Česká pošta

Směrnice

Identifikace	SM-5/2013 - verze 3.0	**Číslo jednací**	ČP/54843/2019/CKA/02
Nahrazuje	SM-5/2013 - verze 2.0	**Klasifikace**	Interní
Platnost	24. 10. 2019	**Účinnost**	1. 11. 2019

Ochrana informací

Verze 3.0

Podpis		**Podpis**	
Datum	22. 10. 2019	**Datum**	24. 10. 2019
Garant dokumentu	Mgr. Václav Navrátil, MBA podepsáno elektronicky	**Schvalovatel**	Ing. Roman Knap v.z. Dipl.-Betriebsw (FH) Roman Schanner podepsáno elektronicky
Funkce	manažer útvaru bezpečnost	**Funkce**	generální ředitel

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
3.0	1.11.2019	Změny oproti předcházející verzi 2.0: Kap. 2.1 – u kategorie informace „obchodní tajemství“ doplněno označení metodického pokynu. Kap. 2.1. – odst. (2) přesunut do kap. 4.1 odst. (6). Kap. 3 – doplněn nový odst. (2). Kap. 6.1 odst. (2) – úprava definic u jednotlivých tříd zabezpečených oblastí. Kap. 6.1 odst. (4) – provozní řád nahrazen „provozními předpisy“. Kap. 6.3 – vymazán odst. (4) z důvodu nadbytečnosti. Kap. 11 – do souvisejících dokumentů doplněna SM-7/2015. Formální úpravy. V rámci příloh došlo pouze k formálním úpravám v souladu s provedenými organizačními změnami.	B	GŘ

1 Úvodní ustanovení

1.1 Účel a cíle

(1) Účelem této směrnice je stanovit a definovat kategorie informací z hlediska jejich významu ve vztahu k potenciálním dopadům v případě jejich nedostupnosti, poškození nebo vyzrazení a definovat základní bezpečnostní požadavky snižující tyto dopady.

(2) Tato směrnice definuje způsob klasifikace a ochrany informací České pošty, s.p. (dále také „ČP“) v listinné i elektronické podobě. Současně vymezuje odpovědnosti v oblasti ochrany a řízení informací a nakládání s nimi.

(3) Dále tato směrnice slouží jako základní rámec pro oblast ochrany informací, pro vymezení odpovědnosti za jejich ochranu a je východiskem pro řízení procesů ochrany informací v rámci ČP.

(4) Tato směrnice se vydává v souladu s obecně závaznými právními předpisy, vnitřními předpisy ČP a obchodními potřebami ČP.

1.2 Působnost

Tato směrnice je v plném rozsahu závazná pro všechny zaměstnance ČP, osoby v obdobném postavení a organizační jednotky ČP, které v rámci své činnosti mají přístup k informacím ČP a které zpracovávají informace ČP.

1.3 Zkratky a pojmy

ZKRATKY	
DI	Důvěrná informace
DSČP	Datová síť ČP
ICT	Informační a komunikační technologie, zkráceně ICT (Information and Communication Technologies), zahrnují veškeré informační technologie používané pro komunikaci a práci s informacemi.
OBT	Obchodní tajemství
OU	Osobní údaj
TZO	Třída zabezpečené oblasti
UI	Utajovaná informace
ZOU	Zvláštní osobní údaj
ZS	Zvláštní skutečnost
POJMY	
Bezpečnostní incident	Událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních politik nebo navazujících řídících dokumentů.
Dokument	Každá písemná, obrazová, zvuková nebo jinak zaznamenaná informace, ať již v podobě listinné (analogové) nebo elektronické (digitální), která byla vytvořena v rámci ČP nebo byla ČP doručena a je evidována v systému spisové služby eSSL

	EZOP, případně v jiném agendovém systému. Úplná definice pojmu je uvedena v řádu ŘA-3/2010 Spisový řád.
POJMY	
Elektronický systém spisové služby (eSSL EZOP)	Systém, který ČP používá pro zajištění výkonu elektronické spisové služby. Tento systém, jako základní evidenční pomůcka spisové služby, obsahuje centrální evidenci v časovém a číselném pořádku o všech zaevidovaných dokumentech přijatých nebo vzešlých z vlastní činnosti ČP. Úplná definice pojmu je uvedena v řádu ŘA-3/2010 Spisový řád.
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).
Informace	Údaj (data) v listinné či elektronické podobě, kterému je přiřazen význam.
Klasifikace informace	Definování kategorie informace z hlediska jejího významu a všech potenciálních dopadů v případě nedostupnosti, poškození nebo zneužití informace. Podle stanovené kategorie se určuje konkrétní způsob její ochrany.
Neoprávněná osoba	Fyzická nebo právnická osoba, která není oprávněna seznamovat se s příslušnou informací.
Nosič informací	Nebo také datové či paměťové médium, datový nosič či záznamové médium. Jedná se o paměťový nosič datových informací (dat) používající k jejich uchování nějaký fyzikální princip. Kromě elektronických lze za datová média považovat i jakékoli jiné hmotné nosiče, pokud slouží k zaznamenání určité informace. Tato datová média se dělí dle principu zápisu a čtení na: - magnetická (DLT, VHS, HDD, Diskety, ZIP) - optická (CD, DVD, Blue ray) - elektronická (Flash Disk, Memory card, SIM card, SSD, Telefon, Tablet) Nosičem informací může být rovněž listina v papírové podobě, ve které je informace obsažena.
Oprávněná osoba	Fyzická nebo právnická osoba, která je oprávněna seznamovat se s příslušnou informací v souladu s principem „Need to know“.
Označení informace (klasifikační znak)	Vyznačení náležitostí vlastníkem informace v návaznosti na určení kategorie informace v souladu s klasifikací informací.
Podatelna	Pracoviště (místnost nebo místnosti) ČP, kde se externí či interní dokumenty (listinné a elektronické) nebo zásilky jiného druhu přijímají, zpracovávají a vypravují (speciální spisový uzel).
Princip „Need to know“	Objektivní a důvodná potřeba na straně oprávněné osoby seznámit se s informací za účelem plnění pracovních či jiných povinností nebo oprávněných zájmů.
Spisový uzel	Základní ucelená část spisové služby ČP, která umožňuje organizovat evidenci údajů o dokumentech a spisech, včetně sledování jejich pohybu v rámci ČP až po jejich uložení a skartaci. Úplná definice pojmu je uvedeno v řádu ŘA-3/2010 Spisový řád.

Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují a která je na základě těchto údajů identifikovatelná. Tento pojem je používán v oblasti ochrany osobních údajů (viz směrnice SM-8/2013 Ochrana osobních údajů).
POJMY	
Vlastník informace	Zaměstnanec ČP, z jehož činnosti informace vznikla, nebo kterému byla při vstupu do prostředí ČP informace přidělena a v rámci své kompetence rozhoduje o způsobu zpracování, ukládání a klasifikaci informace.
Zabezpečená oblast	Zabezpečená oblast je definována jako ohraničený prostor se specifickými prvky ochrany. Jedná se o režimové pracoviště nebo ohraničené prostory zvlášť důležitého charakteru z hlediska provozované činnosti, které vyžadují zvýšenou ochranu a protokolární přístup (např. serverovny, úložiště dat, pokladny, energetické zdroje, apod.). Za zabezpečené oblasti jsou také považovány kanceláře, sklady, či jiné typy ohraničených prostor.
Záznam	Zaznamenaná informace, vztahující se k jedné věci, se kterou lze zacházet jako s jedním celkem. Může být v listinné podobě nebo na jiném hmotném nosiči dat. Záznamy nejsou evidovány v systému spisové služby eSSL EZOP, případně v jiném agendovém systému. K záznamu je nutno přistupovat z pohledu klasifikace, ochrany a označování tak, jako k již klasifikovanému dokumentu dle této směrnice (vyjma evidování).

2 Kategorie a přístup k informacím

2.1 Vymezení kategorií informací

V rámci ČP jsou informace v listinné nebo elektronické podobě zpracovávány ve formě dokumentu nebo záznamu (viz kap. 1.3). Na základě významu a povahy jsou informace zařazeny (klasifikovány) do jedné z následujících kategorií:

Tabulka 1 – Vymezení kategorií informací

	Kategorie	Označení kategorie informace obsažené v dokumentu (klasifikační znak)	Základní popis (nakládání a manipulace s informací příslušné kategorie se řídí níže uvedenými právními předpisy, vnitřními předpisy ČP a touto směrnicí)
CHRÁNĚNÉ INFORMACE	**Utajovaná informace**	**DŮVĚRNÉ (D), VYHRAZENÉ (V)**	*Právní rámec:* **zákon** č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, **nařízení vlády** č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů, **vyhláška** č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. *Vnitřní předpis ČP:* **metodický pokyn** MP-11/2017 Ochrana utajovaných informací - administrativní postupy, **metodický pokyn** MP-12/2017 Postup pro získání přístupu fyzické osoby k utajovaným informacím podle zákona č. 412/2005 Sb., **řád** ŘA-3/2010 Spisový řád.
	Informace zvláštní skutečnosti	**ZVLÁŠTNÍ SKUTEČNOST (ZS)**	*Právní rámec:* **zákon** č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, **nařízení vlády** č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. *Vnitřní předpis ČP:* **metodický pokyn** MP-11/2017 Ochrana utajovaných informací - administrativní postupy, **metodický pokyn** MP-12/2017 Postup pro získání přístupu fyzické osoby k utajovaným informacím podle zákona č. 412/2005 Sb., **směrnice** SM-7/2017 Krizové řízení, **řád** ŘA-3/2010 Spisový řád.

	Kategorie	Označení kategorie informace obsažené v dokumentu (klasifikační znak)	Základní popis (nakládání a manipulace s informací příslušné kategorie se řídí níže uvedenými právními předpisy, vnitřními předpisy ČP a touto směrnicí)
	Osobní údaje	**OSOBNÍ ÚDAJE (OU)**	*Právní rámec:* **nařízení Evropského parlamentu a Rady (EU)** 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které je dnem 25. 5. 2018 přímo aplikovatelné v oblasti ochrany osobních údajů pro všechny členské státy EU (jedná se o nařízení obecně známé pod zkratkou GDPR, v textu dále je zmiňováno pod touto zkratkou) a dále další speciální právní předpisy použitelné pro oblast ochrany osobních údajů. *Vnitřní předpis ČP:* **směrnice** SM-8/2013 Ochrana osobních údajů, **řád** ŘA-3/2010 Spisový řád.
	Zvláštní kategorie osobních údajů	**ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ (ZOU)**	*Právní rámec:* **nařízení Evropského parlamentu a Rady (EU)** 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které je dnem 25. 5. 2018 přímo aplikovatelné v oblasti ochrany osobních údajů pro všechny členské státy EU a dále další speciální právní předpisy použitelné pro oblast ochrany osobních údajů. *Vnitřní předpis ČP:* **směrnice** SM-8/2013 Ochrana osobních údajů, **řád** ŘA-3/2010 Spisový řád.
	Obchodní tajemství	**OBCHODNÍ TAJEMSTVÍ (OBT)**	*Právní rámec:* **zákon** č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. *Vnitřní předpis ČP:* **metodický pokyn** MP-3/2019 Ochrana obchodního tajemství, **řád** ŘA-3/2010 Spisový řád.
	Důvěrná informace	**DŮVĚRNÉ INFORMACE (DI)**	Kategorie důvěrná informace je informace, která nemá charakter žádné jiné z ostatních chráněných informací, ale z rozhodnutí vlastníka informace je důležité ji chránit před zveřejněním a přístupem neoprávněných osob. Je primárně určena úzkému okruhu oprávněných osob, který určí vlastník informace. Nejedná se však o OBT, které je samostatnou kategorií, avšak nakládání s touto kategorií informace se řídí analogicky vnitřním předpisem pro ochranu OBT.

	Kategorie	Označení kategorie informace obsažené v dokumentu (klasifikační znak)	Základní popis (nakládání a manipulace s informací příslušné kategorie se řídí níže uvedenými právními předpisy, vnitřními předpisy ČP a touto směrnicí)
			Vnitřní předpis ČP: **metodický pokyn** MP-3/2019 Ochrana obchodního tajemství, **řád** ŘA-3/2010 Spisový řád.
INTERNÍ INFORMACE	**Interní informace**	**Bez označení**	Kategorie interní informace je neveřejná informace určená primárně pro zaměstnance ČP.
VEŘEJNÁ INFORMACE	**Veřejná informace**	**Bez označení**	Veřejná informace je určená pro zaměstnance ČP i pro externí subjekty. O zveřejnění rozhodují ty organizační jednotky, do jejichž kompetence zveřejňování informací náleží. Jedná se o běžně dostupné informace.

2.2 Definice jednotlivých kategorií informací a vymezení přístupu k nim

2.2.1 Utajovaná informace (UI)

(1) UI dle § 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen **„zákon“**), je informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči informací označená v souladu se zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

(2) Nakládání s touto informací se řídí metodickým pokynem MP-11/2017 Ochrana utajovaných informací - administrativní postupy. Přístup k UI dle odst. (1) této kapitoly lze umožnit pouze té oprávněné osobě, která tuto utajovanou informaci nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti, a splňuje-li zákonem stanovené podmínky pro přístup k utajované informaci příslušného stupně utajení. Pravidla přístupu k UI jsou stanovena v metodickém pokynu MP-12/2017 Postup pro získání přístupu fyzické osoby k UI podle zákona č. 412/2005 Sb.

(3) Jedná-li se o kategorii UI, vlastník informace i oprávněná osoba musí splňovat zákonem stanovené podmínky pro přístup k UI příslušného stupně utajení.

2.2.2 Zvláštní skutečnost (ZS)

(1) ZS dle § 27 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, je údaj z oblasti krizového řízení, jehož zneužití by mohlo vést ke znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu ČP, pokud tento údaj není UI.

(2) V případě, že informace ZS[1] bude vytvořena v prostředí ČP nebo bude doručena do prostředí ČP, se za účelem její ochrany s touto informací nakládá jako s informací kategorie UI a bude označena v nejnižším stupni utajení „Vyhrazené“, ledaže generální ředitel ČP rozhodne jinak.

(3) Nakládání s touto informací se řídí metodickým pokynem MP-11/2017 Ochrana utajovaných informací - administrativní postupy a přístup k ní upravuje metodický pokyn MP-12/2017 Postup pro získání přístupu fyzické osoby k utajovaným informacím podle zákona č. 412/2005 Sb.

2.2.3 Osobní údaje (OU)

(1) Dle nařízení GDPR jsou OU veškeré informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelným subjektem údajů je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby, např. pohlaví, věk, datum narození, osobní stav, IP adresa, fotografický záznam, e-mailová adresa, telefonní číslo, jiné identifikační údaje (číslo občanského či řidičského průkazu, číslo cestovního dokladu…). Jedná se o příkladmý výčet.

(2) OU je informace určená pouze pro omezenou skupinu oprávněných osob, nebo organizační jednotky v rámci ČP, s určeným přístupovým oprávněním podle principu „Need to know“.

(3) Nakládání s OU a přístup k nim se řídí směrnicí SM-8/2013 Ochrana osobních údajů.

2.2.4 Zvláštní kategorie osobních údajů (ZOU)

(1) Dle nařízení GDPR spadají do zvláštní kategorie osobních údajů ty osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, a genetické nebo biometrické údaje jedinečně identifikující subjekt údajů a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci subjektu údajů.

(2) ZOU je informace určená pouze pro omezenou skupinu oprávněných osob, nebo organizační jednotky v rámci ČP, s určeným přístupovým oprávněním podle principu „Need to know“.

(3) Nakládání se zvláštní kategorií osobních údajů a přístup k této kategorii se řídí směrnicí SM-8/2013 Ochrana osobních údajů.

2.2.5 Obchodní tajemství (OBT)

(1) OBT dle § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí s ČP a které mají být podle vůle ČP utajeny, přičemž ČP zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.

(2) OBT mohou tvořit zejména strategické informace a rozhodnutí, koncepce, údaje o zaměstnancích, zákaznících, obchodních vztazích, cenová ujednání, ekonomické, obchodní a marketingové analýzy a plány, souhrnné přehledy a zprávy, speciální know-how, auditní a obdobné zprávy, projekty, bezpečnostní údaje, zásady cenotvorby, zásady bezpečnostní politiky ochrany majetku a osob.

[1] V podmínkách ČP situace nenastává, proto proces není detailně rozpracován.

(3) Informace kategorie OBT je určená pouze pro omezenou skupinu oprávněných osob, nebo organizační jednotky v rámci ČP.

(4) Nakládání s touto informací a přístup k ní se řídí metodickým pokynem MP-3/2019 Ochrana obchodního tajemství.

2.2.6 Důvěrná informace (DI)

(1) Důvěrná informace je informace, která nemá charakter žádné jiné z ostatních chráněných informací, ale z rozhodnutí vlastníka informace je důležité ji chránit před zveřejněním a přístupem neoprávněných osob. Jedná se o kategorii informace, která je z hlediska hodnocení požadavků na ochranu vyšší, než je kategorie informace interní.

(2) Důvěrná informace je určená pouze pro omezenou skupinu oprávněných osob, nebo organizační jednotky v rámci ČP. Dále se může jednat o informace určené výhradně pro adresáta, kde okruh osob stanovuje vlastník informace.

(3) Mezi důvěrné informace patří např. tyto typy informací: autentizační a autorizační informace, zdrojové kódy, bezpečnostní analýzy, hodnocení a výstupy obsahující konkrétní údaje o stavu bezpečnosti ČP apod.

(4) Nakládání s touto informací a přístup k ní se řídí analogicky metodickým pokynem MP-3/2019 Ochrana obchodního tajemství.

2.2.7 Interní informace

(1) Interní informace je informace určená pouze pro zaměstnance ČP a přístup k ní mohou mít všichni zaměstnanci.

(2) Vlastník informace v rámci klasifikace informace může stanovit, že je informace určená pouze pro omezenou skupinu oprávněných osob, nebo organizační jednotky v rámci ČP.

(3) Za interní informace lze považovat např. vnitřní předpisy ČP, sdělení pro zaměstnance, běžnou pracovní e-mailovou komunikaci apod. Interní informací může být také neveřejná informace, která je komunikována mezi zaměstnanci ČP a externími subjekty za současného dodržení povinností dle kapitoly 8 této směrnice.

(4) Nakládání s touto informací a přístup k ní se řídí analogicky ustanoveními této směrnice, která se týkají chráněných informací, kromě označování.

2.2.8 Veřejná informace

Veřejná informace je informace, která zahrnuje široký okruh informací k zajištění činností ČP, nepožívá žádné ochrany ze strany ČP a nakládání s ní nepodléhá regulaci ze strany ČP. Veřejná informace je vždy běžně veřejně dostupná a její prozrazení či zneužití nezpůsobí ČP žádný negativní dopad.

3 Všeobecná ustanovení k ochraně informací

(1) Přístup k chráněné informaci má vždy vlastník informace. Přístup k chráněné informaci může být dále umožněn pouze oprávněné osobě v souladu s touto směrnicí a navazujícími vnitřními předpisy ČP.

Přístupová oprávnění k chráněné informaci stanoví vlastník informace nebo nadřízený vlastníka informace, popřípadě generální ředitel ČP.

(2) V rámci své pracovní činnosti mají oprávnění k přístupu do všech aplikací ČP obsahujících veřejné, interní a chráněné informace (vyjma kategorií Utajovaná informace a Informace zvláštní skutečnosti, kde pravidla přístupu určují jiné vnitřní předpisy – viz kap. 2.1) manažer útvaru bezpečnost, Bezpečnostní manažer ICT, Compliance Officer, manažer specializovaného útvaru interní audit a řízení rizik a dále určení zaměstnanci útvaru bezpečnost, specializovaného útvaru ICT bezpečnost, specializovaného útvaru compliance a korporátní agendy a specializovaného útvaru interní audit a řízení rizik. Toto oprávnění se vztahuje pouze k režimu nahlížení. Určení konkrétních zaměstnanců je v působnosti vedoucích zamětnanců dotčených organizačních jednotek.

(3) Na všechny kategorie informací dle kapitoly 2 této směrnice se vztahují obecně závazná pravidla stanovená touto směrnicí, řádem ŘA-3/2010 Spisový řád a dalšími předpisy uvedenými v kapitole 2.1 této směrnice.

(4) Ochrana chráněných informací v ICT ČP je upravena směrnicí SM-1/2015 Bezpečnostní politika ICT a metodickým pokynem MP-3/2015 Generická systémová bezpečnostní politika ICT.

(5) Ochrana poštovního tajemství se řídí ustanovením § 16 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, a Poštovními pravidly.

(6) Povinnost zaměstnanců zachovávat mlčenlivost je upravena v řádu ŘA-4/2012 Pracovní řád České pošty, s.p.

4 Označování a evidence informací

4.1 Označení chráněných informací

(1) V rámci ČP se označují všechny chráněné informace. Tyto informace jsou označovány klasifikačním znakem dle tabulky 1, jež je umístěn v záhlaví dokumentu.

(2) Označování chráněné informace kategorie UI se řídí metodickým pokynem MP-11/2017 Ochrana utajovaných informací - administrativní postupy.

(3) Označování chráněné informace kategorie OU a ZOU se řídí směrnicí SM-8/2013 Ochrana osobních údajů.

(4) Označování chráněných informací ostatních kategorií než které jsou uvedeny v odst. (2) a (3) této kapitoly, je prováděno v souladu s řádem ŘA-3/2010 Spisový řád.

(5) V případě chráněné informace umístěné na nosiči informací se klasifikační znak vyznačí také na popisném štítku umístěném na příslušném nosiči informací tak, aby byl jasně viditelný, pokud to podoba nosiče umožňuje, případně jiným vhodným způsobem (např. opatření nosiče visačkou s vyznačením klasifikačního znaku).

(6) U dokumentů nebo záznamů, které obsahují více kategorií informací, je vlastník povinen vždy označit tu kategorii, která odpovídá kategorii informace s nejvyšším stupněm ochrany na základě provedené analýzy a vyhodnocení opatření k zabezpečení dané kategorie informace.

4.2 Evidence chráněné informace

(1) Všechny dokumenty obsahující chráněné informace klasifikované podle této směrnice, vyjma UI, se evidují podle řádu ŘA-3/2010 Spisový řád v systému eSSL EZOP.

(2) V případě dokumentů doručených z prostředí mimo ČP musí být jejich evidence a klasifikace provedena v souladu s kategorií informace, v jaké byla ČP přijata.

4.3 Změna a zrušení kategorie chráněné informace

(1) Vlastník informace má právo kdykoliv přezkoumat klasifikaci informace.

(2) Přezkum klasifikace informace a případnou změnu kategorie chráněné informace je vlastník informace povinen provést vždy bez zbytečného odkladu, pokud:

a) uplyne doba, na kterou byla kategorie chráněné informace stanovena,

b) došlo ke změně významu chráněné informace, vzhledem k potřebě její ochrany (i u dokumentů vyřízených nebo uložených ve spisovně ČP),

c) zjistí, že kategorie chráněné informace byla stanovena nesprávně.

(3) Každý zaměstnanec ČP, který zjistí skutečnost, na základě které má dojít k přezkumu klasifikace informace a k případné změně kategorie chráněné informace, je povinen o tom písemně dokumentovatelným způsobem informovat vlastníka informace, případně vedoucího zaměstnance organizační jednotky vlastníka informace.

(4) O změně kategorie informace rozhoduje vlastník informace, který původní kategorii stanovil. Není-li vlastník informace znám, rozhodne o změně kategorie generální ředitel ČP nebo jím pověřená osoba, není-li dále stanoveno jinak. Změna musí být oznámena všem známým oprávněným osobám.

5 Nakládání s chráněnými informacemi

(1) Přístup k informaci má vlastník informace, případně jím určený okruh příjemců. Přístup k informaci může být pro konkrétní osobu, a/nebo pro organizační jednotku. Nakládat s chráněnými informacemi může pouze ta oprávněná osoba, která potřebuje informaci ke své činnosti, a to pouze v rozsahu, v jakém je to nezbytné k plnění jejích pracovních, případně jiných povinností či oprávněných zájmů (uplatnění principu „Need to know“).

(2) V případě, že je ČP povinna poskytnout či zpřístupnit chráněnou informaci na základě platných právních předpisů či pravomocného soudního či správního rozhodnutí, je povinna ji poskytnout v rozsahu stanovené nebo uložené povinnosti. Takové poskytnutí či zpřístupnění se nepovažuje za porušení této směrnice. Osoba, která tímto způsobem informaci poskytuje nebo zpřístupňuje, je povinna v míře, ve které jí to poskytnutí či zpřístupnění dovoluje, dodržet pravidla stanovená touto směrnicí.

(3) Dokumenty obsahující chráněné informace se předávají v souladu s řádem ŘA-3/2010 Spisový řád podle pravidel systému eSSL EZOP a v souladu s navazujícími vnitřními předpisy ČP.

(4) Za nakládání s chráněnou informací a za zajištění ochrany chráněných informací je odpovědný každý zaměstnanec, který má chráněné informace k dispozici.

6 Zajištění ochrany informací

(1) V době nepřítomnosti vlastníka informace může bez souhlasu vlastníka zajistit přístup k chráněné informaci zaměstnanec zastupující vlastníka informace, případně přímý nadřízený zaměstnanec vlastníka informace nebo jím určená osoba.

(2) Při manipulaci a ukládání informací v elektronické nebo listinné podobě musí být přijata taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k informacím, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití. Podrobnosti této manipulace a ukládání jsou stanoveny v kapitole 6.2 této směrnice.

(3) Při skončení pracovněprávního vztahu vlastníka informace zabezpečí předání dokumentu obsahujícího informaci jiné osobě přímý nadřízený zaměstnanec vlastníka informace. Při předávání se postupuje v souladu s řádem ŘA-3/2010 Spisový řád.

(4) Projednávání informací v rámci jednání, porad, pracovních schůzek musí být prováděno tak, aby nemohlo dojít k vyzrazení informací neoprávněné osobě. Vlastník informace, případně jím určená osoba při poradách, na kterých jsou projednávány chráněné informace, odpovídá za upozornění na kategorii příslušné informace, stanovení formy a způsobu záznamu, zvolení vhodné místnosti pro konání porady a stanovení okruhu osob, které se jednání zúčastní.

6.1 Zabezpečené oblasti a zajištění fyzického perimetru

(1) Perimetr zabezpečené oblasti určuje prostory umožňující zpracování a ukládání informací (jak v listinné, tak i v elektronické podobě) v dané kategorii za určitých podmínek. Ty lze charakterizovat jako soubor přijatých technických a organizačních opatření k zajištění dostupnosti, integrity a důvěrnosti informací, například zamezení neautorizovaného přístupu do bezpečnostního perimetru, protipožární opatření atp.

(2) Zabezpečené oblasti se z hlediska ochrany informací dělí do čtyř tříd zabezpečených oblastí (dále jen „TZO“), viz tabulka níže. Detailní požadavky na fyzické zabezpečení jsou definovány v příloze č. 1 této směrnice – Detailní požadavky na třídy zabezpečených oblastí.

Tabulka 2 – Třídy zabezpečených oblastí

Třída zabezpečené oblasti	Podmínka zařazení dle kategorie a množství ukládaných chráněných informací bez nutnosti ochrany informací šifrováním
TZO 1	Centrální zpracování, ukládání a archivace chráněných a interních informací, jedná se především o datové sály v perimetru datového centra. Do této třídy spadají pouze datová centra Malešice a Olšanská.
TZO 2	Decentralizované zpracování a ukládání 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 poštu), a mezinárodní poštu.

TZO 3	Decentralizované zpracování a ukládání chráněných a interních informací. Jedná se především o serverovny pošt mimo KII, serverovny v lokalitách, kanceláře s vyšší mírou zabezpečení, …
TZO 4	Lokální zpracování a ukládání informací. Jedná se především o přepážky pošt, standardní kanceláře a další neveřejné prostory.

(3) Zařazení zabezpečené oblasti do příslušné kategorie stanoví útvar bezpečnost v případné součinnosti s odpovědnými vedoucími zaměstnanci organizačních jednotek v daném objektu.

(4) Zaměstnanci musí být seznámeni s pravidly fyzického zabezpečení svých kanceláří, zabezpečených oblastí a s nimi souvisejících budov ČP. Toto seznámení zajišťuje nadřízený zaměstnanec vhodnou cestou, například provozními předpisy či bezpečnostním řádem daného pracoviště.

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

6.2 Zajištění ochrany informací v elektronické podobě

(1) Veškerá bezpečnostní opatření musí být navržena tak, aby zajistila ochranu informací a minimalizovala v případě bezpečnostního incidentu dopad na ČP nebo subjekt údajů (při zpracování osobních údajů) a zároveň korespondovala s dalšími legislativními požadavky.

(2) V rámci jakéhokoli uložení nebo přenosu chráněných nebo interních informací je nutno posoudit dopady v případě ztráty integrity, dostupnosti nebo důvěrnosti a na základě tohoto případně zvýšit požadavky zabezpečení nad rámec uvedených v této směrnici. Jako jedno z vodítek může být i rozsah ukládaných nebo přenášených informací.

(3) Ochrana informací v elektronické podobě je řešena zejména zajištěním fyzické bezpečnosti daného nosiče informací (interní pevný disk, externí disk, USB Flash Disk, CD, DVD aj.), ochranou samotné informace, a to především šifrováním, nebo jejich vzájemnou kombinací.

(4) Ochrana informací se provádí výhradně schválenými šifrovacími algoritmy uvedenými v příloze č. 1 metodického pokynu MP-3/2015 Generická systémová bezpečnostní politika ICT.

(5) Návody na šifrování informací, aktuální zásady, metody a postupy šifrování jsou uvedeny na Intranetu ČP (Odborné úseky > ICT > Bezpečnost ICT > Návody na šifrování informací).

(6) V případě předávání kryptografických klíčů nebo hesel použitých pro šifrování musí být tyto předány jiným bezpečným komunikačním kanálem (například šifrovaná informace e-mailem a kryptografický klíč pomocí SMS).

6.2.1 Ukládání informací (souborů)

V následující tabulce je rozpracováno ukládání souborů vycházející z generického zajištění ochrany informací dle TZO, které je uvedeno v příloze č. 2 této směrnice.

Tabulka 3 – Ochrana informací dle služeb či systémů ICT

Kategorie informace	*Typ úložiště*						
	Koncové zařízení-nepřenosný pracovní počítač	**Koncové zařízení-přenosné PC nebo externí nosič informací**	**Centrální SharePoint**	**Interní sdílené úložiště[2]**	**Office 365 Azure ČP[3]**	**Úložiště Smluvního partnera[4]**	**Úložiště nesmluvního partnera, nebo free úložiště[5]**
Utajovaná informace	Ukládání povoleno výhradně na dedikovaný lokální systém	Ukládání povoleno výhradně na dedikovaný lokální systém	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno
Informace zvláštní skutečnosti	Ukládání povoleno výhradně na dedikovaný lokální systém	Ukládání povoleno výhradně na dedikovaný lokální systém	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno	Ukládání zakázáno
Zvláštní kategorie osobních údajů	Ukládání šifrovaně	Ukládání šifrovaně[6]	Ukládání šifrovaně[7]	Ukládání šifrovaně[8]	Ukládání šifrovaně	Ukládání šifrovaně	Ukládání zakázáno
Osobní údaje	Ukládání šifrovaně	Ukládání šifrovaně[6]	Ukládání šifrovaně[7]	Ukládání šifrovaně[9]	Ukládání šifrovaně[9]	Ukládání šifrovaně	Ukládání zakázáno
Obchodní tajemství	Ukládání šifrovaně	Ukládání šifrovaně[6]	Ukládání šifrovaně[7]	Ukládání šifrovaně[8]	Ukládání šifrovaně[9]	Ukládání šifrovaně	Ukládání zakázáno
Důvěrná informace	Ukládání šifrovaně	Ukládání šifrovaně[6]	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání šifrovaně	Ukládání zakázáno
Interní informace	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání šifrovaně	Ukládání šifrovaně
Veřejná informace	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně	Ukládání nešifrovaně

[2] Jedná se především o sdílená úložiště fyzicky umístěná v TZO 1 – 3.
[3] Jedná se o Office365 České pošty, jedná se především o provoz pošt.
[4] Jedná se o systémy pro ukládání souborů provozované smluvním partnerem.
[5] Jedná se zde i o veřejně dostupná úložiště jako je například uložto, úschovna, …
[6] V rámci mobilního PC, nebo externího média je možno využít šifrování na úrovni celého zařízení. Šifrování celého úložiště zajišťuje uživatel sám nebo ve spolupráci se specializovaným útvarem PKU. Vždy je ale nutno posoudit, zda je toto zabezpečení dostatečné s ohledem na rozsah a dopad ukládaných informací.
[7] V rámci centrálního SharePoint je využito šifrování na úrovni komunikace a umístění informace v TZO 1. V tomto případě není po uživateli vyžadována žádná akce. Vždy je ale nutno posoudit, zda je toto zabezpečení dostatečné s ohledem na rozsah a dopad ukládaných informací.
[8] V rámci centrálních sdílených složek je umístění informace v TZO 1 - 3. Uživatel musí před uložením ověřit u specializovaného útvaru PKU, zda je fyzické úložiště daného sdílení skutečně uloženo v TZO 1-3. Vždy je ale nutno posoudit, zda je toto zabezpečení dostatečné s ohledem na rozsah a dopad ukládaných informací.
[9] V rámci Office 365 České pošty je využito šifrování na úrovni komunikace a šifrování v rámci ukládání. Vždy je ale nutno posoudit, zda je toto zabezpečení dostatečné s ohledem na rozsah a dopad přenášených informací.

6.2.2 Posílání informací e-mailem

(1) V následující tabulce je rozpracována možnost zasílání informací přes služby elektronické pošty vycházející z generického zajištění ochrany informací dle TZO, které tvoří přílohu č. 2 této směrnice.

(2) **Interním e-mailem** je považována komunikace v rámci a výhradně na adresy: …@cpost.cz.
E-mail provozovaný smluvním partnerem je adresa vycházející z firemní domény, např.: …@kb.cz, …@fitnesskotva.cz, …@alza.cz, …@mvcr.cz, a další.
CloudFreemail je poštovní systém určený široké veřejnosti, např.: …@gmail.com, …@seznam.cz, …@centrum.cz, …@yahoo.com, a další.

(3) Chráněné informace v elektronické podobě, které jsou zasílány elektronickou poštou, musí být chráněny proti neoprávněnému nebo nahodilému přístupu, tj. šifrovány. V případě, že není možno tuto ochranu zajistit, například směrem k fyzické osobě jako zákazníkovi ČP, je nutno provést analýzu rizik a na základě této analýzy je pak možno určit, zda je přenášení elektronickou poštou akceptovatelné, případně navrhnout jiná vhodná technicko-organizační opatření.

Tabulka 4 – Ochrana informací zasílaných e-mailem

Typ přenosu / kategorie	**Interní e-mail** (MS Exchange, SunOne, O365)	**Email provozovaný Smluvním partnerem**	**Cloud Freemail**
Utajovaná informace	Posílání zakázáno	Posílání zakázáno	Posílání zakázáno
Informace zvláštní skutečnosti	Posílání zakázáno	Posílání zakázáno	Posílání zakázáno
Zvláštní kategorie osobních údajů	Posílání šifrovaně	Posílání šifrovaně	Posílání zakázáno
Osobní údaje	Posílání šifrovaně[10] interními prostředky systému.	Posílání šifrovaně	Posílání šifrovaně[11]
Obchodní tajemství	Posílání šifrovaně[10] interními prostředky systému.	Posílání šifrovaně	Posílání šifrovaně
Důvěrná informace	Posílání šifrovaně[10] interními prostředky systému.	Posílání šifrovaně	Posílání zakázáno
Interní informace	Nešifrovaně	Nešifrovaně	Posílání šifrovaně
Veřejná informace	Nešifrovaně	Nešifrovaně	Nešifrovaně

[10] Šifrování je zajištěno interními prostředky systému / aplikace. V tomto případě není po uživateli vyžadována žádná akce. Vždy je ale nutno posoudit, zda je toto zabezpečení dostatečné s ohledem na rozsah a dopad přenášených informací.
[11] V případě komunikace s daným a konkrétním subjektem údajů je možno komunikovat nešifrovaně, vždy je však nutno posoudit rozsah a případný dopad OU.

6.2.3 Chat, obdobná on-line komunikace a sociální sítě

(1) V následující tabulce je rozpracována možnost předávání či zasílání informací přes služby chatu vycházející z generického zajištění ochrany informací dle TZO.

(2) **Firemní Chat** je pro ČP Skype for Business (dříve Lync).
Free Chat a sociální sítě - jedná se o chat volně dostupný na Internetu, především o TeamViewer, Skype, HangOuts, Facebook, Instagram, apod.

Tabulka 5 – Ochrana informací v rámci služby Chat a obdobných on-line komunikacích

Typ komunikace / kategorie	Firemní Chat[12]	Free Chat a sociální sítě[13]
Utajovaná informace	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Informace zvláštní skutečnosti	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Zvláštní kategorie osobních údajů	Komunikace – povolena; sdílení souborů v rámci aplikace - šifrovaně	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Osobní údaje	Komunikace – povolena; sdílení souborů v rámci aplikace - šifrovaně	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Obchodní tajemství	Komunikace – povolena; sdílení souborů v rámci aplikace - šifrovaně	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Důvěrná informace	Komunikace – povolena; sdílení souborů v rámci aplikace - šifrovaně	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Interní informace	Komunikace – povolena; sdílení souborů v rámci aplikace - nešifrovaně	Komunikace – zakázána; sdílení souborů v rámci aplikace - zakázáno
Veřejná informace	Komunikace – povolena; sdílení souborů v rámci aplikace - nešifrovaně	Komunikace – povolena; sdílení souborů v rámci aplikace - nešifrovaně

6.3 Zajištění ochrany informací v listinné podobě

(1) Chráněné informace musí být ukládány v zabezpečených oblastech, které jsou popsány v kapitole 6.1 této směrnice.

[12] Jedná se o Chat provozovaný ČP nebo smluvním partnerem, především Lync, Skype pro firmy, Webex.
[13] Jedná se o chat volně dostupný na internetu, především o TeamViewer, Skype, HangOuts, Facebook, Instagram, …

(2) Informace mohou být ukládány v zabezpečených oblastech následovně:

Tabulka 6 – Ochrana informací v listinné podobě

Kategorie informace	***Třída zabezpečené oblasti***			
	TZO 1	**TZO 2**	**TZO 3**	**TZO 4**
Utajovaná informace	Ukládání těchto informací se řídí vlastním vnitřním předpisem dle tabulky 1.			
Informace zvláštní skutečnosti	Ukládání těchto informací se řídí vlastním vnitřním předpisem dle tabulky 1.			
Zvláštní kategorie osobních údajů	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložené informace musí být chráněny dalšími opatřeními.	Uložené informace musí být chráněny dalšími opatřeními.
Osobní údaje	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložené informace musí být chráněny dalšími opatřeními.	Uložené informace musí být chráněny dalšími opatřeními.
Obchodní tajemství	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložené informace musí být chráněny dalšími opatřeními.	Uložené informace musí být chráněny dalšími opatřeními.
Důvěrná informace	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložené informace musí být chráněny dalšími opatřeními.
Interní informace	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.
Veřejná informace	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.	Uložení a zpracování informací povoleno.

(3) Chráněné informace, které jsou ukládány v nižší TZO, než pro kterou jsou primárně určeny, musí být ukládány v uzamčených schránkách (kancelářské skříně, trezorové skříně, plechové skříně, stolní kontejnery apod.), pokud ukládání chráněné informace neřeší samostatný vnitřní předpis dle kategorie informace, respektive konkrétní informace dané klasifikace, bez možnosti přístupu neoprávněných osob v mimopracovní době i v době krátkodobé nepřítomnosti (oběd, přestávka apod.).

(4) Klíči od uzamčené schránky disponuje vlastník informace nebo jím určená osoba. V případě nepřítomnosti vlastníka informace (nebo jím určené osoby) musí být zajištěno, aby klíče od uzamčené schránky měl k dispozici zastupující zaměstnanec nebo liniově nadřízený vedoucí zaměstnanec.

7 Likvidace a skartace informací a jejich nosičů

(1) Veškeré dokumenty jsou skartovány v souladu s ŘA-3/2010 Spisový řád.

(2) Veškeré informace v elektronické podobě a elektronické nosiče informací jsou likvidovány dle přílohy č. 4 této směrnice. Po provedené likvidaci může být v případě potřeby jako obecný vzor protokolu použit vzor, který tvoří přílohu č. 6 této směrnice.

(3) Veškeré informace v listinné podobě se likvidují dle přílohy č. 5 této směrnice.

8 Povinnosti zaměstnanců při ochraně informací

Každý zaměstnanec ČP je při ochraně informací povinen:

a) dodržovat zásady ochrany chráněných informací a učinit vše, aby se tyto informace nestaly známé neoprávněné osobě;

b) zachovávat mlčenlivost o chráněných informacích, s nimiž přichází do styku při výkonu své pracovní činnosti. Povinnost zachovat mlčenlivost trvá i při změně pracovněprávního vztahu (např. při převedení na jinou pracovní činnost nebo přeložení na jinou pracovní pozici) nebo po skončení pracovněprávního vztahu, a to po dobu, po kterou jsou chráněné informace utajovány;

c) přistupovat ke každé neoznačené informaci vzniklé z činnosti ČP jako k informaci kategorie interní, kterou není možné zveřejňovat, s tím, že o informacích určených ke zveřejnění rozhodují ty organizační jednotky, do jejichž kompetence zveřejňování informací náleží; v případě pochybností se zaměstnanec obrátí na svého liniově nadřízeného vedoucího zaměstnance;

d) seznámit se s navazujícími vnitřními předpisy ČP uvedenými v kapitole 2.1 této směrnice, které upravují ochranu chráněných informací, a důsledně plnit všechna jejich ustanovení;

e) předávat dokumenty obsahující chráněné informace v listinné podobě mimo ČP jen na základě předávacího protokolu; toto ustanovení se týká pouze osobně předávaných dokumentů; vzor předávacího protokolu tvoří přílohu č. 3 této směrnice;

f) nepořizovat více kopií dokumentů s chráněnými informacemi, než je nezbytně nutné k výkonu práce;

g) předkládat ke kontrole chráněné informace podle požadavků nadřízeného zaměstnance nebo kontrolních orgánů (např. Národní bezpečnostní úřad, Úřad pro ochranu osobních údajů);

h) ihned hlásit zjištění bezpečnostního incidentu v souladu s MP-2/2017 Zvládání bezpečnostních incidentů;

i) při ukládání, odesílání, přepravě a přenášení chráněných informací postupovat v souladu s touto směrnicí a navazujícími vnitřními předpisy ČP;

j) v případě, že se zaměstnanec, který není oprávněnou osobou, dostane z jakéhokoli důvodu do styku s chráněnou informací, provést všechna nezbytná opatření, která lze na něm spravedlivě a rozumně požadovat, k ochraně chráněné informace před neoprávněnou osobou, a to i před jiným neoprávněným zaměstnancem, a dále tuto skutečnost neprodleně oznámit svému přímému nadřízenému, vlastníku informace (je-li znám), případně útvaru bezpečnost;

k) při zjištění porušení ustanovení této směrnice (bezpečnostního incidentu) přijímat taková opatření, která povedou k odstranění nepříznivých následků takového porušení a výsledky řešení oznamovat přímému nadřízenému.

9 Odpovědnost v rámci ochrany informací

9.1 Odpovědnost vedoucího zaměstnance

Každý vedoucí zaměstnanec odpovídá**:**

a) za dodržování ustanovení této směrnice v rámci své působnosti;

b) za vytváření podmínek k zabezpečení ochrany chráněných informací v souladu s touto směrnicí;

c) za poučení svých podřízených o povinnostech při ochraně chráněných informací;

d) za zabezpečení a provádění kontroly plnění ustanovení této směrnice v rámci své působnosti.

9.2 Odpovědnost manažera útvaru bezpečnost, Bezpečnostního manažera ICT a Pověřence pro ochranu osobních údajů

(1) Manažer útvaru bezpečnost a Bezpečnostní manažer ICT zajišťují dokumentaci případů porušení ochrany informací v interních evidencích. Do evidence je nutno zaznamenat, o jaký incident se jednalo, kdo incident nahlásil, kdy k incidentu došlo, jaké bylo řešení vzniklého incidentu, případně jaká opatření byla v souvislosti s incidentem přijata.

(2) Pověřenec pro ochranu osobních údajů dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení a případně též přijatá nápravná opatření.

10 Kontrola dodržování pravidel ochrany informací ze strany ČP

Kontrolu dodržování pravidel ochrany informací v souladu s ustanoveními této směrnice provádějí v rámci své působnosti vedoucí zaměstnanci, zaměstnanci útvaru bezpečnost, osoby pověřené generálním ředitelem ČP a další zaměstnanci v rámci své působnosti (např. Pověřenec pro ochranu osobních údajů, specializovaný útvar compliance a korporátní agendy). Kontrolu dodržování pravidel v oblasti ochrany informací v elektronické podobě může provádět též manažer specializovaného útvaru ICT bezpečnost, případně jím pověřené osoby, a to v rámci své působnosti.

11 Související dokumenty

INTERNÍ	
ŘA-3/2010	Spisový řád
ŘA-4/2012	Pracovní řád České pošty, s.p.
SM-8/2013	Ochrana osobních údajů
SM-1/2015	Bezpečnostní politika ICT
SM-7/2017	Krizové řízení
SM-8/2016	Posuzování objektů určených k fyzické ostraze
SM-7/2011	Tvorba a evidence smluv
MP-11/2017	Ochrana utajovaných informací - administrativní postupy
MP-3/2015	Generická systémová bezpečnostní politika ICT

MP-2/2017	Zvládání bezpečnostních incidentů
MP-12/2017	Postup pro získání přístupu fyzické osoby k utajovaným informacím podle zákona č. 412/2005 Sb.
MP-3/2019	Ochrana obchodního tajemství
	Poštovní pravidla
SM-3/2014	Projektová bezpečnostní dokumentace informačního systému pro zpracování utajovaných informací
SM-4/2014	Provozní bezpečnostní směrnice – bezpečnostní správce IS, správce IS
SM-5/2014	Provozní bezpečnostní směrnice – uživatel IS
SM-7/2015	Systém compliance v ČP a Podnikový compliance program proti korupci a dalším formám nekalého jednání
EXTERNÍ	
zákon č. 412/2005 Sb.	o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (zákon)
zákon č. 89/2012 Sb.	občanský zákoník, ve znění pozdějších předpisů
zákon č. 29/2000 Sb.	o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů
zákon č. 240/2000 Sb.	o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016	o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které je dnem 25. 5. 2018 přímo použitelné v oblasti ochrany osobních údajů pro všechny členské státy EU („Nařízení GDPR“)
nařízení vlády č. 522/2005 Sb.	kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů
vyhláška č. 529/2005 Sb.	o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů
nařízení vlády č. 462/2000 Sb.	k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů

12 Přechodná a závěrečná ustanovení

(1) Porušení ustanovení této směrnice lze s přihlédnutím ke všem okolnostem posuzovat jako porušení povinností vyplývajících z právních předpisů vztahující se k zaměstnancem vykonávané práci.

(2) Nepřipouští se označování chráněných informací jinými kategoriemi a klasifikačními znaky, než je uvedeno v této směrnici a metodickém pokynu MP-11/2017 Ochrana utajovaných informací - administrativní postupy, vyjma smluv uzavíraných ČP, v nichž je užíván pojem „Důvěrné informace“, a tento pojem je použit s odkazem na obecný právní předpis (občanský zákoník).

(3) U chráněných informací doručených z prostředí mimo ČP nebo vzniklých z činnosti ČP před nabytím účinnosti této směrnice (tj. SM-5/2013 - verze 3.0) zůstává zachováno jejich označení. K informacím

označeným kategorií „Citlivé informace“ se přistupuje jako ke kategorii „Důvěrná informace“, s výjimkou informací obsahujících OU či ZOU. Ostatní postupy a procesy k ochraně informací se řídí touto směrnicí.

(4) Útvar bezpečnost plní funkci konzultačního místa v otázkách ochrany informací. Specializovaný útvar ICT bezpečnost pak plní funkci konzultačního místa v otázkách, týkajících se kapitoly 6, vyjma podkapitoly 6.3.

(5) Výklad a případnou aktualizaci této směrnice zajišťuje útvar bezpečnost, výklad kapitoly 6 zajišťuje specializovaný útvar ICT bezpečnost, vyjma podkapitoly 6.3.

(6) Související předpisy a dokumenty jsou k dispozici na Intranetu ČP (Odborné úseky > Bezpečnost > Interní předpisy).

13 Přílohy

Přílohy jsou k dispozici na Intranetu ČP (Odborné úseky > Bezpečnost > Ochrana informací). Za aktualizaci příloh odpovídá útvar bezpečnost.

POŘADÍ	NÁZEV PŘÍLOHY
1.	Detailní požadavky na třídy zabezpečených oblastí
2.	Generické zabezpečení informací v elektronické podobě dle TZO
3.	Vzor předávacího protokolu
4.	Likvidace informací v elektronické podobě
5.	Likvidace informací v listinné podobě
6.	Vzor protokolu o provedeném mazání dat / likvidaci nosičů informací