečnostní manažer ICT Gestorovi bezpečnosti ICT, který je garantem Politiky.

2.2. Přidělení odpovědností v oblasti bezpečnosti informací

(1) Politika využívá definici rolí a stanovení odpovědností uvedených ve směrnici Bezpečnostní politika ICT (kapitola 2.1).

(2) Pokud některou z uvedených rolí vykonává pracovník externího subjektu, vztahují se na něj stejné povinnosti jako na zaměstnance ČP.

(3) Neplnění povinností či odpovědností definovaných Politikou je pokládáno za závažné porušení pracovních povinností.

2.3. Zastupitelnost

(1) Všechny definované role musí mít definovaný zástup s ohledem na dopady jejich nedostupnosti, a to jak z hlediska kapacit, tak i znalostí potřebných v případě havárií a mimořádných situací.

(2) Role administrátora systému ICT ČP musí být správcem aktiva přidělena minimálně 2 osobám. V případě, že je požadován provoz daného systému ICT ČP v režimu 7x24, musí být tato role přidělena minimálně 3 osobám.

2.4. Externí subjekty

(1) Přístup externích subjektů k ICT ČP, za účelem plnění smluvního ujednání, musí být schválen specializovaným útvarem ICTB z pohledu možných bezpečnostních rizik a následně musí být

specializovaným útvarem ICTB stanovena požadovaná bezpečnostní opatření (podmínky síťového připojení, přístupy externích subjektů do prostor, pracovní podmínky, školení atd.).

(2) Za zajištění bezpečnostních opatření stanovených specializovaným útvarem ICTB a níže uvedených požadavků ve smluvním ujednání odpovídá vedoucí věcně příslušné organizační jednotky, v jehož gesci je externí subjekt smluvně vázán.

2.4.1. Pravidla a principy pro výběr dodavatelů

(1) Dodavatel aktiv musí být vybrán na základě výběrového řízení, které stanoví potřebné kvalifikační předpoklady.

(2) Musí být stanoveny postupy a odpovědnosti zaměstnanců ČP při procesu prověřování vybraných externích subjektů, se kterými ČP vstupuje do smluvních vztahů. Jedná se o postupy, jejichž cílem je zjistit, shromáždit a zhodnotit informace o externím subjektu získané z interních a také z veřejně dostupných zdrojů. Problematiku detailně řeší MP-3/2016 Compliance prověřování vybraných externích subjektů.

2.4.2. Bezpečnostní požadavky pro přístup externích subjektů

(1) Při přístupu externích subjektů k ICT ČP, za účelem plnění smluvního ujednání, musí být:

a) zajištěna ochrana aktiv (postupy sloužící k ochraně aktiv, opatření zajišťující vrácení či zničení aktiv po ukončení smluvního vztahu nebo v jeho průběhu, zajištění důvěrnosti, integrity a dostupnosti aktiv, omezení kopírování, šíření informací atd.).

b) stanoveny:

- garanti externích osob s vazbou na smlouvu s ČP a důvod přístupu
- povolené metody přístupu a jejich pravidelná kontrola,
- jedinečné identifikátory uživatelů (CPJM)
- schvalovací procesy pro přístup uživatele a jeho role oprávnění,
- požadavky na vedení a dostupnost seznamu osob, které jsou vzhledem ke svým předdefinovaným právům a privilegiím oprávněni využívat nabízené služby.

c) zajištěna možnost monitorovat činnost externích subjektů nebo maximálně omezit neoprávněné aktivity,

d) zajištěno právo auditovat smluvní povinnosti nebo právo nechat provést tyto audity třetí stranou,

e) stanoven popis eskalace problému v případech řešení havárie,

f) určena odpovědnost za instalaci a údržbu technického a programového vybavení,

g) dohodnuta pravidla hlášení a schválený formát těchto hlášení,

h) určen specifikovaný proces řízení změn,

i) přijatá opatření k zajištění ochrany před škodlivým programovým vybavením,

j) umožněno vyšetřování bezpečnostních incidentů.

(2) Za zajištění výše uvedených požadavků odpovídá vedoucí organizačního celku ČP, v jehož gesci je externí subjekt smluvně vázán.

2.4.3. Bezpečnostní požadavky v dohodách s externími subjekty

(1) V případě dodavatelsko-odběratelských vztahů je základním cílem zachovat bezpečnost informací a to i tehdy, kdy odpovědnost za zpracování informací byla přenesena na jiný právnický subjekt.

(2) Ve smluvních ujednáních s externími subjekty (dodavatelé produktů, služeb, outsorcintgu apod.), kteří se mohou dostat do kontaktu s chráněnými informacemi, musí být zejména:

a) přesně definováno, co tvoří chráněné informace,

b) definována povinnost seznámit se s bezpečnostními politikami ČP, případně systémovými bezpečnostními politikami systémů, ke kterým přistupuje, a povinnost je dodržovat, či absolvovat školení, které to obsahuje,

c) definována povinnost mlčenlivosti a ochrana informací ČP,

d) stanoven rozsah odpovědnosti za škody způsobené činností v ČP a v odůvodněných případech také např. autorská práva (majetková autorská práva), případně licenční ujednání k oprávnění výkonu majetkových práv,

e) sankce za nedodržení pravidel uvedených v bezpečnostních politikách ČP,

f) odpovědnosti a povinnosti v případě výskytu bezpečnostních incidentů,

g) hmotná odpovědnost za škody způsobené porušením povinností jejího pracovníka,

h) rozsah předmětu plnění,

i) licenční ujednání,

j) záruky za kvalitní provádění služeb,

k) jasně definované odpovědnosti,

l) systém kontroly plnění smluvního ujednání, právo auditu a monitoringu činností.

(3) Zařazení dodavatele mezi „Významné“ podle VoKB určuje Gestor bezpečnosti ICT na návrh Bezpečnostního manažera ICT. Seznam významných dodavatelů podléhá kontrole aktuálnosti minimálně jednou ročně. Seznam vede a zajišťuje kontrolu Bezpečnostní manažer ICT.

(4) Ve smluvních ujednáních s významnými dodavateli (definovanými podle odstavce (3)) musí být:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),

b) ustanovení o oprávnění užívat data,

c) ustanovení o autorství programového kódu, popřípadě o programových licencích,

d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),

e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,

g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o

1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,

j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),

k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),

l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,

m) pravidla pro likvidaci dat,

n) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a

o) ustanovení o sankcích za porušení povinností.

2.4.4. Pravidla pro hodnocení dodavatelů

Každý dodavatel musí být Bezpečnostním manažerem ICT ve spolupráci s vlastníky aktiv v pravidelných intervalech (minimálně 1x ročně) ohodnocen z hlediska dodržování bezpečnostních požadavků.
V rámci výběrového řízení a před uzavřením smlouvy se provádí hodnocení rizik souvisejících s plněním předmětu výběrového řízení přiměřeně podle přílohy č. 2 k vyhlášce 82/2018 Sb.

3. Řízení aktiv

3.1. Evidence a odpovědnost za aktiva

1) Povinnost evidence a odpovědnost za aktiva je definována ve směrnici Bezpečnostní politika ICT.

2) Vlastník/garant aktiv je povinen Bezpečnostnímu manažerovi ICT hlásit veškeré změny, které mohou mít dopad na jejich bezpečnost.

3.2. Stanovení dostupnosti aktiv

(1) Požadavky na dostupnost aktiv ČP musí stanovit vlastník aktiva na základě business potřeb a analýzy dopadů.

(2) Kritéria dostupnosti jsou:

a) maximální tolerovaná doba nedostupnosti aktiva stanované na základě maximálních akceptovatelných dopadů, (MTPD),

b) procentní dostupnost,

c) požadovaná provozní doba, tj. doba, po kterou službu ICT ČP standardně využívá uživatel,

d) čas a délka pravidelných odstávek pro údržbu.

(3) Procentní dostupnost je poměr mezi očekávanou nebo naměřenou dobou trvání služeb daného aktiva a celkové doby časového období (součtu doby trvání služeb a doby nedostupnosti služeb). Standardně se dostupnost uvádí v procentech pro časové období jednoho roku.

(4) Provozní doba, po kterou službu ICT ČP standardně využívá zákazník ČP, je uváděna jako požadavek na provozní dobu dané služby (např. 7x24 (nepřetržitě 7 dnů 24 hodin), 5x8 (pondělí až pátek v pracovní době), atd.).

(5) Aktiva/ služby ICT ČP jsou považovány za nedostupné (v režimu mimo provoz nebo omezení funkcionality) od okamžiku oprávněného nahlášení nedostupnosti nebo nesprávné funkčnosti uživatelem ICT ČP až do okamžiku obnovení provozu nebo nabídnutí náhradního řešení, které však není finálním vyřešením vzniklého incidentu.

(6) Do výpadku služby není započítáván výpadek za účelem provedení plánované údržby. Odstávka musí být vlastníkem aktiv schválena a nahlášena uživatelům minimálně 5 pracovních dnů předem.

(7) Dostupnost aktiv musí být sledována a vyhodnocována měsíčně. Toto provádí správci aktiv jednotlivých částí ICT ČP a výsledky předkládají vlastníkovi aktiv a Bezpečnostnímu manažerovi ICT.

(8) Provozní třídy aktiv jsou stanoveny na základě analýzy dopadů a dále na základě technických podmínek pro nasazení služby ICT a na základě standardů ICT ČP uvedených v samostatné dokumentaci útvaru ICT vývoj.

4. Personální bezpečnost

Politika se plně řídí ustanoveními personální bezpečnosti uvedenými ve směrnici Bezpečnostní politika ICT.

5. Fyzická bezpečnost

(1) Fyzická bezpečnost je soubor opatření k zamezení neautorizovaného přístupu do bezpečnostního perimetru. Realizace a kontrola opatření podle bezpečnostního projektu na ochranu objektů se zařízením ICT spadá do působnosti útvaru bezpečnost.

(2) Zaměstnanci ČP případně zaměstnanci externích firem mají povinnost dodržovat podmínky stanovené k zabezpečení objektů, oblastí a místností (dále zabezpečené oblasti), kde se nachází aktiva.

(3) Zařazení do kategorií tříd zabezpečených oblastí a bezpečnostní parametry jednotlivých zabezpečených oblastí řeší směrnice SM-5/2013 Ochrana informací.

(4) Tabulka tříd zabezpečení:

Třída zabezpečené oblasti	Podmínka zařazení dle kategorie a množství ukládaných chráněných informací bez nutnosti ochrany informací šifrováním
TZO 1	Centrální zpracování chráněných a interních informací, jedná se především o datové sály v perimetru datového centra.
TZO 2	Decentralizované zpracování chráněných a interních informací v rámci vybraných prvků ČP a kritické informační infrastruktury (KII). Jedná se především o serverovny pošt zařazených v KII, dále pak o Regionální zpracování platebního styku, HP (Hybridní pošta), a mezinárodní pošta.
TZO 3	Decentralizované zpracování chráněných a interních informací. Jedná se především o serverovny pošt mimo KII, serverovny v lokalitách, kanceláře s vyšší mírou zabezpečení.
TZO 4	Lokální zpracování informací. Jedná se především o přepážky pošt, standardní kanceláře a další neveřejné prostory.

5.1. Zabezpečení kanceláří, místností a zařízení

(1) Zaměstnanci musí být seznámeni s pravidly fyzického zabezpečení svých kanceláří a s nimi souvisejících budov ČP uvedenými v bezpečnostním projektu na ochranu objektů se zařízením ICT ČP.

(2) Zaměstnanci musí být dále poučeni se zásadami při zacházení s klíči a kódy, o nesdělitelnosti těchto informací dalším osobám a odpovědnosti za zneužití přístupu.

(3) O vydávání klíčů a bezpečnostních kódů pro vstup do objektů a místností musí být vedena evidence bezpečnostní agenturou nebo organizační jednotkou odpovědnou za bezpečný provoz objektu.

5.2. Ochrana před hrozbami vnějšího prostředí

(1) Při řešení fyzické bezpečnosti musí být brány do úvahy i bezpečnostní hrozby okolí, jako jsou například požár v sousední budově, vytopení vodou z jiné oblasti, letecké koridory, seismologické oblasti, výbuch a přírodní katastrofy.

(2) Nebezpečné a hořlavé materiály musí být uchovávány v dostatečné vzdálenosti od zabezpečené oblasti. V zabezpečené oblasti nesmí být přechovávány velké zásoby provozního materiálu.

(3) Záložní zařízení a zálohovací média nesmí být uchovávány v oblasti, kde se zpracovávají primární informace, ale v zabezpečené oblasti v jiném objektu v dostatečné vzdálenosti.

(4) Hasicí zařízení musí být vhodně rozmístěno i mimo zabezpečené oblasti.

5.3. Práce v zabezpečených oblastech

(1) Kromě bezpečnostního, systémového nebo aplikačního administrátora s oprávněním vstupu do TZO 1 a TZO 2 je dalším osobám povolen vstup pouze na základě souhlasu vlastníka aktiv, správce aktiva nebo jim pověřeného pracovníka, a to pouze za stálé přítomnosti některé z povolaných osob.

(2) Tato opatření se týkají i úklidových prací, údržby a ICT podpory a služeb externích subjektů v těchto zabezpečených oblastech.

(3) Podrobná pravidla a způsoby ochrany jsou dále specifikovány v provozních řádech daného pracoviště (Režimová nebo provozní směrnice zabezpečené oblasti).

(4) Práci v zabezpečené oblasti TZO 3 (např. práce uživatele v kanceláři) schvaluje nadřízený zaměstnance v rámci dislokace jemu přidělených prostorů a jeho kompetencí vyplývajících z řádu ŘA-1/2020 Organizační řád.

5.4. Bezpečnost zařízení

5.4.1. Kontrola vstupu osob, veřejný přístup

(1) Vstup návštěv musí být zaznamenán (např. do knihy Návštěv zabezpečené oblasti) a návštěva musí být v TZO1 a TZO2 pod stálým dohledem. Návštěvu schvaluje vlastník aktiv nebo správce aktiv nebo jím pověřený pracovník. Výjimky schvaluje Gestor bezpečnosti nebo Bezpečnostní manažer ICT.

(2) Je zakázáno, aby návštěva kdykoliv a jakkoliv používala aktiva. Výjimky se týkají pouze servisních zaměstnanců externích subjektů a jsou udělovány pouze na základě předchozího povolení k zásahu správcem aktiva, ovšem vždy musí být doprovázeny oprávněným pracovníkem.

5.4.2. Umístění zařízení a jeho ochrana

(1) K ochraně před poškozením, krádeží nebo kompromitací aktiv musí být aktiva umístěna (uložena) do zabezpečené oblasti podle klasifikace zpracovávaných informací.

(2) Jsou-li informační aktiva chráněna schváleným šifrovacím algoritmem, nemusí být umístěna v zabezpečené oblasti. Nadále však platí povinnost chránit aktiva před poškozením a krádeží.

5.4.3. Podpůrná zařízení a klimatizace

(1) Aktiva musí být v TZO 2 a TZO 1 zabezpečena před poklesem, kolísáním či výpadkem elektrické energie samostatným náhradním zdrojem (aktivní UPS) a dále v TZO 1 musí být zabezpečena a v TZO 2 mohou být zabezpečena náhradním zdrojem energie, který představuje záložní motorgenerátor.

(2) UPS umožní po potřebnou dobu překlenout krátkodobý výpadek v dodávkách elektřiny, případně dostatečný čas pro bezpečné uložení dat a korektní ukončení činnosti aktiv při výpadku primárního zdroje elektrické energie do provozního připojení záložního motorgenerátoru.

(3) Pokud není zabezpečená oblast vybavena motorgenerátorem, musí být nastaveny technické parametry aktiv pro korektní ukončení jejich činnosti.

(4) K zajištění provozních podmínek aktiv stanovených výrobcem musí být datová centra vybavena klimatizací.

5.4.4. Ochrana kabelových rozvodů

(1) Struktura kabeláže spolu s její topologií musí být řádně zdokumentována a tato dokumentace musí být udržována v aktuálním stavu.

(2) Kabeláž musí být dostatečně chráněna proti fyzickému poškození nebo zneužití (např. nežádoucí odposlech).

(3) V případě, kdy jsou rozvody vedeny přes území vně ČP nebo jsou umístěny v místech veřejně dostupných, musí být zavedena další fyzická opatření pro ochranu vedení a rozvodových zařízení ve formě skrytí kabeláže pod omítku, uložení vodičů do pancéřových trubek nebo uzamčení rozvodných zařízení.

5.4.5. Údržba zařízení

(1) Fyzická aktiva musí být zabezpečena ochrannými kryty, umístěna v rackcích nebo jinak fyzicky zajištěna proti nežádoucí manipulaci. Tyto činnosti jsou plně v kompetenci správce fyzického aktiva nebo jim pověřeného pracovníka, kteří jsou oprávněni provádět údržbu a zásahy na těchto aktivech.

(2) Povrchové čištění fyzických aktiv je povoleno pouze předepsaným způsobem, přičemž jsou uživatelé povinni se starat o svěřená fyzická aktiva tak, aby nedošlo k jejich zneužití nebo poškození.

5.4.6. Bezpečnost zařízení mimo prostory ČP

(1) Použití aktiv mimo prostory ČP musí být bez ohledu na jejich vlastníka schváleny Bezpečnostním manažerem ICT.

(2) Toto opatření se netýká mobilních zařízení ICT.

5.4.7. Bezpečná likvidace nebo opakované použití zařízení

(1) Aktiva obsahující paměťová média musí být před likvidací nebo opakovaným použitím kontrolována, zda neobsahují chráněné informace nebo licencované programové vybavení.

(2) Chráněné informace musí být po uplynutí skartační lhůty zničeny fyzicky (např. mechanické zničení paměťového média) nebo bezpečně smazány přepsáním dat znemožňující jejich obnovu. Použitý SW a metodický postup stanovuje a schvaluje Bezpečnostní manažer ICT.

5.4.8. Přemístění zařízení

(1) Zařízení nesmí být bez předchozího schválení vlastníkem nebo správcem aktiva uživatelem přemísťováno mimo určené prostory. O přemístění musí být proveden záznam.

6. Řízení komunikací a provozu

6.1. Provozní postupy a odpovědnosti

6.1.1. Dokumentace provozních postupů

(1) Všechny provozní postupy zmíněné v bezpečnostních politikách a spojené se správou aktiv musí být dokumentovány a udržovány. Tyto postupy musí být dostupné pro příslušné role a musí být s nimi nakládáno jako s formálními dokumenty, které podléhají změnovému řízení.

(2) Provozní postupy, obsažené v dokumentaci, musí být alespoň jedenkrát za 12 měsíců prokazatelně zkontrolovány, zda odpovídají aktuálnímu stavu ICT ČP. Vyhodnocení vlivu změn na provozní postupy musí být také součástí změnového řízení provozní dokumentace.

(3) Za zdokumentování, aktuálnost a správnost provozní dokumentace je odpovědný vlastník nebo správce aktiv dané části ICT ČP.

6.1.1.1. Provozní dokumentace ICT ČP

(1) Provozní dokumentace se musí skládat z následujících dokumentů:

a) uživatelská provozní dokumentace,

b) administrátorská provozní dokumentace (postupy pro nastavení systému, systém zálohování, způsob údržby, postupy pro správu prostředí, provozní a administrátorské deníky),

c) režimová směrnice pracoviště (ve smyslu objektu nebo jeho části),

d) provozní deník pracoviště (respektive provozované části ICT ČP),

e) plány údržby,

f) plány obnovy ICT (DRP).

(2) Režimová nebo provozní směrnice pracoviště musí stanovit pravidla pro práci na daném pracovišti. Minimálně musí obsahovat:

a) definici účelu,

b) rozsah a platnost,

c) popis zabezpečení pracoviště,

d) pravidla pro vnesení, uložení, vynesení materiálů a informací,

e) pravidla pro vstup a pohyb osob,

f) základní pracovní postupy a dokumentace,

g) typy a rozsah kontrol,

h) pravidla pro manipulace s klíči a pečetí,

i) pravidla pro ukládání a likvidace nosičů informací,

6.1.2. Oddělení povinností

(1) Pro zamezení možnosti zneužití aktiv musí být bezpečnostní, projektové a provozní role odděleny a vykonávány různými zaměstnanci ČP.

(2) Pro všechny role v rámci užívání aktiv platí zásada „potřebuje znát“ (need to know). Za oddělení jednotlivých povinností a odpovědností odpovídá vlastník aktiv dané části ICT ČP.

6.1.3. Oddělení vývoje, testování a provozu

(1) Testovací prostředí musí být bezpečně odděleno od ostrého provozu. Testovací data na produkčním prostředí musí být bezpečně zlikvidována před uvedením do ostrého provozu. To platí pro dodavatelská řešení i pro vývoj systémů, programového vybavení a utilit vlastními silami ČP.

(2) Testování jednotlivých stávajících nebo nových částí ICT ČP musí probíhat podle schválených testovacích scénářů. Bezpečnostní testovací scénáře schvaluje Bezpečnostní manažer ICT, provozní scénáře schvaluje správce aktiv a scénáře ověřující funkcionalitu aplikace schvaluje její garant/vlastník.

(3) K zajištění ochrany klasifikovaných informací při přenosu nebo ukládání musí být použity schválené šifrovací prostředky s důvěryhodným klíčovým hospodářstvím. Jsou-li pro testování používána testovací data shromážděná nebo vytvářená z ostrých provozních dat, musí být s daty v testovacím prostředí

nakládáno tak, aby nedošlo ke zneužití či úniku těchto dat. Citlivá data vytvořená z ostrých provozních dat je nutno pro potřeby testování anonymizovat.

(4) Na akceptačním testování se nesmí podílet zaměstnanec ČP obsazený do role řešitele testované části ICT ČP.

(5) Vývoj a testování nesmí z technologického pohledu probíhat v provozním prostředí (příklad: testovaná aplikace nesmí být testována v rámci jednoho OS virtuálního serveru jako produkční aplikace, ale může využívat infrastrukturu virtuálního prostředí pro produkční aplikace jako je síťová infrastruktura, virtuální prostředí Solaris/VMware/Hyper-V/IBM AIX). Výjimky schvaluje Bezpečnostní manažer ICT.

(6) Před nasazením testované části ICT ČP do provozního prostředí musí proběhnout akceptační řízení, o jehož výsledku se pořídí dokumentovaný záznam.

(7) Pracovníci vývoje (řešitelé) nesmí mít do ICT ČP jiný přístup, než jaký je definovaný v projektové a provozní dokumentaci pro danou část ICT ČP. Správa tohoto přístupu musí být řízena standardními provozními postupy.

(8) V mimořádné provozní situaci (havárie, diagnostika závažné poruchy) je možné přidělit na nezbytně nutnou dobu nadstandardní přístup a oprávnění k dané provozní části ICT ČP řešiteli. Generický postup pro případ mimořádné provozní situace stanovuje a schvaluje Bezpečnostní manažer ICT a vlastník aktiv. Situace musí být evidována. Problematiku detailně řeší MP-2/2017 Zvládání bezpečnostních incidentů.

6.2. Řízení dodávek externích subjektů

6.2.1. Dodávky služeb

(1) Dodávky služeb, které mohou ovlivnit bezpečnost a úroveň poskytovaných služeb ICT ČP, musí být kontrolovány. Musí být prověřováno, zda jsou implementovány, provozovány a udržovány ve shodě s uzavřeným smluvním ujednáním. Odpovídá vedoucí organizačního celku ČP, v jehož gesci je externí subjekt smluvně vázán.

(2) V případě dodání služeb zasahujících bezprostředně do provozního prostředí, musí být externím subjektem doložen plán zajištění kontinuity pro případ selhání poskytovaných služeb nebo pro případ krizové události.

6.2.2. Dohoda o mlčenlivosti

(1) Povinnost mlčenlivosti externích subjektů, kteří při plnění pracovních povinností, poskytování služeb či prací mohou přijít do styku s chráněnými informacemi, musí být uplatňována prostřednictvím dohod o mlčenlivosti (NDA – Non disclosure agreement).

(2) Stávající platné smlouvy, které dohodu o mlčenlivosti neobsahují, musí podléhat kontrole na existenci tohoto ustanovení formou revize, případně zajištěním doplnění dodatku s tímto ujednáním podepsaného oprávněným zaměstnancem či zástupcem externího subjektu. Tato dohoda musí být platná i po ukončení smluvního ujednání.

(3) Za splnění uvedených požadavků odpovídá vedoucí organizační jednotky ČP, v jehož gesci je externí subjekt smluvně vázán.

6.2.3. Monitorování a přezkoumávání služeb

(1) Služby poskytované externím subjektem musí být ze strany ČP pravidelně monitorovány a musí být určena osoba nebo tým odpovědný za dodržení souladu smluvního ujednání s poskytováním služby.

(2) Odpovědným za určení osoby nebo týmu je ten, kdo je ve smlouvě uveden nebo kdo dodání služby požadoval.

6.2.4. Řízení změn služeb

(1) Změny v poskytování služeb (nové technologie, aplikace, zařízení, ale i změna bezpečnostních politik, způsobu hlášení bezpečnostních incidentů atd.) musí být řízeny, dokumentovány a schváleny (např. v dodatku smlouvy).

(2) Současně se změnami musí být neprodleně aktualizována i související smlouva uzavřená s externím subjektem tak, aby obsahovala vždy aktuální informace.

(3) Za řízení změn služeb je odpovědný vedoucí organizační celku ČP, v jehož gesci je externí subjekt smluvně vázán.

6.3. Plánování a přejímání ICT

6.3.1. Řízení kapacit

(1) Správcem aktiva musí být zajištěno sledování stávajících kapacit systémů ICT ČP formou monitorování výpočetního výkonu, využití diskových prostorů, propustnosti komunikační infrastruktury apod.

(2) Před nasazením nové části ICT ČP musí být zajištěna kapacita na zabezpečení jeho provozu, případně podpory externími subjekty.

(3) Řízení kapacit musí být prováděno také v rámci projektového řízení jednotlivých projektů ICT ČP v souladu se směrnicí SM-3/2019 Projektové řízení a řízení projektového portfolia, které je v odpovědnosti určeného projektového manažera.

6.3.2. Přejímání systémů

(1) V případě zavádění jednotlivých částí ICT ČP do provozu musí být zpracovatelem provozní nebo projektové dokumentaci stanovena jednoznačná přejímací kritéria, která musí být otestována, zdokumentována a schválena.

(2) Předtím, než je provedeno převzetí, musí být:

a) splněn požadavek systému na provozní prostředí, jako je výpočetní a paměťový výkon, datové úložiště, datová propustnost, napájení, chlazení atd.,

b) stanoveny postupy pro zotavení z chyb, restartů, atd.,

c) specifikována sada přijatých bezpečnostních opatření,

d) zpracován plán obnovy,

e) provedeno školení administrátorů v obsluze a použití.

6.4. Ochrana proti škodlivému programu a mobilním kódům

6.4.1. Antivirová ochrana

(1) Antivirová ochrana musí být zaměřena na odstranění nebo alespoň snížení rizika napadení škodlivým softwarem a mobilním kódem, pod nímž jsou zahrnuty počítačové viry a škodlivé kódy na internetu (Malware, Java skripty, ActiveX objekty apod.).

(2) Infrastruktura ICT ČP je chráněna softwarem pro antivirovou kontrolu:

a) pracovních stanic,

b) serverů,

c) internetového provozu,

d) mail-serverů.

(3) Bezpečnostním manažerem ICT musí být pro ICT zpracována pravidla a zásady antivirové ochrany. Za jejich implementaci odpovídá správce softwarového aktiva antivirové ochrany.

6.5. Zálohování

(1) Pro případy jakéhokoli poškození, ztráty informací či nenadálé havárie mající dopad na integritu a dostupnost informací ICT ČP musí být prováděno jejich zálohování v závislosti na hodnotě aktiva.

(2) Zálohování informací ICT ČP u centrálního ukládání informací musí být řešeno centrálně. Z důvodu obnovitelnosti informací a zachování kontinuity provozu ICT ČP se veškeré zálohy dat musí provádět pravidelně v potřebných intervalech a kopiích. Jedna kopie záloh za určené období musí být uložena mimo budovu ČP, ve které se daná část ICT ČP nachází.

(3) Způsob, rozsah a frekvence centrálního zálohování informací musí být stanovena řešitelem na základě požadavku vlastníka aktiv a zdokumentována správcem aktiv pro jednotlivé části ICT ČP v jejich provozní dokumentaci.

(4) Zálohy jsou nedílnou součástí plánů obnovy ICT, kde musí být zpracovány postupy pro obnovu funkčnosti dané části ICT ČP.

6.5.1. Ukládání, evidence a označování záloh

(1) Všechny vytvářené zálohy musí být ukládány v zabezpečené oblasti a v souladu se stupněm klasifikace informací. Nesmí být vytvářeny žádné další neschválené nebo neevidované kopie.

(2) Za evidenci záloh, způsobu zabezpečení včetně zachování kompatibility programů schopných zálohy obnovit (rozšifrovat atd.) odpovídá zaměstnanec ČP pověřený správcem aktiv.

(3) Každá záloha musí být označena a zaevidována včetně všech potřebných a požadovaných údajů (kdo provedl zálohu, co obsahuje záložní médium, datum vytvoření, datum uložení, expiraci atd.). Náležitosti označování záloh jsou důležité pro pozdější použití v souvislosti s plánem obnovy ICT ČP.

6.5.2. Zálohy SW vybavení a instalačních médií

(1) Pokud to systémy umožňují, musí být pro potřeby obnovy operačních systémů a aplikací vytvořeny zálohy operačních systémů a aplikací provozovaných ve všech částech ICT ČP.

(2) Pro snadnější a zejména rychlejší obnovu prostředků ICT musí být provedena i záloha konfigurace jednotlivých standardizovaných instalací.

(3) Zálohy SW musí být vytvářeny ve dvou záložních kopií, z nichž jedna (provozní záloha) je uložena na bezpečném místě pro provozní potřeby a druhá je uložena na bezpečném místě mimo budovu (pro případ poškození provozní zálohy).

(4) Za aktuální stav záloh odpovídá správcem aktiva pověřený zaměstnanec ČP.

6.5.3. Zálohy souborových nebo databázových serverů

(1) Zálohování souborových nebo databázových serverů se musí provádět za účelem pravidelného vytváření záloh celého systému, tj. serverů nebo jednotlivých diskových svazků (adresářů, souborů), včetně přístupových práv.

(2) Způsob, rozsah a frekvence centrálního zálohování informací musí být stanovena řešitelem na základě požadavku vlastníka aktiv a zdokumentována správcem aktiv pro jednotlivé části ICT ČP v jejich provozní dokumentaci.

6.5.4. Obnova ze záloh

(1) Musí být ověřována použitelnost záloh a prováděno testování čitelnosti záložních médií a obnovitelnosti dat ve stanovených termínech, které určuje vlastník aktiva.

(2) Testování a ověřování použitelnosti záloh je v odpovědnosti správcem aktiv pověřených zaměstnanců ČP.

6.6. Správa bezpečnosti sítě

(1) K ověřování provozu, detekci neobvyklých událostí, pokusů o průnik a identifikaci bezpečnostních incidentů ICT ČP slouží kontrolní provozní záznamy (log soubory, případně ruční záznamy). Za evidenci a kontrolu provozních záznamů odpovídá pracovník pověřený správcem aktiv.

(2) Bezpečnost přenosu dat v počítačové síti zajišťují kontrolní, monitorovací a bezpečnostní aktivní prvky ICT ČP. Správa provozu počítačové sítě je v kompetenci správce příslušného aktiva.

6.6.1. Síťová opatření

(1) V síťovém prostředí musí být zajištěna bezpečnost sdílených dat a přístup k nim pouze oprávněným uživatelům a v určeném rozsahu.

(2) Správa sítě musí zajistit důvěrnost, integritu a dostupnost informací podle stupně jejich klasifikace při přenosu sítí, zabezpečení přístupu zvenčí, zálohování síťových konfigurací, zaznamenávání a monitorování provozu a událostí souvisejících s bezpečností apod.

(3) Za provoz sítě zodpovídá správce příslušného aktiva.

6.6.2. Bezpečnost síťových služeb

(1) Bezpečnost síťových služeb musí zahrnovat zajištění připojení, služby datové sítě ČP a správu bezpečnostních řešení (firewally, vstupní brány, koncové routery, IDS (Intrusion Detection System), IPS (Intrusion Prevention System)). Bezpečnost síťových služeb musí být správcem aktiva ve spolupráci s útvarem bezpečnost zajištěna i v případě, kdy jsou tyto služby zajišťovány prostřednictvím externího subdodavatele (outsourcing).

(2) Pro zajištění bezpečnosti síťových služeb musí být použity postupy a technologie omezující přístup k síťovým službám a aplikacím (metody autentizace, šifrování a kontroly síťových připojení).

6.7. Bezpečnost při zacházení s médii

6.7.1. Správa vyměnitelných počítačových médií a tištěných dokumentů

Všechna média s informacemi v elektronické podobě a tištěné dokumenty musí být ukládány v souladu se směrnicí SM-5/2013 Ochrana informací.

6.7.2. Likvidace médií

6.7.2.1. Bezpečná likvidace informací

(1) Klasifikované dokumenty v listinné podobě musí být likvidovány (skartovány) předepsaným způsobem tak, aby nebylo možné zpětně obnovit jejich obsah. V rámci ČP řeší skartaci řád ŘA-3/2010 Spisový řád.

Pro likvidaci dokumentů v elektronické podobě musí být použity postupy, které znemožní obnovit informace z příslušného nosiče. K spolehlivému zrušení/likvidaci informací mohou být speciální softwarové a hardwarové produkty, které musí být schváleny Bezpečnostním manažerem ICT, nosiče dokumentů v elektronické podobě z aktiv, která jsou zařazena jako KII nebo VIS, musí být likvidována dle směrnice SM-5/2013 Ochrana informací.

6.7.2.2. Ochrana informací

(1) Při dlouhodobém ukládání informací v elektronické podobě musí být zajištěna čitelnost informací i po delší době včetně uchování technického zařízení a technologií kompatibilní s nosičem zálohovaných informací.

(2) Přístup k informacím (dokumentům) chráněných šifrovacím programem musí být zabezpečen i v případě provádění dlouhodobých záloh.

6.7.2.3. Uložení informací

Informace musí být uloženy v odpovídajících zabezpečených oblastech podle klasifikace informací:

- kategorie informací Interní se ukládají minimálně v zabezpečené oblasti TZO 3,
- kategorie informací Chráněné informace (Důvěrné, Obchodní tajemství, Osobní údaje, Zvláštní kategorie osobních údajů) se ukládají v zabezpečené oblasti TZO 2 nebo TZO1.

6.7.3. Bezpečnost systémové dokumentace

(1) Systémovou dokumentací se rozumí Technologický návrh, Technický návrh, Programátorská dokumentace a Administrátorská provozní dokumentace.

(2) Veškerá systémová dokumentace musí být zpracovávána, přezkoumávána a aktualizována průběžně v souladu s rozvojem ICT ČP.

(3) Systémová dokumentace musí být chráněna proti neoprávněnému přístupu a způsob ochrany stanovuje vlastník aktiva.

6.8. Výměna informací

6.8.1. Postupy při výměně informací

Komunikační prostředky, prostřednictvím kterých dochází k výměně chráněných informací mezi ČP a externími subjekty musí být zabezpečeny tak, aby nemohlo dojít k úniku (zachycením, odposlouchávánim, zkopírováním) nebo k modifikaci informací.

6.8.2. Dohody o výměně informací a programů

(3) Výměna informací mezi ČP a externími subjekty musí být v souladu s platnou zákonnou legislativou upravující vztah mezi ČP a externím subjektem nebo upravena smluvním ujednáním.

(4) V případě výměny informací s externími subjekty je nutné vzít v úvahu požadavky stanovené v kapitole 2.4.3. a navíc do smluvního ujednání zapracovat:

- stanovení odpovědnosti vedoucích zaměstnanců týkající se kontroly a potvrzení přenosu, oznámení odesílateli, odeslání a přijetí,
- postupy pro zajištění nepopiratelnosti doručení,
- dodržování autorských práv.

6.8.3. Bezpečnost při přepravě médií

(1) Při přepravě mezi lokalitami musí být aplikována následující opatření:

- používat spolehlivé způsoby dopravy, spolehlivých osob (kurýrů) s ověřením jejich identity,
- používat pevné obaly zabraňující fyzickému poškození médií.

(2) Za zajištění výše uvedených požadavků odpovídá odesílatel média s chráněnými informacemi.

6.8.4. Elektronické zasílání zpráv, (e-mail, chat)

(1) Bezpečnost při elektronickém zasílání zpráv se řídí směrnicí SM-5/2013 Ochrana informací.

(2) V případě požadavku na zajištění ochrany e-mailem přenášených zpráv šifrováním, musí být použity pouze schválené šifrovací mechanizmy (viz příloha č. 1 této Politiky).

6.9. Monitorování provozu

6.9.1. Pořizování auditních záznamů (logů)

6.9.1.1. Sledování logů

(1) Auditní záznamy musí být sledovány, pořizovány a uchovávány a archivovány (musí být uloženy na zabezpečeném úložišti; to může být na jiném povoleném zařízení nebo úložišti, podle povahy logu), aby se daly použít pro účel monitorování řízení přístupu k systému.

(2) Bezpečnostní manažer ICT ve spolupráci se správcem aktiv musí určit pravidla a povinnosti pro nepřetržité:

- sledování provozu sítě,
- udržování přehledu o přístupu uživatelů k ICT ČP,
- zjišťování možných hrozeb a zranitelností,
- identifikování bezpečnostních incidentů a narušení bezpečnosti,
- dodržování zásad pro bezpečné uchovávání logů ICT ČP a přístup k nim pro pozdější vyhodnocení v případě potřeby
- dobu uložení logů.

6.9.1.2. Vytváření logů

(1) Pokud to systémy umožňují, nebo pokud je tak požadováno na základě platných právních předpisů, musí logy protokolovat takové události, aby v případě bezpečnostního incidentu bylo z těchto událostí zřejmé, co tento incident zapříčinilo. Mechanizmy vytváření a ukládání logů musí být navrženy tak, aby nemohlo dojít ke ztrátě jejich dostupnosti, integrity a důvěrnosti.

(2) Logy ICT ČP musí (pokud to technologie umožňuje, resp. platný právní předpis vyžaduje), obsahovat informace o následujících událostech:

- čas a datum spuštění a správné ukončení činnosti daného ICT ČP,
- jednoznačný identifikátor daného ICT ČP,
- jednoznačný identifikátor původce činnosti, která je logována,
- varovná nebo chybová hlášení,
- změny nastavení logování,
- pokus o výmaz logů,
- export logů,
- pokus o neoprávněné přihlášení uživatele,
- odhlášení uživatele,
- změna autentizačního tajemství,
- změna kontextu uživatele (např. příkaz su),
- změna nastavení kontroly přístupu,
- změna nastavení rolí a skupin rolí,
- odmítnutí akce jako důsledek nedostatku práv.

(3) Logy musí obsahovat následující identifikační informace:

- typ události (chyba, varování, informační),
- přesný čas,
- ID zaznamenávajícího systému,

- ID logované události.

(4) Jakékoli výjimky, rozšíření či upravení rozsahu parametrů logování schvaluje Bezpečnostní manažer ICT ČP.

(5) V případě, že logy obsahují OÚ musí se tyto logy řídit zároveň požadavky GDPR. Tyto požadavky definuje u jednotlivých aktiv jejich garant ve spolupráci s Pověřencem GDPR a dalšími věcně příslušnými odbornými organizačními jednotkami.

6.9.2. Monitorování používání systémů

(1) U jednotlivých částí ICT ČP musí být minimálně monitorovány následující parametry:

- funkčnost HW,
- vytížení zdrojů systému (paměť, kondice a kapacita disků, procesor, vstupní a výstupní zařízení, …),
- stav procesů aplikačního SW,
- stav služby systému (aplikace jako celku),
- stav operačního systému.

(2) Za zajištění monitorování používání systémů odpovídá Správce aktiva.

6.9.2.1. Kontrola logů

Kontrola logů musí probíhat pravidelně, a to minimálně:

- jednou denně u aktiv zpracovávající Chráněné informace (v datových centrech) a u aktiv jednotlivých částí ICT ČP přímo přístupných z externích sítí,
- jednou týdně u aktiv ostatních částí ICT ČP.

6.9.2.2. Bezpečnostní monitorování

(1) K zabezpečení monitorování aktiv musí být nastaven systém sběru a vyhodnocení záznamů událostí (logů).

(2) Pro všechna aktiva zpracovávající informace klasifikované jako Důvěrné nebo Obchodní tajemství platí vše jako pro vytváření standardních logů a dále:

- na aktivech ICT ČP musí být instalován SW nabízející mechanizmy kontroly přístupu a jeho záznamu do logu,
- minimálně jednou za 48 hodin musí být logy tvořené systémem vyhodnoceny a zálohovány,
- minimálně jednou za 48 hodin musí být na systému provedena kontrola integrity a autenticity SW a konfigurace systému a o výsledku této kontroly proveden záznam.

(3) Pro všechna aktiva zpracovávající informace klasifikované jako Osobní údaje nebo Zvláštní kategorie osobních údajů platí vše jako pro informace Důvěrné a Obchodní tajemství a dále:

- minimálně jednou za 24 hodin musí být logy tvořené systémem vyhodnoceny a zálohovány,

(4) Systém sběru a vyhodnocení záznamů událostí (logů) musí být definován a nastaven pro všechna zařízení komunikační infrastruktury ICT ČP.

6.9.3. Ochrana logů ICT

(1) Přístup k logům (auditním záznamům) musí být omezen výhradně na příslušného bezpečnostního administrátora a osobu provádějící kontrolu bezpečnostní shody (audit). Správce aktiva nebo jím pověřený zaměstnanec ČP nesmí modifikovat logy. Logy jednotlivých částí ICT ČP musí být chráněny z hlediska důvěrnosti a integrity.

(2) Logy musí být ukládány minimálně po dobu:

- 18 měsíců pro KII systémy
- 3 měsíce u aktiv zpracovávající interní informace, které nespadají pod ZoKB
- 1 rok u aktiv zpracovávající chráněné informace ,

(3) Logy musí být ukládány v elektronické formě a musí k nim být přiložen SW na jejich čtení a další zpracování.

(4) Doba ukládání logů při zpracování OÚ se určuje podle druhu zpracovávaných OÚ a druhu dalších obsažených informací (např. peněžní poukázka obsahuje OÚ, ale ukládá se na 10 let podle zákona o účetnictví).

6.9.4. Administrátorská a operátorská dokumentace

(1) Konfigurace všech významných služeb, programového vybavení, serverů, síťových prvků musí být administrátory zdokumentována. Dále musí být zdokumentovány všechny přístupové kódy a hesla pro administraci všech systémů. Zdokumentované informace musí být aktuální a bezpečně uloženy.

(2) Každá změna v konfiguraci se vždy musí posoudit z hlediska dopadu na jeho bezpečnost. Změny v konfiguraci se musí promítnout do všech relevantních dokumentů a procesů (např. do plánu obnovy ICT ČP, přijatých administrativních opatření a systémové dokumentace).

(3) Administrátoři jednotlivých částí ICT ČP musí o své činnosti vést záznamy formou provozního deníku. Tyto záznamy musí obsahovat:

- čas spuštění a zastavení systému,
- chyby systému a nápravné akce,
- akce definované v provozní dokumentaci systému,
- jednoznačná identifikace pracovníka, který záznam vytvořil.

6.9.5. Záznam selhání

(1) V rámci monitorování musí být zaznamenány a analyzovány chyby a přijata příslušná opatření. Zodpovídá správce příslušného aktiva.

(2) Pracoviště provádějící monitorování provozu ICT musí mít k dispozici informace o tom, kteří pracovníci nebo organizační jednotka mají být informováni v případě poruchy provozu systému ICT ČP.

(3) Udržování aktuálnosti tohoto seznamu musí být součástí personálních procedur pracoviště (při změně pracovního zařazení atd.). Za aktuálnost seznamu odpovídá správce aktiv.

6.9.6. Synchronizace času

(1) Všechny části ICT ČP, kde jsou zpracovávány chráněné informace, musí být časově synchronizovány.

(2) Službu synchronizace času zajišťuje definovaný interní ICT prvek ČP. Způsob synchronizace času schvaluje Bezpečnostní manažer ICT.

6.10. Pravidla a omezení pro provádění auditů bezpečnosti a bezpečnostních testů

(1) Bezpečnostní testy a audity smí být prováděny pouze s vědomím správců aktiv.

(2) Bezpečnostní testy a audity musí být prováděny nedestruktivním způsobem tak, aby neohrozily běžný provoz produkčních systémů.

7. Řízení přístupu

7.1. Požadavky na řízení přístupu

(1) Přístupová práva musí být přidělována na základě potřeby pro výkon pracovních činností a na základě individuálního přístupu tak, aby byla přidělena pouze minimální oprávnění nutná pro výkon pracovních povinností.

(2) Je preferováno řízení oprávnění pomocí rolí, tzn. aplikačních rolí a byznys rolí vázaných na pracovní činnosti a dostatečně srozumitelných pro garanty aktiv.

(3) Proces řízení přístupu musí být zajištěn formálními postupy pro přidělování uživatelských práv k jednotlivým částem ICT ČP. Tyto postupy musí pokrývat všechny fáze životního cyklu přístupu uživatele od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele. V případě přidělování privilegovaných přístupových oprávnění, která umožňují uživatelům překonat ochranná opatření v systému, musí být řízení těchto oprávnění věnována zvláštní pozornost. Takovéto postupy musí být stanoveny v provozní dokumentaci, kde musí být definovány zásady pro vytváření a rušení uživatelských účtů k příslušným komponentám.

(4) Informace o přidělených přístupových oprávnění musí být centrálně uloženy a za jejich aktuální stav odpovídá správce aktiv na základě stanovených požadavků garantů aktiv.

(5) Pravidelně musí být přezkoumáváno přidělení rolí a oprávnění (recertifikace) a o této kontrole musí být proveden záznam. Přezkoumání provádí vlastník aktiva nebo jím stanovený schvalovatel, ve spolupráci se správcem aktiva. Preferována je automatické provádění certifikačních kampaní v IDM.

7.2. Řízení přístupu uživatelů

7.2.1. Identifikace a autentizace uživatelů

(1) Každý přístup do systému musí být jednoznačně identifikován a autentizován před provedením libovolné akce. Každý, kdo přistupuje do systému, musí mít přidělenou jednoznačnou identifikaci (CPJM).

(2) Systémy musí vytvářet záznam o posledním přihlášení uživatele.

(3) Autentizace se provádí jedním z níže uvedených způsobů schváleným při návrhu ICT systému a odpovídající klasifikaci dat a prováděných operací:

- klíčem uloženým na čipové kartě nebo tokenu chráněné PINem,
- klíčem uloženým v zašifrovaném úložišti přístupném pouze po zadání hesla,
- heslem,
- ověřením biometrické informace uživatele,
- kombinací výše uvedených prostředků.

(4) Po deseti za sebou následujících neplatných pokusech o autentizaci musí být uživatelský účet zablokován. V případě použití funkce automatického odblokování účtu, musí být doba zablokování daného účtu minimálně 15 minut.

(5) Pro přístup do systému je zakázáno:

- sdílet uživatelskou identifikaci a autentizaci s jiným uživatelem,
- používat sdílenou nebo skupinovou uživatelskou autentizaci,
- umožnit někomu jinému použít jeho uživatelskou autentizaci,
- pracovat s použitím cizí uživatelské identifikace a autentizace,
- používat chybně přidělená oprávnění,

s následujícími výjimkami:

- je povoleno sdílení uživatele "root" (superuživatel) na systémech s OS Unix za podmínky, že systém nepovoluje přímé přihlášení pod uživatelem "root" a je možná pouze „vtělení“ s využitím příkazů "su" a "sudo",
- neodstranitelná sdílená identifikace a autentizace při přístupu do technologických e-mailových schránek.

7.2.2. Řízení privilegovaného přístupu

7.2.2.1. Přístupová práva

(1) Přístupová práva v aplikacích, operačních systémech a databázových systémech musí být přidělována podle rolí uvedených v dokumentaci ICT ČP, respektive systémové bezpečnostní dokumentaci jednotlivých částí ICT ČP.

(2) Pro každou část ICT ČP musí být v dokumentaci stanoven rozsah práv odpovídající jednotlivým rolím. Rozsah práv přístupu jednotlivých rolí k aktivům ICT musí být odsouhlasen vlastníkem aktiv.

(3) Přístupová práva mohou být uživateli správcem aktiv přidělena nebo odebrána pouze na základě písemného nebo prokazatelného elektronického schválení nadřízeného uživatele nebo garanta identity a schváleny příslušným vlastníkem informačních aktiv nebo jím pověřeným pracovníkem (schvalovatele role). Záznam o schvalování musí být uložen minimálně jeden rok. Preferovanou formou je žádost o roli v aplikaci IDM, případně v aplikaci ServiceDesk u rolí neřízených pomocí IDM.

(4) Při změně typové pozice nebo změně pracovních činností uživatele v ČP odpovídá za kontrolu revizi přiřazených rolí a přístupových oprávnění nový nadřízený uživatele.

(5) Pracovníci externích subjektů musí být evidováni k smluvnímu vztahu, který upravuje jejich povinnosti a definuje rozsah činností, ke kterým mohou být přidělena oprávnění.

(6) Pracovníkům externích subjektů a jejich smluvním partnerům nesmí být povolen přístup do perimetru ČP bez schválení prokazatelného schválení Bezpečnostního manažera ICT nebo jím pověřené osoby.

(7) O přidělení nebo odebrání práv musí být proveden automatizovaný záznam v rámci systému řízení identity ICT ČP nebo záznam do provozní dokumentace (provozního deníku).

(8) Při úplném zrušení práva uživatele používat systém nesmí být po definovanou dobu uživatelský účet smazán, ale pouze zamezeno přihlášení uživatele (zablokován účet) a zrušeno (změněno) přihlašovací heslo.

(9) Účet smí být smazán nejdříve po uplynutí jednoho roku od zablokování účtu. V odůvodněných případech může zkrácení této lhůty schválit Bezpečnostní manažer ICT.

(10) Účty, které nebyly používány po dobu delší než 1 rok, musí být zablokovány. Toto se nevztahuje na systémové účty, pod kterými běží softwarové služby.

(11) Nestandardní požadavky na přidělení oprávnění a privilegované přístupy s možným vysokým rizikem, schvaluje kromě garantů aktiv také Bezpečnostní manažer ICT nebo jím pověřená osoba.

7.2.2.2. Administrátorské a privilegované účty

(1) Zvláštním typem účtu je administrátorský nebo jiný privilegovaný účet (systémový administrátor, administrátor aplikací apod.), který umožňuje provádět zásahy do systému a nastavení.

(2) Použití tohoto typu účtu může mít zásadní vliv na bezpečnost ICT, proto je nutno všechny aktivity pod administrátorskými účty monitorovat a zásahy evidovat v provozní dokumentaci administrátora. Pokud je potřeba sdílet taková oprávnění mezi více administrátory, je nutno vytvořit samostatný účet jmenovitě pro každého administrátora, aby bylo možno změny v logu v jednotlivých částech ICT ČP identifikovat a zabránit anonymnímu přístupu či zásahům více administrátorů.

(3) Přezkoumání přístupových práv pro uživatele s privilegovaným přístupem provádí nadřízený zaměstnanec a Bezpečnostní manažer ICT, nebo jím pověřený zaměstnanec, minimálně jednou za rok. U necentrálních systémů se přezkoumání přístupových práv uživatele s privilegovaným přístupem provádí namátkově.

7.2.3. Správa uživatelských hesel

7.2.3.1. Autentizace heslem – politika hesel

(1) Heslo k administrátorskému účtu musí být dlouhé minimálně 17 znaků a musí být měněno alespoň jednou za 200 dní. Změněné heslo nesmí být shodné s minimálně 12 předchozími hesly. Tyto vlastnosti musí být vynucovány systémem.

(2) Heslo k účtu uživatele musí být dlouhé minimálně 12 znaků a musí být měněno alespoň jednou za 200 dní. Změněné heslo nesmí být shodné minimálně s 12 předchozími hesly. Tyto vlastnosti musí být vynucovány systémem.

(3) Povinnost změny hesla po 200 dnech se netýká účtů, které slouží pro běh softwarové služby nebo aplikace. Takový typ účtu se nesmí používat pro přihlášení fyzického uživatele nebo administrátora, a pokud je to možné, tak jeho délka musí být minimálně 17 znaků.

(4) K účtům typu "superuživatel", které nejsou nezbytně nutné pro provoz ICT ČP, musí být nastaveno dlouhé náhodné heslo o délce minimálně 17 znaků, které musí být uloženo v zapečetěné a neprůhledné obálce v úschovném objektu přístupném pouze oprávněným pracovníkům nebo jinou formou schválenou Bezpečnostním manažerem ICT.

(5) V případě použití čipových karet nebo USB tokenů musí být přístup k datům chráněn osobním identifikačním číslem PIN (Personal Identification number). PIN musí být minimálně devítimístné číslo a limitovaný počet možností zadání může být maximálně 10 pokusů. Podrobná specifikace musí být uvedena v systémových bezpečnostních politikách jednotlivých systémů ICT ČP.

(6) Systémy musí umožnit zadání hesla až 64 znaků dlouhá.

(7) Systém musí vždy umožnit, aby si uživatel heslo mohl bezpečně změnit.

(8) Pravidla tvorby bezpečných hesel a jejich použití musí být součástí školení pro uživatele i administrátory.

(9) Autentizační mechanizmus systému musí umožnit zadat v heslu malé písmeno, velké písmeno, číslici a k zvýšení kvality hesla je doporučeno použít i speciální znaky. V případě, kdy délka hesla z technických důvodů nemůže být minimálně 12 znaků, je použití 3 typů znaků (malé, velké písmeno, číslice) povinné,. Uživatelé nesmí volit snadno odvoditelná hesla například založené na údajích vztahujících se k uživateli nebo jeho příbuzným (jako jsou jméno, příjmení, datum narození, adresa, telefonní číslo) nebo označení organizační jednotky nebo mnohonásobně se opakující znaky (tři a více stejných), sekvence a podobně. Systém musí tyto požadavky v rozumné míře vynucovat.

(10) Heslo uživatele může být oprávněným uživatelem (např. ServiceDesk ČP) resetováno podle postupů schválených Bezpečnostním manažerem ICT. Zejména je požadována změna pouze na základě prokazatelné identifikace uživatele, předání bezpečným kanálem a předání pouze dotčené osobě nebo ve výjimečných zaevidovaných případech nadřízenému. Tato žádost na změnu/reset hesla musí být uložena a doba uložení musí být minimálně shodná s dobou uložení logů.

(11) Po resetu hesla nebo při jeho prvotním nastavení hesla musí být vynucena změna nově nastaveného hesla v okamžiku prvního přihlášení uživatele nebo musí být omezena jeho platnost maximálně do konce následujícího pracovního dne. Pokud tuto funkčnost systém neumožňuje, musí být tato povinnost stanovena v bezpečnostní příručce uživatele ICT ČP.

(12) Systém musí skrývat zadávaná hesla tak, aby je neoprávněné osoby nemohly odpozorovat.

(13) Hesla jsou v kategorií citlivá informace. Uživatel nesmí hesla sdílet ani jinak ohrozit jejich důvěrnost. Dále nesmí používat stejná hesla v interních systémech a mimo systémy, zejména na Internetu.

(14) Hesla v systémech ČP nesmí být uložena v čitelné formě, pokud nesplňují následující podmínky:

- dotčená část ICT ČP (daný server) musí být chráněna na úrovni fyzického přístupu (minimálně zabezpečená oblast TZO 2),

- veškerá oprávnění na soubor, který obsahuje v otevřené formě heslo, musí být omezena pouze na speciální účet určený pro danou aplikaci (nelze se na tento účet přihlásit – je určen pouze pro skripty, služby, démony atd.) a přístup s oprávněním superuživatele (administrátor),

- tento soubor musí podléhat kontrole přístupu – tj. logování veškerých typů přístupu na takový soubor.

(15) Hesla nesmí být součástí softwarového kódu.

(16) Za dodržování politiky hesel v jednotlivých částech ICT ČP v souladu se systémovou bezpečnostní politikou odpovídá správce aktiv.

7.3. Řízení přístupu k síti

7.3.1. Podmínky užívání síťových služeb

(1) V provozní dokumentaci jednotlivých částí ICT ČP musí být uvedeny síťové služby, ke kterým je povolen přístup a podmínky, případně kontrolní mechanismy, za kterých je tento přístup umožněn (podmínky, za kterých mohou uživatelé přistupovat k Internetu, způsob autorizace při použití síťových služeb, kdy je možné využít telefonní připojení k internetu apod.).

(2) Připojení k interním i externím síťovým službám může být správcem aktiv povoleno jen nezbytně nutným službám a portům specifikovaným v příslušných systémových bezpečnostních politikách, směrnicích nebo technické dokumentaci.

7.3.2. Autentizace uživatele externího připojení

(1) Uživatelem externího připojení je zaměstnanec ČP nebo pracovníci externího subjektu, kterým byl umožněn přístup k aktivům ICT ČP z externích sítí.

(2) Přístup externích (vzdálených) uživatelů musí být autentizován a evidován. Přístup ve spolupráci se specializovaným útvarem ICTB povoluje garant externího uživatele. Evidenci provádí správce aktiva, který přístup k aktivům ICT ČP z externích sítí fyzicky realizuje.

7.3.3. Identifikace zařízení v síti

K zajištění iniciace komunikace ze stanovené lokality nebo zařízení, musí být pro identifikaci zařízení, která se připojují ze vzdálených lokalit, použita autentizace.

7.3.4. Ochrana portů pro vzdálenou diagnostiku a konfiguraci

(1) Porty a služby, které nejsou pro činnost ICT ČP potřebné, musí být zakázány nebo odstraněny.

(2) V případě, že jsou pro správu a údržbu zařízení náležející do ICT ČP porty pro vzdálenou konfiguraci a diagnostiku využívány, musí být přístup k nim logicky i fyzicky bezpečně řízen. Tento přístup a technologii schvaluje Bezpečnostní manažer ICT.

7.3.5. Oddělení sítí

(1) ICT ČP nebo jednotlivé logické celky ICT ČP, jejichž alespoň jedna část je z hlediska klasifikace informací umístěna v zabezpečené oblasti TZO 1, respektive TZO 2, musí být provozovány na vlastní

VLAN. Komunikace mezi touto sítí a ostatními sítěmi, tedy i datová síť ČP, musí být řízena a oddělena síťovými prostředky.

(2) K zabezpečení síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení musí být použít firewall, který slouží jako kontrolní bod k definici pravidel komunikace mezi sítěmi, které od sebe odděluje.

(3) Filtrovací pravidla firewallu velmi přesně vymezují přístup na základě zdrojových a cílových IP adres. Komunikace mezi zdrojovými a cílovými IP adresami je pak bezpečně filtrována na základě portů služeb, které si mezi sebou zdrojové a cílové objekty poskytují. Tyto restrikce jsou aplikovány jak na provoz směřující do externích sítí a z externích sítí, tak i na provoz mezi jednotlivými segmenty privátní datové sítě ČP.

(4) Nastavení firewallu musí být zdokumentováno, pravidelně aktualizováno a bezpečně uloženo. Za formulaci filtrovacích pravidel odpovídá Bezpečnostní manažer ICT.

(5) V sítích ČP jsou implementovány bezpečnostní prvky IDS/IPS. Tyto prvky slouží k monitorování a blokování pokusů o průnik do infrastruktury datové sítě ČP a podezřelých aktivit uživatelů a služeb.

7.3.6. Řízení síťových spojení

Připojení uživatelů k sítím musí být časově omezeno. Konkrétní časové úseky spolu s dalšími případnými omezeními (filtrování provozu, omezení přenosu souborů, omezení přístupu k vybraným částem systému) musí být pro jednotlivé části ICT ČP definovány v jeho provozní dokumentaci.

7.3.7. Řízení směrování sítě

(1) K dodržování politiky přístupu musí být zavedeno řízení směrování sítě.

(2) Řízení směrování sítě musí být založeno na ověření zdrojové a cílové adresy, využívání proxy serverů a NAT (Network Address Translation) umístěných na branách interních i externích kontrolních bodů.

7.4. Řízení přístupu k operačnímu systému

7.4.1. Bezpečné postupy přihlášení

(1) Postup přihlášení k operačnímu systému musí být řešen tak, aby předcházel neautorizovanému přístupu.

(2) Přihlašovací postup musí:

- provést kontrolu autentizačních informací až v případě zadání kompletních vstupních dat,
- omezit počet povolených neúspěšných přihlašovacích pokusů na maximálně 10,
- nezobrazovat heslo v čitelné podobě ani ho posílat přes síť,
- omezit maximální dobu povolenou k přihlášení,
- nezobrazovat jakékoliv identifikátory systému nebo nápovědu před dokončením přihlášení (pokud to systém umožňuje),
- zobrazit varování, že přístup k ICT ČP má pouze oprávněný uživatel (pokud to systém umožňuje).

7.4.2. Identifikace a autentizace uživatelů

(1) Všichni uživatelé musí mít vytvořen jedinečný osobní identifikátor (CPJM). Tento princip platí i pro speciální uživatele např. administrátory, programátory a technické pracovníky. Speciální uživatel musí mít jedno uživatelské ID pro speciální činnosti (např. správu ICT) a další uživatelské ID k provádění činností běžného uživatele ICT ČP.

(2) Ve výjimečných případech může být použit sdílený uživatelský identifikátor pro skupinu uživatelů. Tyto případy schvaluje Bezpečnostní manažer ICT se zavedením dodatečných organizačních opatření.

(3) K ověření identity uživatele musí být použita odpovídající autentizace schválená v systémové politice systému. (kombinace hesla, klíčového páru na tokenu/čipové kartě případně biometrické technologie).

7.4.3. Použití systémových nástrojů

(1) Použití systémových nástrojů (speciální SW pro správu, kontrolu a údržbu ICT) je povoleno pouze uživatelům v roli administrátora a kontrolováno bezpečnostními administrátory. Neaktivní relace se musí po stanovené době nečinnosti ukončit.

(2) V operačních systémech mohou být instalovány pouze povolené softwarové nástroje a služby specifikované systémovou bezpečnostní politikou daného typu systému.

7.4.4. Časové omezení relace

(1) V ICT ČP musí být neaktivní relace po stanovené době nečinnosti ukončeny. Maximální doba nečinnosti je stanovena na 30 minut.

(2) Odchylky od tohoto časového omezení schvaluje Bezpečnostní manažer ICT ČP jako výjimku.

7.4.5. Časové omezení spojení

(1) Pokud systémy ICT ČP zpracovávají Chráněné informace a jsou zde požadovány časové úseky (intervaly), kdy uživatel nemá přistupovat, musí být vlastnost daného omezení časového spojení implementována.

(2) Konkrétní časová omezení pro jednotlivé části ICT ČP musí být specifikovány v jejich systémových bezpečnostních politikách nebo v provozní dokumentaci.

7.5. Řízení přístupu k aplikacím a informacím

7.5.1. Omezení přístupu k informacím

(1) Uživatelé mohou přistupovat k informacím a funkcím aplikačního systému pouze v souladu s politikou přístupových práv a povolenou úrovní přístupu stanovenou vlastníkem aktiv.

(2) Přístup k aplikacím a informacím musí být přidělován na základě rolí přidělovaným, schvalovaným a recertifikovaným na základě vykonávaných pracovních činností.

(3) Není-li možno oddělit přístup k informacím v rámci aplikace na úrovni rolí, je nutno přijmout organizační a monitorovací opatření k zajištění auditovatelnosti prováděných operací v aplikacích. Za návrh opatření odpovídá vlastník aktiva ve spolupráci se správcem aktiva a specializovaným útvarem ICTB.

7.5.2. Oddělení citlivých systémů

(1) Pokud jsou z hlediska klasifikace informací vlastníkem aktiv některé systémy ICT ČP stanoveny jako citlivé systémy (zpracovávají Chráněné informace), musí být toto zdokumentováno a stanoven způsob fyzického nebo logického oddělení od ostatních systémů.

(2) V případě provozování citlivých systémů ve sdíleném prostředí, musí být ostatní systémy, se kterými budou sdíleny zdroje, odsouhlaseny vlastníkem citlivého systému a sdílení zdrojů, musí být řízeno, zdokumentováno a monitorováno.

7.6. Mobilní zařízení a vzdálený přístup

7.6.1. Mobilní výpočetní zařízení

(1) K používání mobilních zařízení musí být v uživatelské bezpečnostní dokumentaci stanovena pravidla fyzické ochrany, kontroly přístupu, zálohování a antivirové ochrany. Dále zde musí být zahrnuty požadavky na bezpečné připojování k datovým sítím ČP a pravidla k použití těchto prostředků na veřejných místech.

(2) Mobilní výpočetní zařízení obsahující chráněné informace musí jejich uživatel nebo správce mobilního výpočetního zařízení zabezpečit proti neoprávněné manipulaci, zneužití nebo zcizení. Tam, kde je to technologicky možné, a jsou k dispozici šifrovací programy, musí být informace chráněny šifrováním. Šifrovací programy a způsob ochrany chráněných informací v mobilních výpočetních zařízeních schvaluje Bezpečnostní manažer ICT.

7.6.2. Vzdálený přístup

(1) Vzdálený přístup musí využívat zabezpečené spojení s využitím schválených šifrovacích algoritmů. Vzdálený přístup musí být chráněn dvoufaktorovou autentizací a je schvalován nadřízeným uživatele, specializovaným útvarem ICTB a je určen výhradně k pracovním účelům.

(2) Musí být zajištěna evidence všech zaměstnanců a externích subjektů, kteří mají umožněn vzdálený přístup.

8. Nákup (akvizice), vývoj a údržba

8.1. Bezpečnostní požadavky

(1) Pořízení nových prostředků pro zpracování informací schvalují vlastníci aktiv, kteří odpovídají za jejich rozvoj a údržbu. Součástí schvalovacího procesu musí být i stanovisko Bezpečnostního manažera ICT, aby se zajistilo, že nedojde k porušení ustanovení bezpečnostních politik ICT ČP.

(2) V případech, že je požadována kompatibilita s ostatními částmi ICT ČP, je nutno toto ověřit otestováním nebo smluvní garancí s dodavatelem.

(3) Všechny bezpečnostní požadavky musí být v rámci projektu stanoveny již ve fázi definice požadavků a musí být zdůvodněny, odsouhlaseny a dokumentovány jako součást vývoje ICT ČP dílčích částí.

(4) Bezpečnostní manažer ICT vyhodnocuje rizika související s nákupem (akvizicí), vývojem a údržbou ICT ČP.

(5) Při nákupu aktiv musí být ve smluvních ujednáních specifikovány požadavky na bezpečnost ICT. U aktiv, jejichž bezpečnostní funkce plně nesplňují specifikované požadavky na bezpečnost ICT, musí být ještě před nákupem zvážena opatření na pokrytí nově zavedeného rizika.

(6) Procesy vývoje aplikací musí plně respektovat bezpečnostní politiky ICT ČP a doporučení sdružení OWASP (Open Web Applications Secutity Project). Cílem je zajistit, aby členové vývojového týmu pracovali v souladu se systémovými bezpečnostními požadavky a poskytovali vlastníkům aplikací efektivní řešení bezpečnosti.

(7) Při vývoji se musí postupovat podle interních dokumentů ČP, jako jsou např. metodiky řízení projektů, metodiky programování, metodiky testování, atd.

8.1.1. Vývoj nových částí ICT ČP

(1) Nově vyvíjené části ICT ČP musí respektovat požadavky této Politiky a norem řady ISO/IEC 270xx.

(2) Vyvíjené části ICT ČP musí být navrženy tak, aby i v případě výskytu nestandardních situací nemohlo dojít k porušení bezpečnostních opatření a ohrožení ochrany informací.

(3) Do ICT ČP musí být implementováno pouze programové vybavení, které neobsahuje prokazatelné bezpečnostní zranitelnosti.

(4) Řešitelé nesmí implementovat programové vybavení, které rozšíří nebo omezí funkčnost systému nad vlastnosti popsané v aplikační dokumentaci. Jedná se zejména o instalaci skrytých přístupových cest pro obejití zabezpečovacích mechanizmů.

(5) Vyvíjené aplikace musí zajistit aby:

- v okamžiku, kdy se uživatel připojuje k ICT ČP, byl zobrazen varovný text, upozorňující na přístup k systému ČP. Znění textu schvaluje Bezpečnostní manažer ICT,
- text musel být potvrzen, aby mohl uživatel pracovat dále. Toto neplatí pro části ICT ČP určené zákazníkům ČP, které jsou přímo přístupné z externích sítí,
- při nečinnosti na interaktivním uživatelském rozhraní (terminál, pracovní stanice) s přihlášeným uživatelem byla v nastavené době uzamknuta nebo zrušena uživatelská relace. Odemčení, respektive obnovení této relace, musí být možné až po zadání autentizačního hesla,
- po přihlášení do ICT ČP byly uživateli zpřístupněny pouze služby, ke kterým má na základě svých přístupových oprávnění. Koncovým uživatelům musí být maximálně omezen přístup k příkazům a konfiguračním parametrům HW a SW aktiv.

8.1.2. Dokumentace

Dokumentace nové části ICT ČP se musí minimálně skládat z následujících dokumentů:

- technologického návrhu a technických návrhů,
- licenčního ujednání,
- programátorské dokumentace,
- administrátorské provozní dokumentace,
- uživatelské dokumentace,

- plánů obnovy ICT (DRP plány).

8.1.3. Akceptace a předání

(1) Na procesu testování a akceptace se musí podílet jak zástupci uživatelů, tak i zástupci správců aktiv.

(2) O předání nové části ICT ČP od řešitele do rutinního provozu musí být proveden písemný záznam schválený správcem aktiv.

(3) Na základě předávacího protokolu přebírá správce aktiva plnou odpovědnost za provoz nové části ICT ČP.

(4) Veškeré vyvíjené nové části ICT ČP nesmí být předány do rutinního provozu bez:

- otestování testery,
- bezpečnostního otestování (test zranitelností, test souladu s bezpečnostními požadavky, penetrační testy)
- akceptace,
- provozní dokumentace,
- písemného souhlasu vlastníka aktiva.

(5) Po předání do rutinního provozu musí být požadavky na změny řešeny v rámci zásad změnového řízení.

8.1.4. Zavádění do provozu

(1) Zavádění nových částí ICT ČP, jejich změn nebo nové verze musí být prováděno podle definovaných kritérií, která musí být jasně definována, odsouhlasena, jejich naplnění zdokumentováno a otestováno.

(2) Kritéria musí obsahovat požadavky na:

- výkon a zdroje,
- definování postupů pro řešení bezpečnostních a provozních incidentů (včetně zotavení) a vytvoření plánů obnovy ICT,
- plánování a provedení testů rutinních operačních postupů,
- definování množiny bezpečnostních kontrol,
- posouzení shody s požadavky na bezpečnostní politiky ČP,
- požadavky na pracovníky (včetně školení).

(3) Při instalaci nového programového vybavení musí být všichni předdefinovaní uživatelé nového programového vybavení zrušeni, nebo jim musí být změněny autentizační informace (např. hesla).

8.2. Správné zpracování dat v aplikacích

8.2.1. Kontrola vstupních dat

(1) U chráněných informací musí být prováděna kontrola vstupních dat, která musí minimálně zahrnovat testy na:

- hodnoty mimo rozsah,
- neplatné znaky v datových polích,
- chybějící nebo neúplná data,
- správnost kontrolních součtů.

(2) Výše uvedená kontrola musí být prováděna i v případě, kdy komunikují dvě části ICT ČP přes nechráněné prostředí.

8.2.2. Kontrola vnitřního zpracování

U Chráněných informací musí být implementována opatření pro detekci poškození nebo modifikace informací vzniklých při zpracování nebo úmyslnými zásahy.

8.2.3. Integrita zprávy

Integrita informací je v prostředí ICT ČP zajištěna používáním elektronického podpisu, případně jiných metod schválených Bezpečnostním manažerem ICT.

8.3. Ochrana informací šifrováním

8.3.1. Politika pro použití šifrovacích opatření

(1) Ochrana chráněných informací musí být zabezpečena bezpečnostními prvky v oblasti fyzické, programové, komunikační a personální bezpečnosti.

(2) Chráněné informace nesmí opustit prostředí ICT ČP v otevřené formě. K jejich ochraně jsou určeny šifrovací algoritmy uvedené v příloze.

(3) Způsob implementace šifrovacích prostředků a jejich provozní zajištění schvaluje Bezpečnostní manažer ICT.

8.3.2. Správa šifrovacích klíčů

(1) Šifrovací klíče musí mít stupeň klasifikace minimálně shodný se stupněm klasifikace informace, ke které je šifrovací algoritmus určen.

(2) Šifrovací klíče musí být předávány jiným důvěryhodným způsobem, než je předávána chráněná informace.

(3) V případě použití digitálních certifikátů jsou privátní klíče klasifikovány jako Chráněné informace, stejně jako jiné autentizační údaje (např. heslo).

8.4. Bezpečnost systémových souborů

8.4.1. Správa provozního programového vybavení

(1) Programové vybavení musí být provozováno a udržováno způsobem, který doporučuje a podporuje dodavatel. V případě, že starší verze dodavatel přestal podporovat, musí být toto zjištění SW správcem případně architektem ICT bezodkladně nahlášeno Bezpečnostnímu manažerovi ICT.

(2) Musí být nepřetržitě posuzovány opravné záplaty (patche) pro programové vybavení ICT ČP, které mohou odstranit nebo redukovat bezpečnostní slabiny a zranitelnosti programového vybavení. Použití patchů musí být vyhodnocováno v působnosti Bezpečnostního manažera ICT. O implementaci kritických bezpečnostních patchů identifikovaných v rámci systému včasného varování rozhoduje Bezpečnostní manažer ICT ve spolupráci se správci aktiv. Ke snížení rizika poškození programového vybavení v ICT ČP musí být implementována následující opatření:

a. aktualizaci programového vybavení musí být oprávněni provádět pouze pracovníci pověření správcem aktiv,

b. jednotlivé části ICT ČP provozního prostředí nesmí obsahovat zdrojový kód ani kompilátory (vývojové a testovací prostředí je striktně odděleno od provozního),

c. předávání programového vybavení (např. spustitelných kódů) do provozního prostředí se musí řídit akceptačním procesem a procesem řízení změn,

d. pro jednotlivé aplikace musí být stanoven postup umožňující návrat do původního stavu po implementaci změn,

e. pro případ nouze musí být uchovávány i předcházející verze programového vybavení,

f. pravidelná instalace opravných balíčků a bezpečnostních záplat musí být prováděna po jejich otestování,

g. externě dodávané programy a moduly musí být monitorovány a kontrolovány z hlediska bezpečnosti. Dodavatelům programového vybavení musí být fyzický nebo logický přístup dovolen pouze pro servisní účely a na základě schválení vlastníka aktiva. Přístup externích dodavatelů musí být monitorován, ověřován a zaznamenáván.

8.4.2. Ochrana dat pro testování systémů

(1) Pro účely testování musí být používána speciálně vytvořená testovací data (údaje), které se co nejvíce podobají datům provozním.

(2) V případě, že jsou na základě schválení Bezpečnostním manažerem ICT pro testování použity kopie ostrých dat z ICT ČP včetně seznamu oprávněných osob, musí být splněny následující podmínky:

- řízení přístupu (logického i fyzického) k testovacímu systému musí být stejné jako v případě provozního ICT,
- veškeré kopie a manipulace s provozními daty musí být evidovány v provozním deníku dané aplikace,
- obsahují-li testovací data Chráněné informace, musí být data před použitím pro testovací účely anonymizována nebo pro testovací systémy musí být vytvořena taková bezpečnostní opatření, která zabezpečí jejich odpovídající ochranu.

8.4.3. Řízení přístupu ke knihovně zdrojových kódů, bezpečnost vývoje a prostředí

(1) Prostory, ve kterých probíhá vývoj jednotlivých částí ICT ČP, musí splňovat bezpečnostní požadavky na prostory s probíhajícím vývojem ICT ČP:

1.1. Výstražné systémy

- Všechna čidla musí být vyvedena na samostatné smyčky, které umožní lokalizovat a rozlišit základní druhy incidentů.

1.2. Řízení přístupu

Pro řízení přístupu platí stejné požadavky jako pro zabezpečenou oblast TZO 2 pouze s tím rozdílem, že:

- Okna, jejichž spodní okraj je níže než 5 metrů nad terénem nebo jinými trvalými stavbami, musí být zajištěna vnější nebo vnitřní mříží, fólií s certifikátem jiným způsobem poskytujícím obdobnou úroveň bezpečnosti.

1.3. Zdroj napětí a klimatizace

- Přístup ke kabeláži napájení musí být umožněn jen oprávněným osobám.

(2) Při manipulaci s dokumenty, soubory, zdrojovými texty apod., musí být dodržena ochrana informací z hlediska jejich klasifikace.

(3) Zaměstnanci podílející se na provozu ICT ČP (administrátoři) nesmí mít přístup k vývojovým prostředkům (zdrojové kódy, kompilátory, atd.).

8.5. Bezpečnost procesů vývoje a podpory

(1) Veškeré změny aplikací nebo dalších aktiv musí projít řádným změnovým řízením a musí být otestovány před zavedením do provozního prostředí.

(2) Projektoví manažeři jsou odpovědní v úrovni technického návrhu za bezpečnost projektu a vývojových prostředí. Jsou povinni zajistit, že všechny plánované změny systému budou podrobeny kontrole, aby nenarušily bezpečnost ICT ČP.

8.5.1. Postupy řízení změn

(1) Každá změna software či jeho konfigurace (kromě standardních operátorských činností) v ICT ČP musí být zaznamenána v provozní dokumentaci.

(2) Každá verze programového vybavení uvolněná pro nasazení musí být uložená včetně zdrojových kódů, podpůrného programového vybavení, dokumentace a testovacích protokolů. Každá tato verze musí nést informaci o čase a místě nasazení. Verze programového vybavení musí být řešitelem uchovány nejméně 3 roky po ukončení používání dané verze programového vybavení v provozu.

(3) Změny musí být před schválením ověřeny v testovacím prostředí. Tyto změny musí schválit příslušný vlastník a správce aktiv. Dále o rozsahu změn a čase jejich provedení musí být informován příslušný vlastník aktiva.

(4) Pro všechny změny v jednotlivých částech ICT ČP musí existovat procedura návratu do stavu před změnou (i kdyby jenom formou nové instalace a obnovy ze záloh). Pro menší změny může být společná pro kategorii změn, u významnějších změn, které by mohly ovlivnit dostupnost nebo integritu dat, musí být její příprava a schválení součástí změnového řízení.

8.5.2. Změnové řízení

(1) Změny v ICT ČP představují zařazení nových provozních procedur, inovaci programového vybavení, revize hardwaru, zařazení nových uživatelů, nových skupin uživatelů a nových síťových spojení. Veškeré změny musí být evidovány. Evidenci provádí správce aktiv.

(2) Každá změna musí být z hlediska dopadu na bezpečnost ICT ČP posouzena Bezpečnostním manažerem ICT. Výsledek projednání dopadu změn včetně dopadu na plán Obnovy ICT a případné manažerské rozhodnutí musí být zdokumentováno v rámci změnového řízení.

8.5.3. Technické přezkoumání aplikací po změně operačního systému

(1) Při provádění změn operačního systému (instalace aktualizací, bezpečnostních záplat, opravných balíčků) musí být zajištěno, že tyto změny nenaruší bezpečný chod dané části ICT ČP, tj.:

- změny operačního systému musí být včas oznámeny, aby mohla být provedena náležitá přezkoumání (otestování) ještě před realizací těchto změn,
- po aplikaci změn musí být přezkoumána a otestována daná aplikace.

(2) Přezkoumání provádí tester a v případě projektového řízení přezkoumání zajišťuje projektový manažer.

8.5.4. Omezení změn programových balíků

(1) Modifikace programových balíků (dodávané třetí stranou) zaměstnanci ČP musí být omezeny pouze na nezbytné minimum, a to např. v případech, kdy neexistuje možnost získání požadovaných změn od dodavatele v rámci standardních aktualizací programu nebo servisních úprav. Všechny provedené změny musí být otestovány a zdokumentovány.

(2) Dále musí být přezkoumána následující opatření:

- získání souhlasu dodavatele s provedením změn,
- nenarušení vnitřních kontrol a procesů zajišťujících integritu,
- odpovědnost za budoucí udržování aplikace z důvodu provedení změn.

8.5.5. Programy vyvíjené externím subjektem

Smlouvy s externím subjektem (dodavatelem), který vyvíjí programové vybavení pro ICT ČP, musí kromě standardních bezpečnostních požadavků popsaných v kapitole 2.4.3. obsahovat ustanovení týkající se:

- licenčních ujednání, autorských práv a majetkových práv (dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů),
- právo na audit kvality a správnosti provedené práce,
- smluvní podmínky na dodržení kvality a zabezpečení kódu,
- testování na odhalení škodlivých kódů před instalací.

8.6. Řízení technických zranitelností

(1) Útvar ICT vývoj ve spolupráci s Bezpečnostním manažerem ICT musí vytvořit prostředí k pravidelnému sledování a vyhodnocování standardně publikovaných chyb týkajících se používaného programového vybavení v ICT ČP.

(2) Správci aktiv musí průběžně sledovat, že standardní publikované kritické a bezpečnostní opravy (patche, hot-fixy), týkající se používaného programového vybavení, jsou implementovány.

(3) Pravidelně, minimálně jednou za rok, musí být prováděna kontrola serverů zahrnující:

- kontrolu nainstalovaného SW a aktuálnost verzí,
- kontrolu konfigurace služeb,
- kontrolu přístupových práv do systému a kritických aplikací (prázdné/nedostatečné hesla, nepoužívané účty, sdílené disky apod.) pomocí automatizovaných nástrojů,
- kontrola HW vybavení (kapacita disků, paměti, procesoru apod.),

(4) Prověrku provádí správce aktiva. Ze zjištěných výsledků vypracuje zápis, který předloží nadřízenému s návrhem na odstranění nedostatků.

9. Zvládání bezpečnostních incidentů

9.1. Kategorie bezpečnostního incidentu

Pro potřeby zvládání bezpečnostních incidentů se podle následků a negativních projevů bezpečnostní incidenty dělí do následujících kategorií:

Kategorie	Charakteristika
III	velmi závažný bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.
II	závažný bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých škod.
I	méně závažný bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření bezpečnostního incidentu včetně minimalizace vzniklých škod.

9.2. Hlášení bezpečnostních incidentů

(1) K hlášení bezpečnostních incidentů je využíván ServiceDesk ČP nebo Stálá operační služby. V případě podezření na závažný (Kategorie II) a velmi závažný (Kategorie III) bezpečnostní incident a případně

při hrozbě z prodlení řešení bezpečnostního incidentu, je nutno kontaktovat přímo Bezpečnostního manažera ICT ČP.

(2) Všichni zaměstnanci i pracovníci externích subjektů musí být seznámeni s povinností hlásit bezpečnostní incident nebo podezření na něj.

(3) V případě zjištění zranitelností ICT ČP nebo nedostatků v zabezpečení ICT ČP jsou zaměstnanci povinni tuto skutečnost neprodleně nahlásit jako podezření na bezpečnostní incident.

9.3. Zvládání bezpečnostních incidentů

9.3.1. Odpovědnosti a postupy

(1) Pro účinné zvládání bezpečnostních incidentů musí být v navazující dokumentaci stanoveny odpovědnosti za jednotlivé činnosti a zavedeny formalizované postupy umožňující okamžitou reakci.

(2) Postupy musí pokrýt různé typy bezpečnostních incidentů včetně selhání a ztráty služby, výskyt škodlivého kódu, porušení důvěrnosti, integrity nebo dostupnosti a zneužití aktiv.

(3) Postupy také musí zahrnout analýzu a identifikaci příčiny incidentu, kontrolu zvládání incidentu, plánování opravných prostředků k zabránění opakování incidentu a součinnost s těmi, kteří byli incidentem ovlivněni.

(4) Podrobné postupy zvládání bezpečnostních incidentů řeší MP 2/2017 Zvládání bezpečnostních incidentů.

9.3.2. Ponaučení z bezpečnostních incidentů

(1) Sledování a evidence bezpečnostních incidentů přispívá k přijetí dostatečných bezpečnostních protiopatření v případě jejich budoucího výskytu.

(2) Vyhodnocování bezpečnostních incidentů, sledování a monitoring bezpečnostní situace je v kompetenci Bezpečnostního manažera ICT ve spolupráci s bezpečnostními administrátory.

9.3.3. Testování systému zvládání bezpečnostních incidentů

(1) Systém zvládání bezpečnostních incidentů musí být v pravidelných intervalech (1x ročně) otestován.

(2) Testování provádí pracovníci specializovaného útvaru ICTB ve spolupráci s ServiceDeskem ČP a závěry předkládají Bezpečnostnímu manažerovi ICT.

10. Řízení kontinuity činností ICT

10.1. Aspekty řízení kontinuity činností v ČP

(1) Řízením kontinuity v ČP se zabývá proces Business continuity management (BCM), který formuluje základní principy, zásady a cíle pro zajištění připravenosti řešit jakékoliv typy a úrovně závažnosti událostí, které by mohly vést nebo povedou k narušení nebo přerušení činností ČP.

(2) Základní principy, zásady a cíle zajištění kontinuity činností ČP a stanovení rozsahu a pravidel pro řízení kontinuity ICT služeb systémů ČP určuje směrnice SM-8/2017 Politika systému řízení kontinuity podnikání (BCM).

(3) Zvládání mimořádných (havarijních) situací je řešeno v souladu s postupy uvedenými v Business continuity plánech klíčových (kritických) činností ČP.

10.1.1. Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností ICT

(1) Řízení kontinuity činnosti ICT ČP musí zahrnovat opatření k identifikaci a minimalizaci rizik, omezení důsledků bezpečnostních incidentů a zajištění včasné dostupnosti informací potřebných pro obnovení nezbytných činností ICT ČP.

(2) Pro obnovu zařízení a služeb ICT ČP zajišťujících kritické procesy ČP musí být správcem aktiv ve spolupráci s vlastníkem aktiv zpracovány plány obnovy ICT (DRP). Vypracované plány musí být i v případě havárie dostupné zaměstnancům, kterých se týkají.

(3) Součástí plánů obnovy ICT musí být mimo jiné:

- seznam členů týmu obnovy a způsob jejich vyrozumění,
- odpovědnost za rozhodnutí aktivovat plány (zahájení činnosti podle plánu),
- popisy činností jednotlivých členů týmu v průběhu mimořádné situace,
- popisy činností jednotlivých členů týmu při obnově,
- seznam relevantních dohod a smluv spolu s kontakty na dodavatele zařízení a služeb.

(4) Pro každý plán musí být správcem aktiv určena osoba odpovědná za jeho zpracování a aktualizaci. Nejméně jednou za rok musí být provedena kontrola aktualizace plánu, zejména posouzena jeho aktuálnost v určených rolích.

(5) Proveditelnost každého plánu obnovy musí být pravidelně testována. Testování plánů obnovy se provádí u kritických systémů jednou ročně, u ostatních systémů jednou za dva roky.

(6) V plánech musí být definovány pracovní pozice a role zajišťující činnosti uvedené v plánech. Zaměstnanci zařazení na těchto pozicích (těchto rolích) musí být dosažitelní dle požadované doby dostupnosti dané části ICT ČP. Tyto požadavky musí být brány do úvahy při přidělování rolí a následně při plánování dovolených, služebních cest apod. Přitom je nutné uvažovat i možnost náhlého onemocnění nebo jiné překážky v práci.

(7) Každý zaměstnanec s přiřazenou rolí v plánech musí být prokazatelně seznámen s její aktuální verzí a znát svou roli a zodpovědnost v procesu obnovy.

(8) Podrobné požadavky na zpracování plánů obnovy a obecné požadavky na testování jsou uvedeny ve směrnici SM-8/2017 Politika systému řízení kontinuity podnikání (BCM).

10.1.2. Kontinuita činností ICT ČP a hodnocení rizik

(1) V rámci zajištění kontinuity činnosti ICT ČP musí být z pohledu bezpečnosti informací identifikována rizika, která popisují vznik možných událostí vedoucích k narušení činností ČP. Hodnocení rizik je

obsaženo ve směrnice SM-20/2011 Řízení rizik a v metodickém pokynu MP-12/2011 Řízení rizik v oblastech ISMS, IS KII, GDPR, QMS a v dalších oblastech.

(2) V závislosti na výsledcích hodnocení rizik musí být vytvořena strategie stanovující komplexní přístup k zajištění kontinuity ICT ČP, která musí být schválena řídícím managementem ČP, a následně vytvořen plán její implementace.

10.1.3. Systém plánování kontinuity činností ICT ČP

(1) Pro aktiva kritických systémů musí být zajištěna kontinuita činností (např. v rámci servisní smlouvy, organizačními opatřeními, zajištěním redundantních HW aktiv apod.).

(2) V provozním řádu pracoviště musí být definována procedura, která umožní určeným pracovníkům přístup na pracoviště 24 hodin denně, 7 dní v týdnu. Součástí procedury musí být postupy pro definování a schvalování seznamu pracovníků, kterých se to týká, a změn tohoto seznamu.

(3) Opatření pro nestandardní situace musí být součástí plánů obnovy ICT. U všech takových opatření musí být vyhodnocen během jejich návrhu dopad na bezpečnost fyzického, informačního nebo softwarového aktiva.

10.1.4. Testování, udržování a přezkoumání plánů obnovy ICT

(1) Plány obnovy ICT ČP musí být testovány. Testování je možné provádět několika způsoby:

- Kontrola a aktualizace plánu, revidování postupů a opatření,
- Simulace postupů dle plánu (tento způsob je možné např. použít pro zaučení nového pracovníka, nebo pro ověření aktualizovaného plánu)
- Dílčí testování jednotlivých částí technické obnovy - obnova jednotlivých komponent systému,
- Testování obnovy v jiném umístění/lokalitě,
- Kompletní test (otestování, zdali postupy, organizace, pracovníci, vybavení a jiné zdroje jsou schopny překlenout výpadek ostrého provozu).

(2) Způsob testování na návrh správce aktiv schvaluje Gestor bezpečnosti ICT s ohledem na kritické systémy, provozní možnosti a potenciální rizika.

10.1.5. Způsoby hodnocení dopadů bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik

(1) V případě, že bezpečnostní incident působí na aktivum, jehož úroveň důležitosti aktiva je Vysoká nebo Kritická, je nezbytné ihned po vyšetření příčin bezpečnostního incidentu provést zhodnocení reálných dopadů na zasažené aktivum a provést nové posouzení souvisejících rizik.

(2) Za realizaci hodnocení dopadů a posouzení souvisejících rizik odpovídá Bezpečnostní manažer ICT.

10.1.6. Postupy pro realizaci opatření vydaných Národním úřadem pro kybernetickou a informační bezpečnost (NUKIB)

(1) V případě, že NUKIB vydá rozhodnutí, ve kterém uloží provést reaktivní opatření k řešení bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí před bezpečnostním

incidentem, případně vydá ochranné opatření obecné povahy pro zvýšení kybernetické bezpečnosti, Bezpečnostní manažer ICT je povinen zajistit realizaci tohoto opatření.

11. Soulad s požadavky

11.1. Soulad s právními normami

11.1.1. Určení relevantní legislativy

(1) Specifické bezpečnostní požadavky vyplývající z předmětných zákonů musí být Bezpečnostním manažerem ICT konzultovány se specializovaným útvarem právní.

(2) Pro každý systém ICT ČP musí být jednoznačně definovány legislativní a smluvní požadavky, které se na daný systém vztahují.

11.1.2. Zákon na ochranu duševního vlastnictví, licenční čistota

(1) Správce SW licencí musí provádět evidenci zakoupených licencí a provozovaného software v ICT ČP. Povinnost vedení evidence a její aktualizace je nutná pro plánování potřeby nákupu licencí a udržování deklarované licenční čistoty v souladu s autorským zákonem (zákon č. 121/2000 Sb.).

(2) Pokud je potřeba dodat software z jiného zdroje (např. z Internetu), je nutné u tohoto software ověřit integritu licenčního balíku způsobem nabízeným tvůrcem konkrétního software a ověřením v testovacím prostředí.

11.1.3. Ochrana záznamů

(1) Veškeré záznamy zpracovávané v ICT ČP (účetní, databázové, transakční, logy, provozní postupy atd.) musí být uloženy odpovídajícím způsobem v souladu se směrnicí SM-5/2013 Ochrana informací tak, aby nedošlo k jejich poškození, ztrátě, zneužití, modifikaci či znehodnocení (ať se jedná o tištěnou či elektronickou podobu).

(2) Lhůta uchování dokumentů a důležitých záznamů je stanovena v řádu ŘA-3/2010 Spisový řád. Po celou dobu uchování záznamů musí být zajištěna jejich čitelnost. Po uplynutí předepsané skartační lhůty jsou záznamy předány do skartačního řízení.

11.1.4. Ochrana osobních údajů

(1) V případě, kdy systémy ICT ČP obsahují osobní údaje, musí být při jejich návrhu a provozu přihlédnuto k příslušným platným právním předpisům, ke směrnici upravující ochranu osobních údajů (SM-8/2013 Ochrana osobních údajů), resp. smluvním ujednání o zpracování osobních údajů. Zejména musí být připraveny postupy pro zajištění bezpečnostních opatření vyplývajících z právních a interních norem.

(2) V případě, kdy ČP je zpracovatelem osobních údajů v systémech ICT ČP, avšak není správcem těchto osobních údajů (ve smyslu příslušných předpisů), musí být mezi ČP a správcem osobních údajů uzavřena smlouva definující povinnosti a odpovědnost obou smluvních stran. Taková smlouva musí být uzavřena i v případě, kdy je ČP správcem osobních údajů a tyto osobní údaje ze svých ICT systémů předává druhé smluvní straně jako pověřenému zpracovateli osobních údajů a řídí se platnou legislativou na ochranu osobních údajů.

11.1.5. Zákon o kybernetické bezpečnosti

(1) Bezpečnostní manažer ICT sleduje opatření vydaná NUKIB v oblasti zajištění ochrany kybernetické bezpečnosti, zejména v oblasti hodnocení rizik a bez zbytečného odkladu je zohlední v rámci systému řízení bezpečnosti informací ČP.

(2) Bezpečnostní manažer ICT řeší reaktivní opatření vydaná NUKIB tak, že posoudí očekávané dopady reaktivního opatření na provozovaný informační systém a na zavedená bezpečnostní opatření, vyhodnotí možné negativní účinky a bez zbytečného odkladu je oznámí NUKIB.

(3) Bezpečnostní manažer ICT stanoví způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určí časový plán jeho provedení.

(4) Bezpečnostní manažer ICT stanoví a aktualizuje postupy pro provedení opatření vydaných NUKIB, ve kterých zohlední:

4.1. výsledky hodnocení rizik provedených opatření,

4.2. stav dotčených bezpečnostních opatření

4.3. vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury.

11.2. Soulad s bezpečnostními politikami, normami a technická shoda

11.2.1. Shoda s bezpečnostními politikami a normami

(1) Ověření shody systémů ICT ČP s vnitřními předpisy ČP týkajícími se bezpečnosti ICT musí být prováděno vlastníky aktiv ve spolupráci s Bezpečnostním manažerem ICT.

(2) V případě, že některé systémy ICT ČP neumožňují dostatečně chránit zpracovávaná data, musí být provedena aktualizace systému ICT ČP nebo zvolit jiné adekvátní řešení, které zajistí bezpečnost dat. K odstranění problému musí být aktivován proces změnového řízení v gesci vlastníka aktiv.

11.2.2. Kontrola shody s požadavky bezpečnosti, penetrační testy

(1) V pravidelných stanovených intervalech nebo při významné změně v ICT ČP musí být prováděná či revidována analýza rizik dle směrnice SM-20/2011 Řízení rizik. Na základě vyhodnocení analýzy rizik může být požadováno provedení dalších kontrol a penetračního testu.

(2) Cíle penetračních testů musí být předem stanoveny a musí reflektovat závěry analýzy rizik.

(3) Rozsah kontroly shody s požadavky bezpečnosti je zpravidla v tomto rozsahu:

- nastavení a konfigurace HW, operačních systémů a aplikací,
- účty a oprávnění,
- relevantní dokumentace a provozní procesy,
- rozsah, způsob, frekvence logování; vyhodnocení logů,
- bezpečnostní povědomí uživatelů či administrátorů.

(4) V rámci kontrol shody s požadavky bezpečnosti může Bezpečnostní manažer ICT a jím pověřené osoby vyžadovat součinnost osob podílející se na provozu a správě ICT systémů i vlastníků/garantů aktiv.

11.3. Audit bezpečnosti

11.3.1. Opatření k auditu bezpečnosti

(1) Audit bezpečnosti je prováděn buďto interními silami (interní audit ve spolupráci s útvarem bezpečnost) nebo externím dodavatelem.

(2) V průběhu provádění auditu ICT ČP musí být tím, kdo provádí audit bezpečnosti, zajištěna jak bezpečnost auditovaného ICT ČP, tak i vlastních auditních nástrojů.

(3) K provedení auditu musí být správcem a vlastníkem aktiva:

- ve spolupráci s auditorem schválen rozsah a harmonogram auditu,
- omezen přístup k programům a datům pouze na čtení,
- plný přístup k programům a datům povolen jen na samostatné kopie souborů,
- veškerý přístup monitorován a evidován a vytvořen referenční záznam,
- zdokumentovány všechny postupy, požadavky a odpovědnosti.

11.3.2. Ochrana nástrojů pro audit

(1) K nástrojům určeným pro audit systémů ICT ČP musí mít přístup pouze osoby oprávněné k provádění auditu, přičemž přístup do systému musí být zaznamenáván (tj. monitorován a logován).

(2) Musí být přijata opatření pro minimalizaci možnosti zneužití nástrojů pro audit ICT ČP (okamžitá změna hesla, v případě, že kontrolu provádí třetí strana, ukládání záznamů z kontroly na nepřepisovatelné médium apod.).

12. Přechodná a závěrečná ustanovení

(1) Výklad a aktualizaci této Politiky zajišťuje specializovaný útvar ICTB.

(2) Zpracované systémové bezpečnostní politiky systémů ICT ČP jsou umístěny na IntraNetu ČP zde: Odborné úseky -> ICT -> Bezpečnost ICT -> Bezpečnostní dokumentace -> Systémové bezpečnostní politiky

(3) Odpovědným za aktuálnost a správnost této Politiky, stejně jako pravomoc kontrolovat a ověřovat jejich dodržování, je Bezpečnostní manažer ICT.

(4) Výjimku z této Politiky uděluje Bezpečnostní manažer ICT, včetně délky platnosti této výjimky, maximálně však na jeden rok. V závažných případech, majících dopad na finanční plnění nebo zásadní zabezpečení provozu, uděluje výjimku a platnost na návrh Bezpečnostního manažera ICT Gestor bezpečnosti ICT. Udělená výjimka musí být náležitě dokumentována a obsah chráněn podle jeho klasifikace

13.Související dokumenty a další informační zdroje

INTERNÍ	
SM-1/2015	**Bezpečnostní politika ICT**
SM-5/2013	**Ochrana informací**
SM-20/2011	Řízení rizik
MP-12/2011	Řízení rizik v oblastech ISMS, IS KII, GDPR, QMS a v dalších oblastech
ŘA-3/2010	Spisový řád
SM-8/2017	Politika systému řízení kontinuity podnikání (BCM)
ŘA-1/2020	Organizační řád
ŘA-3/2015	Globální bezpečnostní politika
SM-8/2016	Posuzování objektů určených k fyzické ostraze
SM-12/2012	Ukládání finančních hotovostí a cenin a způsoby jejich ochrany
MP-2/2015	**Bezpečnostní příručka uživatele ICT ČP**
ŘA-4/2012	Pracovní řád České pošty, s.p.
SM-8/2013	Ochrana osobních údajů
SM-3/2019	Projektové řízení a řízení projektového portfolia
SM-12/2011	Správa SW aktiv ČP
OP-23/2019/GŘ	Jmenování bezpečnostních rolí informačního systému kritické informační infrastruktury
MP-3/2016	Compliance prověřování vybraných externích subjektů
EXTERNÍ	
zákon č. 181/2014 Sb.	o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
vyhláška 82/2018 Sb.	o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti)
zákon č. 110/2019 Sb.	o zpracování osobních údajů
Nařízení Evropského parlamentu a rady (EU) 2016/679	o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
zákon č. 262/2006 Sb.	zákoník práce
zákon č. 121/2000 Sb.	o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
DALŠÍ INFORMAČNÍ ZDROJE	
IntraNet ČP	Odborné úseky -> ICT -> Bezpečnost ICT -> Bezpečnostní

	dokumentace Systémové bezpečnostní politiky systémů ICT ČP

14. Seznam příloh

POŘADÍ	NÁZEV PŘÍLOHY
1. samostatná	Schválené šifrovací algoritmy

Příloha je uveřejněna na IntraNetu ČP (Odborné úseky -> ICT -> Bezpečnost ICT -> Bezpečnostní dokumentace). Za její obsah, uveřejnění a aktualizaci odpovídá specializovaný útvar ICTB.

Schválené šifrovací algoritmy

Funkce přílohy

V této příloze jsou uvedené povolené šifrovací algoritmy určené k využití v ČP. Dokument vychází z Vyhlášky 82/2018 Sb. a dokumentu „**Minimální požadavky na kryptografické algoritmy“ uvedených na webových stránkách NÚKIBu (www.nukib.cz).**

Minimální požadavky na kryptografické algoritmy podle NÚKIBu

Podle § 26 písm. d) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“) mají povinné osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“) povinnost zohlednit doporučení v oblasti kryptografických prostředků vydaná Národním úřadem pro kybernetickou a informační bezpečnost za účelem ochrany aktiv informačního a komunikačního systému. Tento dokument obsahuje zmíněná doporučení. (https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf).

Doporučení v oblasti kryptografických prostředků

Kategorie kryptografických algoritmů podle omezení doby své použitelnosti

Níže uvádíme dvě kategorie kryptografických algoritmů, které nazýváme „schválené“ a „dosluhující“.

Schválené kryptografické algoritmy (Approved, Recommended, Future) jsou algoritmy, u kterých jsme přesvědčeni, že jsou bezpečné alespoň ve střednědobém horizontu.

Dosluhující kryptografické algoritmy (Legacy) jsou algoritmy, u kterých doporučujeme přestat s jejich používáním do r. **2023**. A dále doporučujeme nově zavádět pouze takové kryptografické systémy, které obsahují pouze schválené kryptografické algoritmy (a neobsahují dosluhující).

1) **Symetrické algoritmy**
   a) **Schválené blokové a proudové šifry**
      (1) Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
      (2) Twofish s využitím délky klíčů 128 až 256 bitů
      (3) Serpent s využitím délky klíčů 128, 192, 256 bitů
      (4) Camellia s využitím délky klíčů 128, 192 a 256 bitů
      (5) SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů
      (6) ChaCha20 s délkou klíče 256 bitů a se zatížením klíče menším než 256 GB

   Doporučujeme preferovat:

   - Použití blokových šifer před proudovými.
   - V případě blokových šifer: AES, Camellia a Serpent (v uvedeném pořadí).
   - Délku klíče 256 bitů.

   b) **Dosluhující blokové a proudové šifry**
      (1) Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu
      (2) Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB
      (3) Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB

   c) **Schválené módy šifrování s ochranou integrity**
      (1) CCM
      (2) EAX
      (3) OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1
      (4) GCM s noncí dlouhou 96 bitů a s tagem dlouhým 128 bitů, nejpozději po 2^{32} hodnotách nonce musí dojít k výměně klíče
      (5) 5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB
      (6) 6. Složená schémata typu „Encrypt-then-MAC“

Poznámky:

- Schválené módy šifrování musí používat schválené blokové šifry.
- Schémata typu „Encrypt-then-MAC“ musí používat k šifrování pouze šifrovací módy uvedené v odstavci d) a k výpočtu MAC pouze schválené módy pro ochranu integrity.
- Inicializační vektor (nebo nonce) musí být součástí vstupu pro výpočet MAC.

   d) **Módy šifrování (jejich samostatné použití je dosluhující, ale schválené je jejich použití ve složených schématech typu „Encrypt-then-MAC)**
      (1) CTR
      (2) OFB
      (3) CBC
      (4) CFB

Poznámky:

- Pro použití v rámci schváleného složeného schématu typu Encrypt-then-MAC musí tyto módy používat pouze schválené blokové šifry.
- Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným, inicializačním vektorem.
- Při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- Při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače.
- V případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

e) Schválené módy pro šifrování disků

(1) XTS – délka jednotky dat (sektoru) nesmí přesáhnout 220 bloků šifry (v případě šifry se 128-bitovým blokem je to zhruba 16 MB)
(2) EME

f) Schválené módy pro ochranu integrity

(1) HMAC se schválenou hašovací funkcí
(2) EMAC
(3) CMAC
(4) UMAC s délkou tag 64 bitů

g) Dosluhující módy pro ochranu integrity

(1) 1. HMAC-SHA1
(2) 2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 109 MAC

(2) Asymetrické algoritmy

a) Schválené algoritmy pro technologii digitálního podpisu

(1) Digital Signature Algorithm (DSA) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
(2) Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více
(3) Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 3072 bitů a více
(4) Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 256 bitů a více

b) Dosluhující algoritmy pro technologii digitálního podpisu

(1) Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
(2) Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů
(3) Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 224 bitů

c) Schválené algoritmy pro procesy dohod na klíči a šifrování klíčů

(1) Diffie-Hellman (DH) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
(2) Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 256 bitů a více
(3) Elliptic Curve Integrated Encryption System – Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více
(4) Provably Secure Elliptic Curve – Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů více
(5) Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více
(6) Rivest Shamir Adleman – Optimal Asymetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 3072 a více
(7) Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 3072 a více

Doporučení:

U kryptografie na bázi eliptických křivek doporučujeme preferovat délku klíčů 384 bitů.

d) Dosluhující algoritmy pro procesy dohod na klíči a šifrování klíčů

(1) Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
(2) Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů
(3) Elliptic Curve Integrated Encryption System – Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 224 bitů
(4) Provably Secure Elliptic Curve – Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 224 bitů
(5) Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 224 bitů
(6) Rivest Shamir Adleman – Optimal Asymetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 2048 bitů
(7) Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 2048 bitů

(3) Algoritmy hašovacích funkcí

a) Schválené hašovací funkce SHA-2

(1) SHA-256
(2) SHA-384
(3) SHA-512
(4) SHA-512/256

b) Schválené hašovací funkce SHA3

(1) SHA3-256
(2) SHA3-384
(3) SHA3-512
(4) SHAKE128
(5) SHAKE256

c) Ostatní schválené hašovací funkce

(1) Whirlpool
(2) BLAKE2

Doporučení:

U schválených hašovacích funkcí doporučujeme preferovat délku výstupu 384 bitů.

d) Dosluhující hašovací funkce

(1) 1. SHA2 s délkou výstupu 224 bitů (SHA-224, SHA-512/224)
(2) 2. SHA3-224
(3) 3. RIPEMD-160