Česká pošta

Směrnice

Identifikace	SM-1/2015 - verze 3.0	**Číslo jednací**	ČP/53099/2019/CKA/02
Nahrazuje	SM-1/2015 - verze 2.0	**Klasifikace**	Interní
Platnost	13. 11. 2019	**Účinnost**	15. 11. 2019

Bezpečnostní politika ICT

Verze 3.0

Podpis		**Podpis**	
Datum	6. 9. 2019	**Datum**	13. 11. 2019
Garant	Ing. Jaroslav Hloušek podepsáno elektronicky	**Schvalovatel**	Ing. Roman Knap podepsáno elektronicky
Funkce	ředitel divize ICT a eGovernment	**Funkce**	generální ředitel

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
1.0	1.2.2015	Základní dokument	BICT	GŘ
2.0	1.3.2017	Aktualizace dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a navazujících legislativních předpisů v aktuálním znění. Nové přílohy č. 1 až 4. Formální úpravy.	BICT	GŘ
3.0	15.11.2019	Oproti předcházející verzi 2.0 došlo k těmto změnám: Aktualizace dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a navazujících legislativních předpisů v aktuálním znění. Upravena klasifikace informací podle směrnice SM-5/2013 Ochrana informací. Aktualizovány částí týkající se BCM a řízení dodavatelů a jejich přístupů Nové přílohy č. 1 až 4. Změna názvů organizačních jednotek v souvislosti se změnou organizační struktury k 1. 6. 2019. Formální úpravy.	ICTB	GŘ

1. Úvodní ustanovení

1.1. Účel a působnost

(1) Bezpečnostní politika ICT (dále BPICT) rozpracovává Globální bezpečnostní politiku České pošty, s.p. (ŘA-3/2015) v oblasti zajištění bezpečnosti informačních a komunikačních technologií České pošty, s.p. (dále ICT ČP) a stanovuje základní rámec pravidel pro řízení bezpečnosti informací v oblasti ICT ČP.

(2) Cílem BPICT je definovat **bezpečnostní požadavky** ČP pro vymezení, zavedení, udržování a zlepšování systému řízení bezpečnosti informací v oblasti ICT ČP v souladu s požadavky ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky (dále ISO 27001) a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů v aktuálním znění (dále ZoKB).

(3) Dle požadavku ZoKB je zpracována Politika systému řízení bezpečnosti informací v kybernetickém prostoru, která je souborem závazných bezpečnostních a organizačních principů a stanovuje základní zásady pro zajištění kybernetické bezpečnosti ČP, tj. zásady pro řízení bezpečnosti informací v kybernetickém prostoru (viz příloha č. 1 této směrnice).

(4) Postupy pro naplnění bezpečnostních požadavků, tzn. zavedení bezpečnostních opatření pro jednotlivé oblasti ICT ČP, jsou nebo budou postupně dle potřeb rozpracovány v navazujících bezpečnostních dokumentech.

1.2. Rozsah a hranice systému řízení bezpečnosti informací

(1) Systém řízení bezpečnosti informací stanovený touto bezpečnostní politikou a navazující dokumentací se týká provozu veškerých informačních a komunikačních technologií (ICT) ČP.

(2) Rozsah a hranice systému pro ZoKB jsou stanoveny fyzickým a logickým perimetrem (viz přílohy č. 2 a 3 této směrnice).

1.3. Působnost

(1) BPICT je závazná pro všechny uživatele (zaměstnanci ČP, externí subjekty) ICT ČP, kteří v rámci své pracovní činnosti mají přístup k informacím ČP a využívající služeb ICT ČP. Příslušní zaměstnanci ČP jsou oprávněni za tímto účelem poskytnout informace týkající se této směrnice zaměstnancům třetích stran.

(2) BPICT stanovuje bezpečnostní požadavky pro ICT v majetku a správě ČP. **Použití vlastních zařízení v ICT ČP je zakázáno.** Výjimky schvaluje Bezpečnostní manažer ICT.

(3) Předmětem BPICT není ochrana utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

1.4. Zkratky a pojmy

ZKRATKY	
BPICT	Bezpečnostní politika ICT
ISO 27001	požadavky ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky
ZoKB	zákon č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
POJMY	
Aktivum	všechno, co má pro ČP hodnotu, zde se rozumí aktiva spadající do ICT. Model aktiv je uveden v MP-12/2011 Řízení rizik v ISMS.
Analýza rizik v ICT ČP	proces zjišťování možných kombinací hrozeb, zranitelností a následků (scénářů) k příslušnému aktivu. Jedná se tedy o proces, během něhož jsou identifikována a hodnocena aktiva, hrozby působící na aktiva, jejich zranitelná místa, pravděpodobnost realizace hrozeb a odhad jejich následků (dopadů).
Auditní záznam	pro účely BPICT se jedná o záznam o všech událostech, které mohou ovlivnit bezpečnost ICT ČP.
Autentizace	prokázání identity uživatele, zdroje nebo zařízení.
Autorizace	řízení oprávnění, které zahrnuje udělení přístupu na základě přidělené role.
Bezpečnost informací	zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. odpovědnost, nepopiratelnost a spolehlivost.
Bezpečnostní incident	událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních požadavků
Bezpečnostní opatření	souhrn prostředků a postupů, kterými je snižována možnost ohrožení bezpečnosti informací a dopadů
Fyzický a logický perimetr	souhrn fyzických, technických a technologických prvků, které definují hranice chráněného systému.
BCMS – (Business Continuity Management Systém - Systém řízení kontinuity činností)	ucelený systém řízení kontinuity činností organizace, který zahrnuje politiku BCMS, analýzu dopadů, strategie obnovy, stanovení zodpovědností, plánovací činnosti, tvorbu a testování BCP a postupů obnovy, zajištění zdrojů pro obnovu, kontrolu, měření a provádění reportingu k dosažení stanovených cílů organizace v oblasti zajištění kontinuity činností.
BIA – (Business Impact Analysis - Analýza dopadů)	analýza činností organizace a dopadů, které mohou být způsobeny jejich narušením. Je základním zdrojem pro klasifikaci aktiv společnosti, určuje priority BCMS a stanoví požadované parametry obnovy činností a jejich podpůrných aktiv.
BCP – (Business Continuity Plan - Plán kontinuity činností)	popisuje postupy analýzy situace, řízení obnovy, komunikaci při narušení a obnově, zdroje pro obnovu a konkrétní postupy obnovy a jejich cíle, resp. BCP rozpracovává strategii obnovy ČP do postupů obnovy jednotlivých činností.
Data	záznamy nebo údaje (libovolná posloupnost znaků bez ohledu na jejich srozumitelnost), které reprezentují informace formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování.

Dokument	Každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace ať v podobě analogové (listinné) či digitální (elektronické), která byla vytvořena, doručena anebo vznikla z činnosti ČP v rámci zákonných povinností nebo jako důkaz o pracovních činnostech. Dokument je evidován v systému spisové služby eSSL EZOP, případně v jiném agendovém systému. Základní vlastnosti dokumentu jsou: autentičnost, hodnověrnost, integrita, použitelnost (ISO 15489 - Informace a dokumentace-Správa dokumentů).
Dostupnost	znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
Důvěrnost	znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
Hodnota aktiva	pro účely BPICT založena na vyjádření ceny nebo na ocenění důležitosti aktiva pro ČP, případně kombinace obou přístupů.
Hrozba	možný zdroj potenciálního poškození aktiv.
Chráněná informace	informace, která na základě rozhodnutí příslušné autority (vlastníka informace) musí být chráněna, protože její zpřístupnění, modifikace, zneužití, zničení nebo ztráta by mohlo poškodit nebo ohrozit zájmy ČP, a/nebo způsobit ČP nebo jinému subjektu újmu (materiální i nemateriální).
Informační a komunikační technologie (ICT)	veškerá technika, která se zabývá zpracováním a přenosem informací, zejména výpočetní a komunikační technika a její programové vybavení.
Informace	data nebo údaje, která mají svůj význam.
Informační systém	funkční celek nebo jeho část zabezpečující cílevědomé a systematické shromažďování, zpracování, uchování a zpřístupňování informací. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a zaměstnance.
Integrita	zajištění správnosti a úplnosti informací.
Informační systém základních služeb (ISZS)	soubor prvků kritické infrastruktury a kritické informační infrastruktury podle ZoKB. Fyzický a logický perimetr ISZS je uveden v přílohách č. 2 a 3 této směrnice.
Klasifikace informací	definování kategorie informace z hlediska jejího významu a povahy. Podle stanovené kategorie se určuje konkrétní způsob její ochrany.
Kybernetický bezpečnostní incident	Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
Kybernetická bezpečnostní událost	Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Mobilní zařízení ICT ČP	přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod.
Monitorování	sledování, dozor, kritické pozorování nebo určování stavu pro identifikování odchylek od požadované nebo očekávané úrovně.
Oprávněná osoba	fyzická nebo právnická osoba, která splňuje podmínky přístupu nebo je oprávněna seznamovat se s příslušnou kategorií informace.

Plán obnovy ICT (DRP - disaster recovery plan)	plán obsahující postupy pro obnovu ICT provozu nebo ICT služeb po havárii (odpovídá pojmu BCP u ICT činností a služeb.
Riziko	pro účely této BPICT je tímto pojmem myšlena hrozba vzniku určité události, která může způsobit škodu na aktivu/dopad (škoda je např. ztráta, zničení, poškození nebo snížení hmotných i nehmotných aktiv, zranění nebo poškození zdraví lidí, poškození dobrého jména podniku, důvěry apod.).
Zabezpečená oblast	stavebně ohraničený prostor se specifickými prvky ochrany.
Zranitelnost	slabé místo aktiva, které umožní působení příslušné hrozby.

2. Organizace bezpečnosti

2.1. Definice rolí a stanovení odpovědností

Bezpečnostní role	Odpovědnost
Gestor bezpečnosti ICT	vedoucí organizační jednotky v úrovni G-1 (ředitel divize ICT a eGovernment), odpovědný za vývoj, provoz a bezpečnost ICT ČP, který v souladu s obchodní činností a úkoly ČP poskytuje odpovídající finanční, materiálové a personální zdroje a definuje a schvaluje strategii dalšího rozvoje ICT ČP.
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.
Bezpečnostní architekt	bezpečnostním manažerem ICT určený zaměstnanec specializovaného útvaru ICT bezpečnost, který je odpovědný za formulaci a zpracování bezpečnostní dokumentace, za vývoj a implementaci bezpečnosti ICT ČP, za návrh a prosazování bezpečnosti v projektech a implementovaných ICT technologiích a za formulaci požadavků na konfiguraci bezpečnostních a monitorovacích technologií ICT ČP. Metodicky řídí bezpečnostní administrátory. Zastává jmenovanou bezpečnostní roli architekta kybernetické bezpečnosti dle § 6 odst. 3 písm. b) vyhlášky 82/2018 Sb., o kybernetické bezpečnosti.
Bezpečnostní administrátor	bezpečnostním manažerem ICT určený zaměstnanec specializovaného útvaru ICT bezpečnost, je odpovědný za kontrolu a soulad bezpečnosti ICT ČP v jemu přidělené části ICT ČP. Bezpečnostní administrátor odpovídá za shromažďování a vyhodnocování hlášení o bezpečnostních incidentech, sledování průběhu řešení bezpečnostních incidentů, monitorování implementace a používání bezpečnostních opatření v oblasti ICT ČP, bezpečnostní školení zaměstnanců v souladu s bezpečnostní dokumentací ICT ČP, bezpečnostní dohled (monitorování a vyhodnocování logů) a provádění bezpečnostních kontrol.

Bezpečnostní auditor	určený zaměstnanec specializovaného útvaru interní audit a řízení rizik odpovědný za plánování a přípravu auditu, realizaci auditu, vyhodnocení a porovnání získaných výstupů, vypracování auditní zprávy a podílení se na realizaci nápravných opatření. Zastává jmenovanou bezpečnostní roli auditora kybernetické bezpečnosti dle §6 odst. 3 písm. d) vyhlášky 82/2018 Sb., o kybernetické bezpečnosti.
Bezpečnostní ředitel ČP	zaměstnanec ČP jmenovaný generálním ředitelem ČP v souladu s požadavky zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Ve vztahu k ZoKB je kontaktní osobou k Národnímu bezpečnostnímu úřadu, která je oprávněna jednat ve věcech upravených ZoKB.
Projektové role	**Odpovědnost**
Projektový manažer	řídí projekt v souladu s bezpečnostními požadavky.
Řešitel	zaměstnanec, tým, organizační jednotka nebo dodavatel, který zajišťuje vývoj dílčích částí ICT ČP a odpovídá za kvalitu vývoje a implementaci požadovaných bezpečnostních opatření.
Dodavatel	fyzická nebo právnická osoba, která má uzavřený smluvní vztah pro vznik nebo dodání aktiv.
Významný dodavatel	provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou (ČP) vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému,
Provozní role	**Odpovědnost**
Vlastník/Garant aktiva	vedoucí zaměstnanec organizační jednotky, který aktivum spravuje a plně za něj odpovídá (tj. za jeho identifikaci, rozvoj, revize, údržbu, převody a evidenci). A zároveň zastává bezpečnostní roli garanta aktiva dle §6 odst. 3 písm. c) vyhlášky 82/2018 Sb., o kybernetické bezpečnosti (fyzická osoba pověřená správcem informačního systému kritické informační infrastruktury k zajištění rozvoje, použití a bezpečnosti aktiva (viz příloha č. 4))
Správce aktiva	určen Vlastníkem/Garantem aktiva pro plnění specifických činností při správě aktiva po dohodě s vedoucím organizační jednotky, kde bude příslušný druh správy vykonáván v souladu s pokyny Vlastníka/Garanta aktiva.
Správce informačního systému kritické informační infrastruktury	dle ZoKB generální ředitel ČP.
Správce sw licencí	zaměstnanec ČP, který odpovídá za evidenci a sledování počtu zakoupených licencí, kontrolu jejich využívání a včasné plánování nákupu potřebných licencí.
Administrátor	zaměstnanec ČP, který je odpovědný za správu svěřených aktiv v souladu s požadavky bezpečnostní a provozní dokumentace ICT ČP. Má nejvyšší přístupová oprávnění. Je zpravidla určen správcem příslušného aktiva.
Tester	zodpovědná osoba za provádění testů v souladu s testovacími scénáři a systémovou bezpečnostní politikou daného systému.
Uživatel	každá fyzická osoba (zaměstnanec ČP nebo osoba v jiném smluvním vztahu s ČP), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění.

2.2. Výbor pro řízení kybernetické bezpečnosti

(1) Funkci výboru pro řízení kybernetické bezpečnosti dle §6 odst. 2 a 7 vyhlášky 82/2018 Sb. vyhláška o kybernetické bezpečnosti zastává Krizový štáb ČP (dle opatření OP-4/2016/GŘ Pravidla řízení za krizových situacích).

(2) Krizový štáb ČP je pracovním orgánem generálního ředitele k řešení krizových situací podle § 9 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů a § 11 a § 21 ZoKB.

(3) Tajemníkem pro zákon o kybernetické bezpečnosti Krizového štábu ČP je manažer specializovaného útvaru ICT bezpečnost.

(4) Tajemník kromě řešení stavu kybernetického nebezpečí předkládá k projednání také zejména následující oblasti:

- navrhování změn Globální bezpečnostní politiky ČP, Bezpečnostní politiky ICT ČP, případně dalších bezpečnostních dokumentací,
- rozvoj a řízení kybernetické bezpečnosti pro informační systém kritické informační infrastruktury,
- monitorování a kontrolu implementace bezpečnosti ICT ČP a kybernetické bezpečnosti,
- postupů při prosazování povědomí o problémech bezpečnosti ICT ČP,
- strategické hodnocení bezpečnosti informací v oblasti ICT a kybernetické bezpečnosti,
- dodatečné vyhodnocování závažných bezpečnostních incidentů.

2.3. Oddělení rolí

(1) Z důvodu zabránění neoprávněné modifikace nebo zneužití informací musí být výkon některých rolí prováděn odděleně, tj. různými zaměstnanci ČP.

(2) Zaměstnanec zastávající roli administrátora nemůže zastávat roli bezpečnostního administrátora a naopak.

2.4. Ochrana důvěrnosti informací

Klasifikaci a úroveň ochrany informací v listinné i elektronické podobě stanovuje směrnice SM-5/2013 Ochrana informací.

2.5. Dohody o ochraně informací

(1) Každé smluvní ujednání, jehož obsahem jsou chráněné informace, musí obsahovat ustanovení o ochraně informací a povinnost zachovávat mlčenlivost.

(2) Za přezkoumání smluvního ujednání odpovídá vedoucí věcně příslušné organizační jednotky, do jehož působnosti smlouva spadá.

2.6. Přístup externích subjektů

(1) Přístup externích subjektů (fyzická nebo právnická osoba) k ICT ČP nesmí být umožněn, s výjimkou potřebných servisních zásahů nebo služeb zajišťovaných dodavateli na základě smluvních vztahů.

(2) Požadavek externího subjektu na zřízení časově omezeného přístupu k ICT ČP prostřednictvím uživatelského účtu musí být posouzen specializovaným útvarem ICT bezpečnost. Přístup k aktivům musí být následně schválen Vlastníkem/Garantem aktiv nebo jím pověřenou osobou. Zpravidla se tak děje schválením přiřazení příslušné role.

(3) Externí subjekty přistupující k ICT ČP musí být prokazatelně seznámeni s požadavky BPICT a související bezpečnostní dokumentací a jsou povinni jejich ustanovení dodržovat. Sankce za nedodržení musí být uvedeny ve smluvním ujednání.

(4) Přístup externích subjektů musí být specializovaným útvarem ICT bezpečnost hodnocen z pohledu možných bezpečnostních rizik, za činnost odpovídá Bezpečnostní manažer ICT. Smluvní ujednání s externím subjektem musí být uzavřeno před povolením přístupu k ICT ČP a musí respektovat bezpečnostní standardy ČP a platné legislativy (ZoKB, ISO:270xx) apod. Přístup musí být povolen pouze v nezbytně nutném rozsahu pro výkon smluvních závazků.

(5) Za zahrnutí požadavků na zajištění bezpečnosti informací v souladu s BPICT a souvisejících bezpečnostních dokumentací do smluvních ujednání odpovídá vedoucí věcně příslušné organizační jednotky, která smlouvu uzavírá. Relevantní ustanovení smlouvy musí být k dispozici specializovanému útvaru ICT bezpečnost ke kontrole.

3. Posuzování a ošetření rizik

(1) Posuzování a ošetření rizik se provádí podle metodického pokynu MP-12/2011 Řízení rizik v ISMS.

(2) Bezpečnostní manažer ICT bez zbytečného odkladu posoudí reaktivní a ochranná opatření popsaná interní dokumentací a Národním úřadem pro kybernetickou a informační bezpečnost v hodnocení rizik. V případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní plán zvládání rizik.

4. Klasifikace a řízení aktiv

(1) Aktiva musí být jasně identifikována, evidována, seznam aktiv musí být udržován aktuální, každé aktivum musí mít stanoveného Vlastníka/Garanta. Za aktuální data v evidenci odpovídá Vlastník/Garant aktiva. Členění základních aktiv je uvedeno ve směrnici SM-20/2011 Řízení rizik, jejichž výklad a aktualizaci zajišťuje specializovaný útvar interní audit a řízení rizik.

(2) Evidence aktiv musí obsahovat typ aktiva, jeho popis (formát), umístění, případně licenční informace, hodnotu aktiva pro ČP a další informace stanovené jako povinné v evidenci.

(3) V případě, že Vlastník/Garant aktiv není určen nebo je jeho určení sporné, rozhoduje o Vlastníkovi/Garantovi aktiv ICT Gestor bezpečnosti ICT.

(4) Na základě důležitosti aktiva a klasifikace informace musí být stanovena odpovídající úroveň ochrany, tedy stanovená bezpečnostní opatření.

5. Personální bezpečnost

(1) Personální bezpečnost je systém opatření omezující rizika zapříčiněná působením lidského faktoru, jako jsou chyby, krádeže, úmyslné i neúmyslné poškození či zneužití informací, nebo nesprávné používání ICT ČP.

(2) Základní pravidla a povinnosti personální bezpečnosti jsou dále specifikována v řádu ŘA-4/2012 Pracovní řád České pošty, s.p.

5.1. Vznik pracovněprávního vztahu

5.1.1. Role a odpovědnosti

(1) Při ustanovení do rolí musí být zaměstnanci seznámeni s požadavky definovanými v Bezpečnostní politice ICT a navazujících bezpečnostních dokumentech.

(2) Specifické požadavky na prověření uchazečů o konkrétní pracovní pozici musí být vždy upřesněny vedoucími věcně příslušných organizačních jednotek, případně Vlastníky/Garanty aktiv, ke kterým bude zaměstnanec přistupovat s ohledem na požadovanou funkci.

(3) Základní povinnosti zaměstnanců jsou uvedeny v metodickém pokynu MP-2/2015 Bezpečnostní příručka uživatele ICT ČP.

5.1.2. Podmínky výkonu pracovní činnosti

Všichni zaměstnanci musí být zavázáni mlčenlivostí. Povinnost mlčenlivosti a dodržování důvěrnosti chráněných informací v ČP vymezuje řád ŘA-4/2012 Pracovní řád České pošty, s.p.

5.2. Průběh pracovněprávního vztahu

5.2.1. Vzdělávání a školení

(1) Všichni uživatelé ICT ČP musí být při nástupu nebo nejpozději před zahájením používání ICT ČP (převzetí uživatelského přístupu) seznámeni s Bezpečnostní politikou ICT ČP a proškoleni v bezpečnostních pravidlech, zásadách a platných řídících dokumentech pro uživatele ICT ČP. To se týká jak zaměstnanců vykonávajících pro ČP práci na základě pracovní smlouvy, tak i zaměstnanců vykonávajících pro ČP práci na základě dohod o pracích konaných mimo pracovní poměr, stážistů a zaměstnanců externích subjektů.

(2) Školení uživatelů je zajišťováno úsekem řízení lidských zdrojů přímo tam, kde uživatel má přístup k e-learningovému školení. V ostatních případech zajišťuje úsek řízení lidských zdrojů školení ve spolupráci s vedoucími organizačních celků a v součinnosti se specializovaným útvarem ICT bezpečnost připravuje a provádí školení pro zaměstnance poštovních technologií (pošty, depa, SPU).

(3) V přípravě školení Bezpečnostní manažer ICT stanoví plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení.

(4) Součástí školení musí zejména být:

a) zásady bezpečnostních politik a navazujících řídících dokumentů,

b) implementování bezpečnostních mechanismů (s přihlédnutím k potřebě znát) a jejich používání,

c) postupy pro hlášení bezpečnostních incidentů,

d) chování v havarijních situacích.

(5) Školení musí proběhnout:

a) při nástupu zaměstnance na pracovní pozici a do role, která toto školení vyžaduje (v rámci jeho adaptačního procesu),

b) pravidelně, minimálně jednou za 24 měsíců (školení musí obsahovat popis změn v bezpečnostních politikách a nejvážnější bezpečnostní incidenty včetně způsobu jejich řešení),

c) při zásadních změnách bezpečnostních politik.

(6) O každém školení musí být proveden záznam o prokazatelném seznámení, který vede ten, kdo školení organizuje.

(7) Bezpečnostní manažer ICT hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.

(8) Disciplinární řízení

Porušení ustanovení bezpečnostních politik a navazujících metodických pokynů a příruček na základě posouzení závažnosti, míry zavinění a konkrétního rizika, případně míry dopadu a následků tohoto porušení (bezpečnostního incidentu) může být považováno za porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci se všemi důsledky z toho vyplývajícími.

5.3. Ukončení nebo změna pracovněprávního vztahu

5.3.1. Navrácení zapůjčených předmětů

(1) Při ukončení nebo změně pracovněprávního vztahu musí zaměstnanec prokazatelně odevzdat všechna přidělená aktiva, která potřeboval k výkonu své pracovní činnosti.

(2) Informace, které byly zpracovávány a uchovávány zaměstnancem v rámci jeho pracovního zařazení u ČP a jsou na základě rozhodnutí nadřízeného zaměstnance dále využitelné pro ČP, musí být před jeho odchodem z ČP prokazatelně předány nadřízenému daného zaměstnance.

5.3.2. Odebrání přístupových práv

(1) Postup odebrání přístupových práv (zablokování účtů) musí být nezávislé na zaměstnanci, jehož se týká. Tato procedura musí být navázána na ukončení nebo změnu pracovněprávního vztahu, vynětí z evidenčního stavu nebo změny pracovního zařazení, tak aby bylo zajištěno, že i bez součinnosti zaměstnance jsou přístupová práva odebrána.

(2) Toto lze realizovat následujícími způsoby:

a) standardně systémem centrální správy uživatelů (IDM), který automaticky zohledňuje změny v pracovní pozici zaměstnance,

b) nestandardně, v případě okamžitého ukončení pracovněprávního vztahu, kdy přímý nadřízený zaměstnance předá požadavky na odebrání přístupových práv správci daného aktiva, který zajistí jejich odebrání,

c) jiným způsobem, jestliže je součásti daného ICT ČP jiná procedura pro odebrání přístupových práv, je nutno postupovat podle ní, ale musí být zohledněn princip požadavku na odebrání přístupových práv nadřízeným daného zaměstnance.

6. Fyzická bezpečnost

(1) Fyzické zabezpečení ICT v objektech ČP je realizováno souborem vybraných prvků ochrany, jako je např. ostraha (bezpečnostní agentura), autentizace čipovými kartami s možností kombinovat biometrické prostředky, monitoring vstupu do chráněných objektů, kontrola fyzického přístupu, elektronická požární signalizace (EPS), poplachové zabezpečovací a tísňové systémy (PZTS), elektronické i mechanické zámky atd.

(2) Stupeň úrovně fyzického bezpečnostního perimetru (zabezpečené oblasti) se stanovuje na základě hodnoty aktiv pro ČP a kategorií a množství ukládaných chráněných informací. Stanovuje Vlastník/Garant aktiv ve spolupráci se zaměstnanci specializovaného útvaru ICT bezpečnost.

(3) Zabezpečené oblasti se dělí dle třídy zabezpečené oblasti na TZO 1, TZO 2 a TZO 3. Způsob zabezpečení jednotlivých tříd zabezpečených oblastí je stanoven v metodickém pokynu MP-3/2015 Generická systémová bezpečnostní politika ICT.

(4) Fyzická aktiva nesmí opustit prostory ČP bez výslovného souhlasu příslušného Vlastníka/Garanta nebo správce. To se netýká mobilních zařízení ICT ČP. Jsou-li aktiva umístěna v prostředí s nekontrolovaným pohybem osob, musí být fyzicky zajištěna proti krádeži.

(5) Všechny osoby včetně návštěv v zabezpečených oblastech musí být prokazatelně identifikovány. Provoz v zabezpečené oblasti se řídí režimovou směrnicí zabezpečené oblasti, kterou musí zpracovat Vlastník/Garant nebo správce zabezpečené oblasti.

(6) Návštěvy, které vstupují do oblastí, kde se zpracovávají chráněné informace, musí být doprovázeny. Doprovod musí zajistit, aby nedocházelo k neoprávněnému přístupu k informacím.

(7) Kabely pro přívod energie (silové rozvody) a komunikační kabely přenášející data nebo podporující služby, ICT ČP, zásuvky nebo konektory musí být zabezpečeny proti poškození, přetížení, proti napojení cizího zařízení, případně odposlouchávání. Odpovědnost za bezpečnost kabeláže má Vlastník/Garant případně správce těchto ICT podpůrných aktiv a služeb.

7. Řízení komunikací a provozu

7.1. Provozní postupy ICT a základní principy

(1) Provozní postupy využívající prostředky ICT ČP musí být definovány, dokumentovány a udržovány aktuální. Za aktualizaci odpovídá Vlastník/Garant aktiva.

(2) Všechny změny v provozních systémech a aplikačním vybavení musí být Vlastníkem/Garantem aktiv ve spolupráci se správcem aktiv řízeny a dokumentovány. Musí být stanoveny odpovědnosti za tyto změny v souladu s interními předpisy. Proces vývoje, testování a ověřování nesmí zasahovat do provozního prostředí.

(3) Bezpečnostní architekt ve spolupráci s architekturou ICT v rámci prosazování bezpečnosti v projektech ICT ČP formuluje konkrétní požadavky a způsob realizace požadavků BPICT, např. na oddělení vývoje, testování a provozu. Realizaci v rámci projektů ICT ČP řídí projektový manažer.

7.2. Řízení zranitelností

(1) Cílem řízení zranitelností je definovat činnosti spojené s životním cyklem zranitelnosti tj. od jejího zjištění přes implementaci nápravného opatření po retest existence zranitelnosti.

(2) Pro tyto činnosti musí být zpracován a zdokumentován postup, který definuje jednotlivé kroky a dílčí odpovědnosti od okamžiku identifikace zranitelnosti až do okamžiku jejího odstranění.

(3) Za oblast řízení zranitelností je odpovědný Bezpečnostní manažer ICT.

7.3. Řízení dodávek externích subjektů

(1) Je-li k zabezpečení komunikací a provozu nezbytné využít služeb externích subjektů musí být již ve smluvním ujednání specifikován požadavek na dodržování BPICT a související bezpečnostní dokumentace.

(2) Ve smluvním ujednání musí být dále specifikován požadavek na možnost ověřovat dodržování stanovených bezpečnostních požadavků a vymahatelnost odpovědnosti a možnosti monitorovat a přezkoumávat dodávané služby externích subjektů (např. formou auditu). Smluvní ujednání musí také obsahovat ustanovení o možnostech změnového řízení např. v důsledku organizačních změn v ČP během dodávky, licenční ujednání a další požadavky vyplývající z bezpečnostní dokumentace ČP a legislativních požadavků (např. ZoKB a jeho vyhlášky, ISO 270xx a podobně).

(3) Za zapracování výše uvedených požadavků do smluvních ujednání odpovídá vedoucí věcně příslušné organizační jednotky, která smlouvu uzavírá.

7.4. Ochrana proti škodlivým programům a škodlivým mobilním kódům

(1) Aktiva ICT ČP musí být chráněna před škodlivým kódem nebo programem (počítačovými viry) odpovídající antivirovou ochranou. Tato ochrana musí plnit jak detekční funkce, tak preventivní opatření k zabránění průniku nebo šíření škodlivého programu či kódu do ICT ČP.

(2) U systému ICT ČP, kde je stanovená povinnost antivirové ochrany, musí být povinně zapnuta rezidentní ochrana a musí být konfigurována tak, aby ji uživatel nemohl vypnout nebo omezit. Výjimku tvoří zaměstnanci se specifickou náplní pracovní činnosti, u které je požadováno vypnutí rezidentní ochrany. Výjimku schvaluje Bezpečnostní manažer ICT ČP.

(3) Za definování opatření antivirové ochrany ICT ČP odpovídá Bezpečnostní manažer ICT. Za implementaci SW nástrojů antivirové ochrany odpovídá správce aktiv.

(4) Antivirový systém je aktualizován po otestování, aktualizace schvaluje manažer bezpečnosti. Virové definice a databáze se aktualizují automaticky.

7.5. Zálohování

(1) K zajištění dostupnosti a integrity informací musí být prováděny zálohy informací a SW.

(2) Za definování pravidel, způsobu a stanovení odpovědností za provádění záloh odpovídá řešitel na základě analýzy dopadů a požadavku Vlastníka/Garanta aktiv.

(3) Za provádění zálohování a za zpracování a vedení provozní dokumentace zálohování odpovídá správce aktiv.

(4) Záložní kopie musí být pořizovány a testovány v pravidelných intervalech.

(5) Odpovědnost za individuální zálohy informací nebo oddělených agend na lokálních ICT ČP je na daném správci aktiva.

7.6. Bezpečnost při zacházení s médii (nosiče informací)

(1) Nosiče informací (interní disky, vyjímatelné disky, USB zařízení, magnetooptická zařízení atd. a informace v listinné podobě) musí být fyzicky chráněny a zabezpečeny proti neautorizovanému přístupu, narušení nebo zneužití informací. Pravidla označování a zabezpečení informací vhodným prostředkem upravuje zejména řád ŘA-3/2010 Spisový řád a směrnice SM-5/2013 Ochrana informací.

(2) Nosiče obsahující chráněné informace musí být ukládány v prostředí ČP na bezpečném místě, a to jak s ohledem na zabezpečení obsahu, tak i zabránění fyzickému poškození nosiče, neoprávněnému nakládání apod. Přístup osob musí být omezen na minimum a schválen a dokumentován. Za bezpečné uložení nosičů informací a manipulaci s nimi zodpovídá každý zaměstnanec, který s nosiči informací v rámci své pracovní činnosti nakládá.

(3) Musí být zajištěna spolehlivá a bezpečná likvidace nosičů informací (např. skartováním) tak, aby na nich uchovávané chráněné informace nebylo možné zpětně obnovit. Za bezpečnou likvidaci nosičů informací odpovídá příslušný správce aktiv nebo koncoví uživatelé ICT ČP. O bezpečné likvidaci nosičů musí být proveden zápis. Likvidace nosičů informací v elektronické formě se řídí přílohou 4 směrnice SM-5/2013 Ochrana informací.

7.7. Výměna informací

(1) Nosiče informací, které obsahují chráněné informace a opouští chráněné prostředí ČP z důvodu předávání či výměny informací, musí být zabezpečeny před nežádoucí manipulací nebo odcizením, viz směrnice SM-5/2013 Ochrana informací a řád ŘA-3/2010 Spisový řád. Výměna informací musí být s externími subjekty smluvně upravena a předem schválena Vlastníkem/Garantem vyměňovaných informací.

(2) Za zabezpečení vyměňovaných informací, včetně smluvního ujednání, zodpovídá jejich Vlastník/Garant. Před zaznamenáním informace na nosič informací je nutno bezpečně odstranit dřívější nebo nepotřebné informace (data).

(3) Všechny informace (s výjimkou veřejných) musí být při odesílání e-mailem mimo ICT ČP prostřednictvím internetu zabezpečeny (viz příloha směrnice SM-5/2013 Ochrana informací).

7.8. Služby elektronického obchodu a další služby

(1) ČP poskytuje služby elektronického obchodu a další služby na veřejně přístupných systémech. V rámci těchto služeb jsou informace přenášeny přes veřejnou síť. Tyto informace musí být chráněny před

podvodnými aktivitami, prozrazením či neoprávněnou modifikací např. šifrováním a elektronickým podpisem.

(2) Za zabezpečení provozu úloh elektronického obchodu odpovídá příslušný správce aktiv.

7.9. Monitorování bezpečnostních událostí

(1) Za účelem detekování událostí, které mohou ovlivnit bezpečnost ICT aktiv ČP, musí být zabezpečeno jejich nepřetržité zaznamenávání formou auditních záznamů. Chronologický sled auditních záznamů musí být zajištěn správným nastavením systémového času a jeho pravidelnou synchronizací jednotným časem ICT ČP.

(2) Auditní záznamy musí být zabezpečeny před neautorizovaným přístupem. Pravidla pro stahování, vyhodnocování a uchovávání auditních záznamů pro případné budoucí vyšetřování bezpečnostních incidentů musí být stanovena v systémových bezpečnostních politikách jednotlivých částí ICT ČP. Pravidla stanovuje bezpečnostní architekt a projektový manažer řídí jejich zapracování v rámci projektu.

8. Řízení přístupu

8.1. Řízení přístupu uživatelů

(1) Přístup k ICT ČP je povolen pouze pro oprávněné (autorizované) uživatele, kterým je přiřazen jednoznačný identifikátor. Samostatný identifikátor je přidělován i přistupujícím aplikacím a softwarovým službám (service). Přístup je povolen na základě autentizace uživatele a schválených přístupových rolí (oprávnění). O přidělení příslušných rolí (oprávnění) musí být proveden písemný nebo elektronický záznam.

(2) Rozsah uživatelských oprávnění se přiděluje principem „need to know“, tedy jsou přidělována pouze taková uživatelská oprávnění, která jsou nezbytná pro plnění pracovních povinností uživatele.

(3) Autorizace uživatele musí být revidována při změně jeho pracovních činností nebo změně jeho funkčního zařazení (typové pozice) a zrušena při zániku jeho pracovněprávního vztahu nebo jiného smluvního vztahu. (např. u externích dodavatelů).

(4) V případě, kdy bylo zjištěno porušení základních zásad bezpečnosti nebo existuje vážné podezření na neoprávněné jednání při použití aktiv, musí být uživateli bezpečnostním administrátorem ve spolupráci se správcem aktiv okamžitě odepřen přístup do ICT ČP.

(5) V ICT ČP je k autentizaci využíváno autentizační tajemství (např. heslo, PIN), autentizační předmět (např. karta, klíč) nebo jedinečné biometrické autentizační informace (např. otisk prstu) nebo nejlépe jejich kombinace. Autentizační tajemství je vždy v kategorii „Citlivá informace“.

(6) Požadavky ke zřízení nebo zrušení přístupu uživatele k ICT ČP, jakož i příkazy ke změně práv uživatele, musí být podávány v písemné nebo prokazatelné elektronické formě (IDM, ServiceDesk) a schváleny nadřízeným/garantem uživatele a příslušným Vlastníkem/Garantem informačních aktiv nebo jím pověřeným zaměstnancem. Realizaci požadavku provádí příslušný správce aktiv nebo je realizována automaticky (IDM).

(7) Administrátoři ICT ČP mají přidělené uživatelské účty s privilegovanými přístupy výhradně určené ke správě ICT ČP. K běžné činnosti uživatele ICT ČP nesmí být privilegované přístupy používány.

(8) Pokud daná část ICT ČP není napojena na systém centrální správy uživatelů (IDM) nebo pokud tento systém centrální správy uživatelů nezohledňuje automaticky změny v pracovní pozici zaměstnance, musí být Vlastníkem/Garantem aktiva ve spolupráci se správcem aktiva každých 12 měsíců zkontrolovány přidělené role a o této kontrole provede správce aktiva zápis do provozního deníku dané části ICT ČP.

(9) Bezpečnostní zásady pro tvorbu, změnu, používání, ukládání, zabezpečení a kvalitu uživatelských hesel jsou definovány v MP-3/2015 Generická systémová bezpečnostní politika ICT, případně jsou dále specifikovány v systémových bezpečnostních politikách jednotlivých částí ICT ČP.

8.2. Odpovědnost uživatelů

(1) Uživatelé jsou povinni dodržovat stanovená pravidla, zachovávat mlčenlivost, nesdělovat svá hesla žádné další osobě, nepoužívat cizí přihlašovací účty a nepoužívat chybně přidělená oprávnění. Hesla a jiná autentizační tajemství musí být náležitě chráněna, nesmí být ponechána na místě, kde by mohlo dojít k jejich kompromitaci jinými osobami. V případě podezření ze zneužití uživatelské identifikace se jedná o bezpečnostní incident a uživatel má povinnost ho nahlásit.

(2) Při opuštění pracoviště uživatelem (i krátkodobém) musí osobní počítače, počítačové terminály apod. uživatel zabezpečit proti neoprávněnému přístupu uzamčením nebo odhlášením.

(3) Každý uživatel, kterému byl umožněn přístup k aktivům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s aktivy a ochranu informací ve své působnosti.

8.3. Řízení přístupu k síti, operačnímu systému a aplikacím

(1) Uživatelé mohou přistupovat k informacím, k operačnímu systému, k síti a funkcím aplikačního systému pouze v souladu s politikou přístupových práv a povolenou úrovní přístupu stanovenou Vlastníkem/Garantem aktiv.

(2) Uživatelé musí mít správcem aktiva na úrovni přístupových oprávnění zakázáno zasahovat do konfigurace systému a upravovat přístupy k informačnímu systému.

(3) Plný přístup k operačním systémům na koncových pracovních stanicích a serverech mají pouze administrátoři, kteří mají oprávnění zasahovat do konfigurace systému a definovat přístupové účty uživatelů.

(4) Každý uživatel se musí korektně přihlašovat k danému systému svým jménem a heslem, příp. jiným povoleným způsobem autentizace uživatele vůči systému.

(5) 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. Návrh opatření provádí bezpečnostní architekt ve spolupráci s Vlastníkem/Garantem aktiva.

8.4. Řízení vzdáleného přístupu

(1) Vzdálený přístup k aktivům je povolen pouze určeným administrátorům, externím subjektům a oprávněným uživatelům zabezpečeným (šifrovaným) způsobem, tj. prostřednictvím VPN (virtuální privátní síť) případně jiným schváleným typem připojení.

(2) Vzdálený přístup schvaluje přímý nadřízený administrátora nebo oprávněného uživatele a určený schvalovatel specializovaného útvaru ICT bezpečnost.

(3) U externích subjektů schvaluje přístup garant externího uživatele a schvalovatel určený Vlastníkem/Garantem aktiva, ke kterým externí subjekt přistupuje.

8.5. Mobilní výpočetní zařízení

(1) Uživatelé jsou povinni manipulovat s mobilními zařízeními (notebooky, chytré telefony-smartphones apod.) tak, aby nedošlo k jejich ztrátě nebo zneužití.

(2) V případě krádeže nebo ztráty je uživatel mobilního výpočetního zařízení povinen toto neprodleně ohlásit jako bezpečnostní incident.

9. Pořízení (akvizice) vývoj a údržba ICT

(1) ICT ČP (včetně nově pořizovaných a vyvíjených částí) musí splňovat požadavky na zabezpečení informací a ochranu dat v průběhu celého životního cyklu v souladu s BPICT, a to i v případě dodavatelského řešení.

(2) Vývoj webových aplikací musí respektovat doporučení sdružení OWASP (Open Web Application Security Project) tak, aby byly schopny odolat případným kybernetickým útokům.

(3) Každá změna v procesu pořízení (akvizice), vývoje a údržby ICT musí být podložená odpovídajícími dokumenty popisujícími tuto změnu a musí obsahovat identifikaci dotčených aktiv, důvod změny a odhad souvisejících rizik a potenciálních dopadů této změny včetně dopadu na bezpečnost informací.

(4) Bezpečnostní požadavky v předmětném projektu v rámci projektového řízení řídí projektový manažer. Definici bezpečnostních požadavků zajišťuje bezpečnostní architekt ve spolupráci s Vlastníkem/Garantem a správcem aktiv.

10. Řešení bezpečnostních incidentů

(1) Každý zaměstnanec ČP, smluvní strany a uživatelé třetích stran jsou povinni hlásit podezření na bezpečnostní incidenty, hrozby a zranitelnosti aktiv na ServiceDesk ČP. Operátor ServiceDesku musí informaci o podezření na incidenty, hrozby a zranitelnosti aktiv předat specializovanému útvaru ICT bezpečnost k řešení.

(2) Bezpečnostní administrátoři musí vést evidenci a vyhodnocovat hlášení o bezpečnostních incidentech a sledovat průběh jejich řešení. O řešení bezpečnostních incidentů informují Bezpečnostního manažera ICT prostřednictvím zprávy o vyhodnocení bezpečnostního incidentu.

(3) Při závažných bezpečnostních incidentech, které mohou vést k disciplinárnímu řízení nebo soudnímu sporu a podobně, musí být bezpečnostními administrátory ve spolupráci se správci aktiv shromážděny důkazy o

činnostech a osobách, které byly příčinou bezpečnostního incidentu. Vždy musí být zajištěna integrita důkazních materiálů.

(4) U důkazů v papírové formě je nutné zajistit originály dokumentů, pořídit záznamy o tom, kdo jej nalezl, kdy, kde a bezpečné je uchovat.

(5) U důkazů v elektronické formě je nutné zajistit kopii všech výměnných médií, informací na pevných discích nebo v paměti počítače (o vytvoření kopie musí být vytvořeny záznamy o tom, kdy, kde a jak, jakými nástroji byla kopie vytvořena, a kdo kopii prováděl), bezpečné uchování logů o všech činnostech a bezpečné uchování kopie médií.

(6) Je-li v rámci řešení bezpečnostního incidentu prováděna forenzní analýza, pak musí být prováděna vždy na kopiích důkazního materiálu.

(7) Bezpečnostní incidenty jsou pravidelně projednávány a hodnoceny. Hodnocení stavu bezpečnostních incidentů předkládá Bezpečnostní manažer ICT Gestorovi bezpečnosti ICT zpravidla v měsíčním přehledu současně se zprávou o jejich řešení. O závažných bezpečnostních incidentech a jejich řešení informuje Bezpečnostní manažer ICT Gestora bezpečnosti ICT neprodleně. Zvládání bezpečnostních incidentů řeší MP-2/2017 Zvládání bezpečnostních incidentů.

11. Řízení kontinuity činností organizace

11.1. Základní aspekty

(1) Cíle řízení kontinuity činností organizace jsou detailně popsány ve směrnici SM-8/2017 Politika Systému řízení kontinuity podnikání (BCM) . Cílem je především minimalizace dopadů plynoucích z přerušení dodávky služeb poskytovaných ČP či jiných činností v případě vzniku neočekávané nebo nepříznivé události (mimořádná událost). V oblasti ICT to znamená zejména ochranu před následky závažných selhání informačních systémů a zajištění včasné obnovy ICT aktiv a služeb v případě havárie.

(2) Vlastníci/Garanti aktiv musí před jejich uvedením do provozu a dále v průběhu provozu identifikovat kritické procesy, a činnosti a aktiva, které je nutno obnovit či nahradit při přerušení nebo výpadku ICT služeb. Pro tyto procesy a aktiva zpracovává správce aktiv Plán obnovy ICT (požadavky na zpracování DRP plánů a BCP jsou uvedeny v SM-8/2017). Minimální úroveň poskytovaných služeb určuje Vlastník/Garant aktiva.

(3) Pro každý kritický proces musí být stanoven časový úsek maximálního akceptovatelného přerušení, v jehož průběhu je nutné zajistit obnovu procesu. Časový úsek maximálního akceptovatelného přerušení stanovuje Vlastník/Garant aktiva na základě analýzy dopadů (BIA).

(4) Požadavky na zálohování systémů a dat, tj. způsob, četnost, periodicitu ukládání, dostupnost a možnost obnovy musí korespondovat s požadavky na dostupnost, maximální akceptovatelnou dobu přerušení procesu a maximální akceptovanou ztrátu dat.

11.2. Plány obnovy ICT

(1) Plány obnovy ICT ČP musí rozpracovávat popisy postupů a potřebných zdrojů pro obnovu zařízení a služeb ICT ČP zajišťujících kritické procesy. Plány obnovy ICT ČP musí pokrývat všechny scénáře narušení (při

výpadku části systému, výpadku celého systému, výpadku podpůrné infrastruktury, výpadku více systémů, výpadku lokality, ztráty dodavatele či obsluhy, atd.).

(2) Plány obnovy musí odpovídat stanoveným požadavkům na obnovu (časy obnovy, ztráta dat, stav po obnově), přičemž za jejich zpracování odpovídá správce aktiv.

11.3. Testování a aktualizace plánů obnovy ICT

(1) Kontrola a aktualizace plánů obnovy musí být správcem aktiv ve spolupráci s Vlastníkem/Garantem aktiv provedena minimálně jednou ročně. Testování plánů musí být prováděno minimálně jednou ročně u systémů zajišťující kritické procesy, jednou za dva roky u ostatních systémů a po každé zásadní změně v systému. Testování musí být v souladu s provozními možnostmi a se schválením Gestora bezpečnosti ICT.

(2) Forma testování je dána směrnicí SM-8/2017 a musí zajistit dostatečnou jistotu, že plány obnovy jsou funkční a splňují stanovené požadavky na obnovu.

(3) Součástí testu plánů obnovy ICT musí být protokol o výsledcích testu obsahující případné požadavky na aktualizaci plánů obnovy.

12. Řízení shody

12.1. Vyhodnocení účinnosti systému řízení bezpečnosti

(1) Gestor bezpečnosti ICT ve spolupráci s Bezpečnostním manažerem ICT zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně. Zprávu z přezkoumání systému řízení bezpečnosti informací ISZS předloží vedení ČP.

(2) Gestor bezpečnosti ICT na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami zajistí odpovídající aktualizaci systému řízení bezpečnosti informací a příslušné dokumentace.

12.2. Zajištění shody se zákonnými požadavky

(1) Pro ICT ČP nebo jednotlivé části musí být Vlastníkem/Garantem aktiv určeny, dokumentovány a udržovány aktuální veškeré relevantní zákonné, regulatorní a smluvní požadavky a musí být Vlastníkem/Garantem aktiv s nimi zajištěn soulad.

(2) K zajištění souladu licenčních ujednání s legislativními požadavky musí být Správcem sw licencí prováděna evidence a sledování počtu zakoupených licencí a včasné plánování nákupu potřebných licencí.

(3) Veškeré smlouvy související s dodávkou nebo užíváním aplikací vytvářených na zakázku pro ČP externími výrobci/dodavateli musí obsahovat ujednání o poskytnuté licenci v souladu se zákonem č.121/2000 Sb., autorským zákonem.

(4) Veškeré smlouvy uzavřené s významnými dodavateli ČP musí obsahovat relevantní položky z přílohy 7 VoKB (82/2018 Sb.). Významné dodavatele určuje Gestor bezpečnosti ICT na návrh Bezpečnostního

manažera ICT. Seznam významných dodavatelů podléhá kontrole aktuálnosti minimálně jednou ročně, kterou provádí Bezpečnostní manažer ICT.

(5) ČP vykonává svým jménem a na svůj účet autorská majetková práva k dílu, které zaměstnanec vytvořil ke splnění svých povinností vyplývajících z pracovněprávního vztahu k ČP.

(6) Tato práva i povinnosti jsou upraveny v § 58 zákona č. 121/2000 Sb., o právu autorském a zůstávají nedotčena i po skončení pracovněprávního vztahu.

(7) Osobní údaje odpovídající definici Nařízení Evropského parlamentu a rady (EU) 2016/679 v režimu zákona 110/2019 Sb. musí být v ČP zabezpečeny odpovídajícím způsobem proti zneužití a neoprávněnému přístupu. V rámci ČP se jejich ochrana řídí směrnicí SM-5/2013 Ochrana informací a směrnicí SM-8/2013 Ochrana osobních údajů.

(8) Provoz informačního systému kritické informační infrastruktury se řídí ZoKB a prováděcí vyhláškou 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) v platném znění.

12.3. Audit kybernetické bezpečnosti

(1) Bezpečnostní auditor zajišťuje 1x ročně provedení auditu kybernetické bezpečnosti, který hodnotí správnost a účinnost zavedených bezpečnostních opatření.

(2) V rámci auditu kybernetické bezpečnosti je posuzován soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k provozovaným informačním systémům.

12.3.1. Soulad s bezpečnostními politikami a řídícími dokumenty ČP

(1) Vedoucí zaměstnanci organizačních jednotek ČP musí zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně v souladu s touto Bezpečnostní politikou ICT a navazujícími řídicími dokumenty ČP.

(2) Jednou ročně musí být provedena kontrola dodržování Bezpečnostní politiky ICT specializovaným útvarem ICT bezpečnost případně externím dodavatelem.

(3) Průběh a závěry kontrol musí být zdokumentovány a výsledky těchto kontrol musí být rovněž zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

(4) Kontrolu shody ICT ČP na úrovni souladu s bezpečnostními politikami lze provádět manuálně nebo pomocí automatizovaných SW prostředků včetně bezpečnostních testů. Intervaly, rozsah a pravidla kontroly stanovuje MP-3/2015 Generická systémová bezpečnostní politika ICT nebo systémové bezpečnostní politiky jednotlivých částí ICT ČP, případně kontrola může proběhnout na základě rozhodnutí Gestora bezpečnosti ICT, Bezpečnostního manažera ICT nebo Vlastníka/Garanta či správce aktiv.

(5) Při zavádění nových aktiv nebo při významné změně stavu stávajících aktiv musí být posouzen soulad s bezpečnostními politikami ICT ČP.

(6) Bezpečnostní testy musí být prováděny pouze k tomu pověřenými zaměstnanci nebo dodavateli vždy se souhlasem Bezpečnostního manažera ICT. V ostatních případech jsou bezpečnostní testy zakázány.

(7) Výsledky kontroly shody bezpečnosti s bezpečnostní politikou ICT a bezpečnostních testů musí být vyhodnoceny a zdokumentovány. K identifikovaným neshodám schvaluje Bezpečnostní manažer ICT bezpečnostní opatření.

13. Související dokumenty

(1) Tato BPICT je dále rozpracována v navazující interní bezpečnostní dokumentaci divize ICT a eGovernment.

(2) Veškerá navazující interní bezpečnostní dokumentace divize ICT a eGovernment musí být zpracovávána, přezkoumávána a aktualizována průběžně v souladu s rozvojem ICT ČP.

(3) Za zpracování, přezkoumání, aktualizaci a distribuci bezpečnostní dokumentace odpovídá Bezpečnostní manažer ICT. BPICT je přezkoumávána minimálně jedenkrát ročně.

INTERNÍ DOKUMENTACE DICTG **Intranet -> Odborné úseky->ICT->Bezpečnost ICT->Bezpečnostní dokumentace**	
Bezpečnostní dokumentace dle požadavků ZoKB: ▪ Zpráva o hodnocení aktiv a rizik. ▪ Plán rozvoje bezpečnostního povědomí. ▪ Stanovování cílů systému bezpečnosti informací.	
Systémové bezpečnostní politiky jednotlivých částí ICT ČP – interní dokumenty divize ICT a eGovernment, které budou průběžně zpracovávány pro jednotlivé části ICT ČP a zpřístupňovány na Intranetu ČP URL https://intranet.ceskaposta.cz/web/intranet/bezpecnostni-dokumentace.	
Metodické pokyny pro uživatele ICT ČP např. v oblasti antivirové ochrany, šifrování apod., které budou průběžně zpracovávány a jsou průběžně zpřístupňovány na Intranetu ČP URL https://intranet.ceskaposta.cz/web/intranet/bezpecnostni-dokumentace.	
INTERNÍ DOKUMENTACE	
SM-5/2013	**Ochrana informací**
SM-20/2011	Řízení rizik
MP-12/2011	Řízení rizik v ISMS
ŘA-3/2010	Spisový řád
SM-8/2017	Politika systému řízení kontinuity podnikání (BCM)
ŘA-3/2015	Globální bezpečnostní politika
OP-4/2016/GŘ	Pravidla řízení za krizových situací
MP-3/2015	**Generická systémová bezpečnostní politika ICT**
MP-2/2015	**Bezpečnostní příručka uživatele ICT ČP**
ŘA-4/2012	Pracovní řád České pošty, s.p.
SM-8/2013	**Ochrana osobních údajů**

SM-5/2016	Projektové řízení
SM-19/2011	Vnitřní kontrolní systém v ČP
SM-12/2011	Správa SW aktiv ČP
Opatření - 58/2010	Operativní evidence prvků ICT
RO-304/2016/GŘ	Jmenování bezpečnostních rolí informačního systému kritické informační infrastruktury
EXTERNÍ DOKUMENTACE	
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 likvidaci dat (vyhláška o kybernetické bezpečnosti)**
zákon č. 262/2006 Sb.	zákoník práce
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)

14. Přechodná a závěrečná ustanovení

(1) Vedoucí zaměstnanci organizačních jednotek ČP zajistí, aby s touto směrnicí byli v potřebném rozsahu prokazatelně seznámeni všichni jim podřízení zaměstnanci, kteří přicházejí do styku s aktivy.

(2) Výklad a případnou aktualizaci této směrnice zajišťuje specializovaný útvar ICT bezpečnost.

(3) Výjimku a délku platnosti výjimky z plnění konkrétních ustanovení této směrnice uděluje Bezpečnostní manažer ICT. 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.

(4) Struktura bezpečnostní dokumentace je zveřejněna na Intranetu ČP v sekci (Odborné úseky > ICT > Bezpečnost ICT). Tento přehled průběžně aktualizuje specializovaný útvar ICT bezpečnost.

15. Přílohy

POŘADÍ	NÁZEV PŘÍLOHY
1.	Politika systému řízení bezpečnosti informací v kybernetickém prostoru
2.	Fyzický perimetr Informačního systému základních služeb ČP – příloha je označena kategorií Důvěrné dle směrnice SM-5/2013 Ochrana informací a v souladu s touto směrnicí je s přílohou třeba nakládat.
3.	Logický perimetr Informačního systému základních služeb ČP

4.	Garanti aktiv Informačního systému základních služeb ČP (určení dle požadavku zákona o kybernetické bezpečnosti)

Politika systému řízení bezpečnosti informací v kybernetickém prostoru

ČP je důvěryhodným poskytovatelem kvalitních služeb v oblasti zprostředkování informací, plateb a zboží tradičními i elektronickými formami. ČP využívá při svých činnostech informace týkající se obyvatel ČR a vnímá povinnost zajištění bezpečnosti informací v kybernetickém prostoru ČP, ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho prováděcích předpisů, za jednu ze svých priorit.

Pro zajištění kybernetické bezpečnosti ČP, tj. pro řízení bezpečnosti informací v kybernetickém prostoru, deklaruje ČP tyto principy:

1. Kybernetická bezpečnost ČP je centrálně řízena prostřednictvím systému řízení bezpečnosti informací, a to včetně kybernetických bezpečnostních událostí, incidentů a komunikace s Národním úřadem pro kybernetickou a informační bezpečnost.
2. Minimálně jednou za 2 roky a při významných změnách probíhá audit kybernetické bezpečnosti.
3. Důsledně jsou využívány standardizované postupy a ověřené technologie.
4. Směřování rozvoje kybernetické bezpečnosti:
   a) řídí se dle platných právních předpisů ČR, které respektují evropskou legislativu a na tomto základě jsou v rámci ČP zpracovány příslušné interní normy,
   b) zohledňuje mezinárodní a národní smlouvy o sdílení a výměně informací,
   c) je realizováno na základě průběžného sledování a vyhodnocování aktuálního vývoje kybernetických hrozeb a jejich možného dopadu na důvěrnost, integritu a dostupnost aktiv spravovaných ČP.
5. ČP při zajišťování kybernetické bezpečnosti spolupracuje s relevantními národními institucemi.
6. Při plánování rozvoje a provozu informačních a komunikačních technologií a při volbě bezpečnostních opatření k minimalizaci identifikovaných kybernetických hrozeb, zranitelností a rizik, postupuje ČP vždy, jako dobrý hospodář tzn., zavádí bezpečnostní opatření důsledně se stanovenou mírou přijatelnosti kybernetických rizik.
7. Všichni zaměstnanci ČP jsou poučeni v oblasti kybernetické bezpečnosti.
8. Činnosti nevykonávané zaměstnanci ČP jsou zajišťované pečlivě vybranými dodavateli, kteří procházejí pravidelným hodnocením spolupráce a se kterými jsou nastavené dohody směřující k zabezpečení informací.

V Praze dne

……..

Ing. Roman Knap

generální ředitel ČP

Logický perimetr Informačního systému základních služeb ČP

1. Úvodní ustanovení

(1) Tento dokument definuje logický bezpečnostní perimetr Informačního systému základních služeb ČP - ISZS, který je vymezen poskytováním následujících služeb:

a) služba dodání poštovních zásilek do 2 kg,

b) služba dodání poštovních balíků do 10 kg,

c) služba dodání peněžní částky poštovním poukazem,

d) služba dodání doporučených zásilek, kterou se rozumí služba poskytující záruku náhrady škody v paušální výši pro případ ztráty, poškození nebo úbytku obsahu poštovní zásilky a dávající odesílateli důkaz o poštovním podání poštovní zásilky a případně na jeho žádost důkaz o jejím dodání adresátovi,

e) služba dodání cenných zásilek, kterou se rozumí služba poskytující záruku náhrady škody pro případ ztráty, poškození nebo úbytku obsahu poštovní zásilky, a to až do výše odesílatelem udané hodnoty poštovní zásilky,

f) služba bezúplatného dodání poštovních zásilek do 7 kg pro nevidomé osoby,

g) služba, které musí být zajištěny na základě závazků vyplývajících z členství České republiky ve Světové poštovní unii.

(2) Na základě těchto služeb byly stanoveny následující prvky kritické infrastruktury ČP:

a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,

b) sběrný přepravní uzel,

c) řídící a mezinárodní pošta,

d) poštovní dopravní infrastruktura.

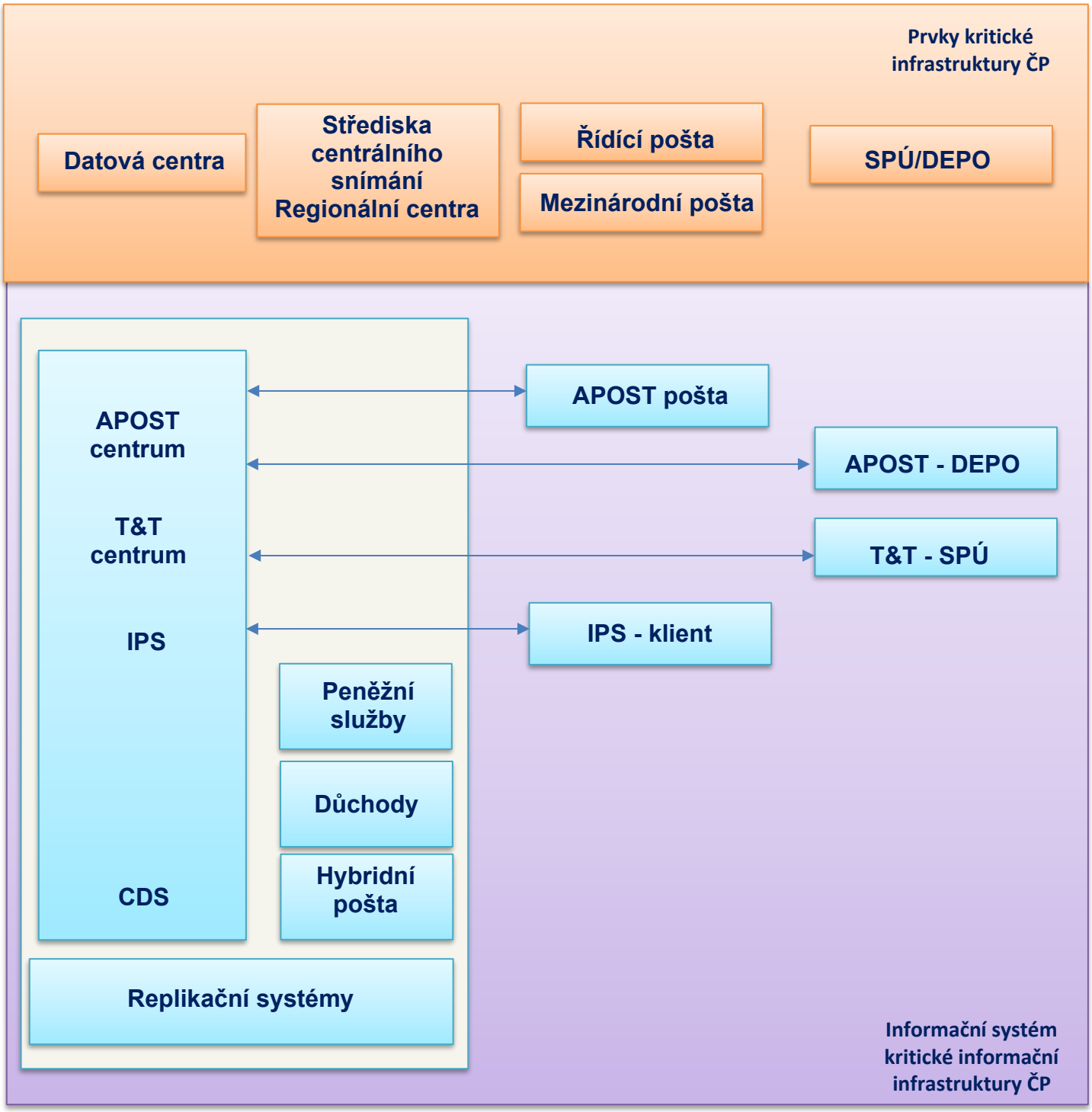
(3) K zajištění činností jsou používány následující aplikace/systémy:

Aktivum	Název aktiva	Popis aktiva
EFLOW (eFlow)	EFLOW_eFlow	SW pro skenování, vyhodnocování dokumentů
HP (Hybridní pošta)	HP_Hybridní pošta	Informační systém pro příjem zakázek, statistiku evidenci a řízení procesu zpracování zakázek až po předání podkladů k fakturaci. Systém má centrální a střediskovou část, které si vyměňují data pomocí replikací. Skládá se z HP-C_Hybridní pošta - centrum a HP-R_Hybridní pošta - regiony.
INS (Inspire)	INS_Inspire	SW pro vývoj tiskových aplikací - dynamické a podmíněné formátování
PRI (Prisma)	PRI_Prisma	SW pro řízení tiskových front pro produkční tiskárny.
UPU (Brána do poštovní unie)	UPU_Brána do poštovní unie	Rozhraní pro výměnu dat s Mezinárodní poštovní únií

IPS (Mezinárodní poštovní systém)	IPS_Mezinárodní poštovní systém	Aplikace pro evidenci a sledování mezinárodních zásilek. Aplikace používaná na vyměňovacích poštách Praha 120, Cheb 120 a Břeclav 120
MPS (Zpracování mezinárodních poštovních peněžních služeb)	MPS	Aplikace pro zajištění provozu poštovního styku na základě mezinárodní dohody, úmluvy a ujednání. Aplikace určená pro zpracování mezinárodních plateb na poukázkách
APOST-CEN (APOST - Centrum)	APOST-POSTA_APOST Pošta	Klientská část aplikace APOST (na poštách) - zahrnuje nAPOST, xAPOST, xAPOST2. Dále zahrnuje APOST-EXT_APOST Externí služby (Aplikace zajišťuje veškeré online služby externích partnerů (BankService, Celní správa, ČSOB, Datový Trezor, IZIP, PES, QPostal, SIPO, SuperCASH) pro aplikaci APOST-ONLINE. Jsou provozované na klientských stanicích automatizované pošty APOST), APOST-ONLINE_APOST Online ověřování (Aplikace zajišťuje veškeré online služby provozované na klientských stanicích automatizované pošty APOST.Aplikace poskytuje následující aplikační služby:Centrální dodávací záznam, SZK, Master Data management (podpora vyhledání adres), ZPRO - zprostředkování prodejeTIPSPORT, SAZKA, CZP - ověření dokladu, Předání dat MRN z Celní správy, Ověřování ABC, Ověřování ABD, Ověřování ARES, Archivace CZP, Ověřování Šekových, vkladových a úrokových Pk, Příděly a odvody hotovosti, Centrální číselník klientů (CCK), Bankovní služby, CCP Služby centrálního ceníku, Centrum denního zúčtování, CPoj Česká pojišťovna,Předávání MRN VVD z Celní správy, DBS Ověřování DB Sankcionovaných subjektů, Dobíjení kreditu mobilních telefonů (DCP), DINO, FTS Služby pro přenos souboru na pošty, LDAP ověření dat zaměstnanců, JISKRO kontrola průkazů zaměstnanců, MRE mezinárodní reklamace, NDS ověření důchodových Pk, Zápis dat zásilek do centra, Předání dat zásilek na pošty, PES - Western union, Předávání dat PNC na pošty), xAPOST2_xAPOST - CentOS (Náhrada stávajícího OS pro xAPOST SuSe novým CentOS (LinuxBOX) pro pošty (aplikace xAPOST, klient Checkpoint 602 XML Filler, Mozilla Thunderbird, Mozilla Firefox, Libre Office kompatibilní s Microsoft Word a Excel, ESET antivirus, PDF prohlížeč, ovladače pro Tokeny, runtime Java, Citrix receiver, souborový manažer, security modul pro tlačítko tísně, nástroj pro Printscreen, uživatelské aplikace PS ČSOB), APOST_Systém APOST (Systém na podporu činností na poštách. Jedná se o front-end systém poštovního provozu, který navazuje na řadu dalších služeb. Systém zajišťuje veškeré poštovní služby provozované na klientských stanicích na poštách. Dále obsahuje moduly pro synchronizaci a přenos souborů mezi poštami a Centrem, prezentaci dat z žurnálů a komunikaci s externími službami).
APOST-POSTA (APOST - Pošta)	APOST-CEN_APOST Centrální část	Serverová (centrální) část systému APOST. Dále se skládá z APOST-CI_APOST Centrální nalívání (Zpracování souborových dat z pošt), APOST-FMS_APOST File Management Systém (Zajišťuje přenos souborů z centra na pošty a opačně, dále zajišťuje centrální zpracování souborů balíků a žurnálu z pošt), APOST-PORTAL_APOST Interní portál (Webová aplikace sloužící k prezentaci výstupů z žurnálů. Informační modul nad poštami a vybranými daty APOST), CDS-PES_PES - Boxing dat APOST (Boxing dat APOST, přenos dat do systému SAP).

CRYPTA	CRYPTA2_Crypta 2	Aplikace na podpis, šifrování a dešifrování souborů. Přímá náhrada za původní aplikaci Crypta 1.3.
NDS	NDS_Důchodová služba	Systém evidence kmene důchodců a jeho průběžná aktualizace změnami z ČSSZ a pošt, centrální zpracování a vedení dat potřebných k výplatám důchodů.
PID (Prohlížení image dokladů)	PID_Prohlížení image dokladů	Prohlížení aktuálního stavu a Image všech typů Pk.
PPS (Zpracování poštovních peněžních služeb)	PPS_Poštovní platební styk	Platební styk pro převody peněžních částek, zahrnuje aplikace FTM, IMG, PID, PKA, PKB, PKC, PPS-RZPK.
	PPS-PM_Poštovní platební styk - podpůrné moduly	Zahrnuje aplikace, které jsou pro více subsystémů (např. Centrální statistické práce s Pk (cpkstat.exe), Tiskové práce Pk (cpktisk.exe), Centrální archivní práce s Pk (cpkarch.exe), Centrální zpracování - prohlížení přijatých Pk (najdi_pk.exe), monitoring stavu párování atd.)
T&T	TNT-PE_Poštovní editor	Systém pro evidenci jízdních řádů kurzů.
	TNT-SVAZ_Potisk svazovek	Systém pro evidenci a potisk svazovek na SPU.
	TNT-SPU_Track and Trace SPU	Základním účelem aplikace je zajistit softwarovou evidenci informací o průchodu sledovaných balíkových zásilek poštovní přepravou.
	TNT_Track and Trace	Základním účelem aplikace je zajistit softwarovou evidenci informací o průchodu sledovaných balíkových zásilek poštovní přepravou.
	TNT-ZRE_Interní prohlížení zásilek	Interní prohlížení zásilek na URL zasilky.cpost.cz
	TNT-TD_Track and Trace Trans Data	Regionální část TNT zahrnující komunikační servery na jednotlivých SPU.
CDS	CDS_Centrální datový sklad	Architektura CDS modelu, zajištění reportingu ČP, analytické aplikace
Replikační systémy	RS-CEN	Replikační systém centra.
	RS-REG	Replikační systém regionální.
	RS-PPS	Replikační systém PPS.

2. Základní schéma logického perimetru ISZS



Garanti aktiv Informačního systému základních služeb ČP

(určení dle požadavku zákona o kybernetické bezpečnosti)

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
ředitel útvaru logistika	**SPU - poštovní přeprava**		Klíčové činnosti: Služba zajišťuje poštovní přepravu zásilek (tzv. velkou logistiku) zahrnující jak silniční, tak železniční dopravu. Součástí služby jsou činnosti sestavování plánu přepravy, tvorba jízdních řádů poštovních kurzů, zajišťování a realizace plánu poštovní přepravy v celém atrakčním obvodu SPU a určené části hlavní přepravní sítě, zpracování poštovních zásilek podaných v atrakčním obvodu SPU a určených k dodání do atrakčního obvodu SPU, vedení poštovních kurzů ObPS, příslušné části HPS a vybraných kurzů ÚPS, vyhodnocování kvality služby a řešení plánů při odchylkách od standardního provozního režimu.
	SPU - třídění zásilek		Klíčové činnosti: SPU jsou hlavními třídícími centry zásilek v logistické síti ČP a jsou vybavené třídícími stroji. Veškeré zásilky se svážejí z podacích provozoven k roztřídění do SPU. Automatické třídění se provádí prostřednictvím specializované třídící technologie. Ruční třídění se provádí pro specifické typy zásilek (nadrozměrné, nestandardní rozměry) nebo zásilky, které automatizovaným způsobem třídit nelze.
	Data o stavu vnitrostátní zásilky (T&T)		Kategorie dat: Citlivé (osobní údaje)
	Data poštovních kurzů		Kategorie dat: Interní
		T&T	Aplikace je složena z modulů: T&T-MZ (T&T-Mezinárodní), T&T-PE (Poštovní editor), T&T-PS (Potisk svazovek), T&T-PZ (Prohlížení zásilek), T&T-SPU (T&T-Vnitrostátní).
		Třídící stroje	Koncová zařízení, využívají data z aplikace APOST.
manažer specializovaného útvaru mezinárodní poštovní provoz	**Mezinárodního poštovní provoz**		Klíčové činnosti: Řídí a organizuje mezinárodní poštovní provoz a mezinárodní poštovní přepravu listovních a balíkových zásilek. Součástí služby je třídění a zpracování mezinárodních zásilek v Praze, Břeclavi a Chebu.
	Data přepravní pro mezinárodní zásilky		Kategorie dat: Citlivé (osobní údaje)
		IPS (Mezinárodní poštovní systém)	Aplikace
		PNGUPU (Brána do poštovní unie)	Aplikace
manažer specializovaného útvaru hybridní pošta	**PostServis - Příprava zakázek**		Klíčové činnosti: Probíhá příprava grafické podoby tisků, příprava programů tisku a řízení linek.
	PostServis - Tisk a Kompletace		Klíčové činnosti: Hromadný tisk a kompletace (obálkování) dokladů pro NDS (Důchody), PKB a PKC, SIPO, Česká spořitelna (TOC), ČSOB, Homecredit, Česká pojišťovna, O2 - výpisy.
	Data požadavků pro zpracování zásilek,		Kategorie dat: Interní

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
	data HP, podklady fakturace		
	Data pro tisk a kompletaci zásilek (spooling)		Kategorie dat: Citlivé (osobní údaje)
		HP (Hybridní pošta)	Aplikace
		INS (Inspire)	Aplikace: SW pro vývoj tiskových aplikací - dynamické a podmíněné formátování.
		PRI (Prisma)	Aplikace: SW pro řízení tiskových front pro produkční tiskárny.
		Typový samostatný server v serverovně lokality	Typy serverů: Jedná se o servery, které jsou umístěny mimo DC ČP. Jejich provoz je zajišťován zaměstnanci hybridní pošty.
manažer útvaru řízení doručovací sítě	**Dodací účelová síť - depo - přeprava**		Klíčové činnosti: Služba zajišťuje přepravu zásilek mezi SPU - DEPO - zákazník. Zahrnuje cca 71 Dep, 11500 okrsků. Zásilky jsou skenovány do APOSTu. Sledování v T&T.
	Dodací účelová síť - depo - služba hromadného podání		Klíčové činnosti: Služba zajišťuje hromadné podání zásilek na depu.
	Data hromadného podání zásilek		Kategorie dat: Citlivé (osobní údaje)
manažer specializovaného útvaru zpracování peněžních služeb	**Peněžní služby - zpracování poukázek - A**		Klíčové činnosti: V rámci služby jsou zpracovávány poukázky typu A a A-V, s výjimkou poukázky typu A - daňová složenka. Podstatou služby je zajištění převodu hotovosti složené klientem na přepážce na bankovní účet. V rámci služby je prováděno skenování a OCR převod na strukturovanou podobu dat.
	Peněžní služby - zpracování poukázek - daňová složenka		Klíčové činnosti: V rámci služby jsou zpracovávány poukázky typu A, přičemž jsou uzavřeny specifické smluvní podmínky s GFŘ. U poukázek je prováděno skenování a OCR převod na strukturovanou podobu dat. Mimo smlouvy s GFŘ jsou uzavřeny smlouvy s jednotlivými krajskými FÚ a jsou definována pravidla elektronické komunikace.
	Peněžní služby - zpracování poukázek - B		Klíčové činnosti: V rámci služby jsou zpracovávány poukázky typu B. Služba zajišťuje převod peněz z účtu na hotovost formou výplatní poukázky. Vzhledem k tomu, že data jsou pořízena již na začátku procesu elektronicky (případně jsou zaměstnanci ČP z papírové podoby manuálně převedena do elektronické podoby) není v procesu zpracování prováděno skenování a OCR převod na strukturovanou podobu dat.
	Peněžní služby - zpracování poukázek - C		Klíčové činnosti: V rámci služby jsou zpracovávány poukázky typu C. Služba zajišťuje převod hotovosti na hotovost. Poukázky typu C vznikají při podání obdobně jako poukázky A, na výstupu jsou doručovány jako poukázky B.

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
	Peněžní služby - zpracování poukázek - D		Klíčové činnosti: V rámci služby jsou zpracovávány poukázky typu D. Služba zajišťuje převod hotovosti na hotovost. Poukázky typu D vznikají na rozdíl od ostatních typů až v průběhu/resp. po realizaci hotovostního převodu. Hotovostní převod je realizován postupy definovanými mezi poštovními pobočkami a jako takový probíhá mimo systém. Zpracování poukázek D je tedy formálním dokončením již poskytnuté služby, tak aby byla relevantní data o transakci regulérně zanesena do příslušných systémů.
	Peněžní služby - zpracování platebních příkazů		Klíčové činnosti: V rámci služby jsou realizovány téměř všechny platební příkazy k úhradě realizované ze strany ČP. Službu zajišťuje ČSOB. Na tuto službu jsou napojeny jak business služby ČP (např. peněžní poukázky A, B, C, SIPO, NDS,…) tak i interní/podpůrné služby jako úhrada mezd, daní, pojistného, dodavatelských faktur apod.
	Mezinárodní peněžní služby - zpracování poukázek		Klíčové činnosti: V rámci služby jsou realizovány mezinárodní peněžní služby - zpracování poukázek typu Z/A (Hotovost-Účet) a Z/C (Hotovost-Hotovost). Podání probíhá na pobočkách, služba je limitována částkou, kterou je možné zaslat a cílovou zemí. Součástí služby je i skenování a tvorba dávky pro tisk poukázek.
	Data zpracování poukázek - strukturovaná data		Kategorie dat: Citlivé (osobní údaje)
	Data zpracování poukázek - image		Kategorie dat: Citlivé (osobní údaje)
	Data komunikace s ČSOB		Kategorie dat: Interní
	Data mezinárodních poukázek		Kategorie dat: Citlivé (osobní údaje)
		MPS (Zpracování mezinárodních poštovních peněžních služeb)	Aplikace je složená z modulů: MPS_SS-B (Béčka), MPS_SS-BP (Bankovní převody), MPS_SS-D (Dobírky), MPS_SS-DEV (Devizové vyúčtování), MPS_SS-ETK (Etikety), MPS_SS-KV (Kontrola PSČ v VDS pro OZ Stč a vyúčtování PkB), MPS_SS-PPL (Poplatky), MPS_SS-SPS (Statistické výpočty střediska peněžních služeb), MPS_SS-TNB (Tisk PkB nepřijatých k výplatě), MPS_SS-VRA (Vratky), MPS_SS-VUZ (Výpisy z účtu)
		PPS (Zpracování poštovních peněžních služeb)	Aplikace je složená z modulů: PPS-AC (Poukázky A, C), PPS-AC-CV (Centrální výplata Pk A), PPS-AC-CZA (Centrální zpracování Pk A), PPS-AC-CZCD (Centrální zpracování Pk C, D), PPS-AC-CZCD-EVD (Centrální zpracování - emitace výplatních dokladů Pk C,D), PPS-AC-UC (Údržba číselníku Pk A), PPS-AC-VI (Centrální výběr image), PPS-B (Poukázky B - NPS - Nový platební styk), PPS-B-CS (Centrální snímání Pk B), PPS-B-CZ (Centrální zpracování Pk B), PPS-B-CZA (Centrální zpracování-práce s archivem vyúčtování Pk B), PPS-B-GK (Generování kódů pro ČSOB (vyúčtování B)), PPS-FTM (FTM - přenosy souborů), PPS-nPkB (nPkB), PPS-PM-CAP (Centrální archivní práce s Pk)

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
manažer specializovaného útvaru regionálního zpracování peněžních služeb Praha	**Regionální zpracování peněžních služeb**		Klíčová činnost: Zajišťuje systém centrálního snímání, digitalizace a vyhodnocování dat v aplikaci peněžních služeb
		PID (Prohlížení image dokladů)	Aplikace: PPS-RZPK (Regionální zpracování Pk), PPS-RZPK-ADMIN (Administrátor Pk), PPS-RZPK-IK (Import Kodak), PPS-RZPK-KP (Kontrola příjmu Pk), PPS-RZPK-PI (Přenos image region/CVS), PPS-RZPK-PPK (Přenos Pk A do CVS), PPS-RZPK-PRZ (Proložky – regionální zpracování), PPS-RZPK-SV (Stanice výjimek)
		EFLOW (eFlow)	Aplikace: SW pro skenování, vyhodnocování dokumentů
		Vysokorychlostní scanner	Koncová zařízení
		Typový samostatný server v serverovně lokality	Typy serverů: Jedná se o servery, které jsou umístěny mimo DC ČP. Jejich provoz je zajišťován zaměstnanci odboru regionálního zpracování peněžních služeb.
		DB-SYBASE-DC	Databáze
manažer specializovaného útvaru regionálního zpracování peněžních služeb Ostrava	**Regionální zpracování peněžních služeb**		Klíčová činnost: Zajišťuje systém centrálního snímání, digitalizace a vyhodnocování dat v aplikaci peněžních služeb
		PID (Prohlížení image dokladů)	Aplikace: PPS-RZPK (Regionální zpracování Pk), PPS-RZPK-ADMIN (Administrátor Pk), PPS-RZPK-IK (Import Kodak), PPS-RZPK-KP (Kontrola příjmu Pk), PPS-RZPK-PI (Přenos image region/CVS), PPS-RZPK-PPK (Přenos Pk A do CVS), PPS-RZPK-PRZ (Proložky – regionální zpracování), PPS-RZPK-SV (Stanice výjimek)
		EFLOW (eFlow)	Aplikace: SW pro skenování, vyhodnocování dokumentů
		Vysokorychlostní scanner	Koncová zařízení
		Typový samostatný server v serverovně lokality	Typy serverů: Jedná se o servery, které jsou umístěny mimo DC ČP. Jejich provoz je zajišťován zaměstnanci odboru regionálního zpracování peněžních služeb.
		DB-SYBASE-DC	Databáze
manažer specializovaného útvaru zpracování centrálních úloh	**Zpracování služeb - NDS (Národní důchodová služba)**		Klíčové činnosti: Komplexní zpracování Důchodové služby včetně vyúčtování s ČSSZ na základě Mandátní smlouvy o výkonu důchodové služby uzavřené mezi Českou správou sociálního zabezpečení a ČP, s.p. Jedná se o zprostředkování výplaty důchodů v hotovosti prostřednictvím výplatních dokladů.
	Data NDS		Kategorie dat: Citlivé (osobní údaje)
		NDS	Aplikace je složena z modulů: NDS (Důchodová služba), NDS-ARCHIV (Lokální aplikace pro prohlížení dat z archivu), NDS-CSSZ (Aplikace pouze pro uživatele ČSSZ).

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
manažer útvaru poštovní technologie	**Poštovní technologie**		Klíčové činnosti: Agenda provozní kontroly provozních technologií. Agenda technologie balíkových a listovních služeb. Agenda technologie finančních služeb. Agenda autom. technol. poštovních služeb Agenda technologie nepoštovních služeb
	Centrální data APOST		Kategorie dat: Citlivé (osobní údaje)
	Centrální ceník produktů		Kategorie dat: Interní
		APOST-CEN (APOST - Centrum)	Aplikace
		APOST-POSTA (APOST - Pošta)	Aplikace
manažer specializovaného útvaru provozní kontroly a reklamace	**Reklamace a stížnosti**		Agenda reklamační a náhradové řízení. Agenda vyřizování a evidence stížností. (EMS - „Rugby“, u balíků v systému „Cricket“).
	Provozní kontrola		Agenada provozní kontroly.
	Poštovní úložna		Agenda poštovní úložny.
manažer specializovaného útvaru oběh hotovosti a cenin	**Zajištění zásobování pobočkové a dodávací sítě hotovostí a ceninami**		Klíčové činnosti: Příděly a odvody hotovosti a cenin jsou poskytovány pro celou pobočkovou síť a dodávací síť. Zpracování požadavků pobočkové sítě je prostřednictvím APOST.
	Data požadavků na hotovost a ceniny		Kategorie dat: Interní
manažer útvaru sekce strategický rozvoj a BI	**Centrální datový sklad (CDS)**		Klíčové činnosti: Řízení, organizace a zabezpečení analýzy, rozvoj a vývoj úloh, které podporují operativní, provozní a business činnosti ČP v oblasti analýzy datové kvality, korporátního reportingu nad centrálním datovým skladem, centrálních číselníků a podpůrných úloh.
		CDS	Aplikace: CDS (Centrální datový sklad), CDS-ADW (ADW - Databázová vrstva pro informace o zásilkách), CDS-CDS2B (CDS2B - Databázová vrstva pro reporting), CDS-ČAD (Čištění adresních údajů), CDS-PP, CDS-RA (Řízení procesu ETL), CDS-TR (CDS-Transformace)
vedoucí pošty	**Zpracování pobočkových služeb**		
	Data APOST-POŠTA (poštovní a peněžní žurnály)		Kategorie dat: Citlivé (osobní údaje)
		Pošta - zázemí	Podpůrné
ředitel divize ICTG		**ICT podpůrná aktiva a služby**	Klíčové činnosti: Zajišťuje architekturu, bezpečnost, provoz a vývoj ICT ČP a provádí klíčové činnosti obnovy zejména v případě incidentů a havárií. Jedná se o služby datového centra - Olšanská, služby datového centra - Malešice, služby datového centra - Vítkov a služby LAN, WAN (aktivní prvky, kabeláž, datové linky, DNS,...) serverovny.
		CRYPTA	Aplikace na podpis, šifrování a dešifrování souborů.

Garant aktiva	Název aktiva - primární	Název aktiva - podpůrné	Popis aktiva
		Replikační systémy	RS-CEN (Replikační systém centra), RS-REG (Replikační systém regionální), RS-PPS (Replikační systém PPS).
manažer útvaru správa majetku		**Správa fyzických objektů**	Klíčové činnosti: Zajištění správy a provozu objektů
manažer útvaru bezpečnost		**Zabezpečení fyzických objektů**	Klíčové činnosti: Služba fyzické bezpečnosti zajišťuje zejména bezpečnost v oblastech: - objektová ochrana ČP, - bezpečnost poštovního provozu, - ochrana informací, - řízení oblasti rozvoje, údržby a obnovy bezpečnostních systémů, - zabezpečení nepřetržitého provozu systému kontroly vstupu (vjezdu) do budov (objektů) ČP, - zajišťování dohledu nad systémem kontroly vstupu a docházkového systému budov ČP.