

PŘÍLOHA 5: PRAVIDLA OCHRANY JEDNOTLIVÝCH ÚROVNÍ AKTIV – MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu			
datum	verze	změněno	provedená změna
15. 2. 2026	1.0	Manažer KB	Vytvoření dokumentu
4. 3. 2026	1.0	Výbor pro řízení KB	Schválení dokumentu

1 Předmět a účel

Na informace má z hlediska ochrany informací zásadní vliv jejich úroveň důvěrnosti. Pro účely ochrany informací se informační aktiva ministerstva dělí dle úrovně důvěrnosti na klasifikační stupně veřejné, interní, citlivé a diskrétní (viz *Tabulka 1*). Na určení úrovně důvěrnosti a klasifikace informace nemá vliv forma, v jaké se vyskytuje (elektronická nebo listinná forma). Klasifikace se vztahuje na všechny formy informace (např. kopie).

Není-li informace nijak označena, je nutné na ni pohlížet a zabezpečit ji minimálně opatřeními dle úrovně dostupnosti střední (klasifikace informací – interní).

Pokud původce dané informace není schopen stanovit příslušný klasifikační stupeň sám, může požádat manažera KB o metodické vedení při posouzení.

V případě informací, které kombinují několik rozdílných klasifikačních stupňů, musí být výsledný klasifikační stupeň určen podle informace s nejvyšším klasifikačním stupněm. Pro větší množství informací může být vhodné zvážit vyšší klasifikační stupeň. O změně klasifikačního stupně rozhoduje původce dané informace.

Tato pravidla ochrany jednotlivých úrovní aktiv obsahují také pravidla pro nakládání s aktivy stanovující minimální označování informací, manipulaci s aktivy a správu výměnných médií, dále pravidla pro ochranu integrity, pravidla pro ochranu dostupnosti a pravidla pro likvidaci dat v souladu s § 7 písm. h) vyhlášky.

Pravidla ochrany jednotlivých úrovní aktiv musí být minimálně 1× za 2 roky přezkoumána manažerem KB. I v případě, že nedojde k žádným změnám, musí být u verze uvedeno datum přezkoumání.

2 Klasifikace informací

Klasifikace informací (aktiv) je identická pouze s ohodnocením aktiv dle atributu důvěrnosti.

Pomocí klasifikační tabulky budou uživatelé snadněji schopni rozhodnout o klasifikaci aktiva. V případě nejjasností mohou rozhodnutí konzultovat s manažerem KB.

Tabulka 1: Stanovení klasifikačních stupňů a jejich označování TLP dle úrovně důvěrnosti

Úroveň důvěrnosti	Klasifikace informací	Popis	Požadovaná bezpečnostní opatření
Nízká	Veřejné	Informace je veřejně přístupná nebo byla určena ke zveřejnění. Informace může být dále poskytována a šířena bez omezení. Narušení důvěrnosti informací neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takové informace s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:CLEAR.	Není vyžadována žádná ochrana.
Střední	Interní	Informace nejsou veřejně přístupné a tvoří know-how ministerstva, ochrana informací není vyžadována žádným právním předpisem nebo smluvním ujednáním. Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti musí být využívány prostředky pro řízení přístupu.
Vysoká	Citlivé	Informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit, např. pouze na organizaci příjemce informace využitím označení TLP:AMBER+STRICT. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER nebo TLP:AMBER+STRICT.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí musí být chráněny pomocí krypto-grafických prostředků. Zálohy by měly být zabezpečeny fyzicky nebo alespoň zahaslovány.
Kritická	Diskrétní	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	Pro ochranu důvěrnosti musí být využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabráňující zneužití informací ze

INTERNÍ TLP:GREEN

	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED, TLP:AMBER+STRICT nebo TLP:AMBER.	strany administrátorů. Přenosy informací musí být chráněny pomocí kryptografických prostředků.
--	--	---

3 Pravidla pro nakládání s aktivy

Všechny dokumenty musí být vypracovány v oficiálních šablonách ministerstva, které obsahují i označení informací. Původce informace je povinen vybrat označení podle příslušné kategorie. V případě nejasností může postup konzultovat s manažerem KB.

Pokud původce ani osoba odpovědná za dokument neurčí klasifikaci informace (případně není-li původce znám), rozhoduje o způsobu nakládání s ní manažer KB.

3.1 Minimální označování informací a médií

Tabulka 2: Minimální označování informací

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Označování dokumentů	Minimálně na poslední straně	Minimálně na první straně a poslední straně	Na všech stranách	Na všech stranách
Evidence počtu stránek	Neřízeno	Ve formátu: strana / počet stran	Ve formátu: strana / počet stran	Ve formátu: strana / počet stran
Verze dokumentu a jeho stav	Neřízeno	Na 1. straně	Na 1. straně	Na 1. straně
Označování elektronických dokumentů použitím metadat	Doporučeno	Doporučeno	Požadováno	Požadováno
Označování médií	Ne	Ano, je-li to možné, jinak musí být jednoznačně označen obsah po otevření média	Pouze oficiální média	Všechna média

3.2 Manipulace s aktivy

Tabulka 3: Popis opatření pro různé úrovně důvěrnosti

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Kopírování a skenování informací a aktiv	Neřízeno	Povoleno v rámci interních procesů	Jen se souhlasem původce aktiva	Jen původce aktiv nebo přímo pověřená osoba v rámci své pracovní náplně, všechny kopie musí být evidovány
Změna obsahu informace / aktiva	Neřízeno	Povoleno v rámci interních procesů, změna musí být evidována	Jen se souhlasem původce aktiva, změna musí být řízená	Jen původci aktiv nebo přímo pověřená osoba v rámci své pracovní náplně, změna musí být řízená

INTERNÍ TLP:GREEN

Sdílení informací a aktiv interně	Neřízeno	S kolegy v rámci organizace	S kolegy v rámci oddělení nebo pracovního týmu na principu need-to-know	Jen vybrané osoby s need-to-know
Sdílení informací a aktiv s externím subjektem	Neřízeno	Požadována dohoda o mlčenlivosti	Požadována dohoda o mlčenlivosti, sdílení informací jen ve smluvně definovaném rozsahu	Požadována dohoda o mlčenlivosti, sdílení informací jen ve smluvně definovaném rozsahu
Sdílení informací na jednáních a pracovních schůzkách	Neřízeno	Nevyužívat veřejné prostory	Účastníci vybráni na základě principu need-to-know	Přísně vybraní účastníci jednání
Předávání informací a aktiv prostřednictvím komunikačních sítí	Neřízeno	Skrze schválené nástroje	Informace musí být uloženy v adresáři s řízením přístupu přímo na to určeném	Informace musí být uloženy v adresáři s řízením přístupu a šifrováním, přímo na to určeném
Předávání informací a aktiv pomocí interní elektronické pošty	Neřízeno	Podpisový certifikát či šifrování	Informace nesmí být napsané v textu e-mailu, musí být uloženy v zašifrované příloze	Informace nesmí být napsané v textu e-mailu, musí být uloženy v zašifrované příloze, vyžadováno šifrování komunikace
Předávání informací a aktiv formou telefonického hovoru	Neřízeno	Nevyužívat veřejné prostory	V uzavřeném prostoru mimo doslech nepovolaných osob	Zakázáno
Ochrana návrhů dokumentů, pracovních poznámek apod.	Neřízeno	Neřízeno	Stejně jako u oficiálních dokumentů	Stejně jako u oficiálních dokumentů
Logické uložení informací a aktiv	Neřízeno	Ve služebním notebooku, na služební síti, na služebním paměťovém médiu	Ve služebním notebooku, na služební síti v přímo na to určeném adresáři, na šifrovaném služebním paměťovém médiu	Ve služebním notebooku na šifrovaném disku, na služební síti v přímo na to určeném adresáři, na šifrovaném služebním paměťovém médiu, data v šifrované podobě
Fyzické uložení informací a aktiv (ve formě dokumentu)	Neřízeno	V interní zóně, ve skřínce na chodbě nebo v kanceláři	V důvěrné zóně, v uzamykatelné skřínce v kanceláři	V důvěrné nebo kritické zóně, v trezoru nebo uzamykatelné plechové skříni v kanceláři nebo serverovně
Ukládání informací a aktiv mimo prostory organizace	Neřízeno	V uzamčeném prostoru	Pod nepřetržitým dohledem, např. v hotelovém trezoru apod.	Ukládání papírových dokumentů není přípustné, pro paměťová média jako pro „Citlivé“, je vyžadováno šifrování
Snížení klasifikačního stupně (o jednu úroveň)	Neřízeno	Souhlas původce aktiva	Souhlas původce aktiv a manažera KB	Souhlas původce aktiv a výboru KB

3.3 Správa vyměnitelných médií a datových nosičů

Tabulka 4: Správa výměnných médií

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Určení garanta vyměnitelného média nebo datového nosiče	Neřízeno	Pouze pro schválená média a nosiče využívané v rámci organizace (např. média pro zálohování)	Pouze pro schválená média a nosiče využívané v rámci organizace (např. média pro zálohování)	Pro všechna média a nosiče
Evidence vyměnitelných médií a datových nosičů	Neřízeno	Pouze pro schválená média a nosiče využívané v rámci organizace (např. média pro zálohování)	Pouze pro schválená média a nosiče využívané v rámci organizace (např. média pro zálohování)	Pouze pro schválená média a nosiče využívané v rámci organizace (např. média pro zálohování)
Řízení životnosti oficiálních médií a nosičů	Neřízeno	Vyžadováno (dle spisového a skartačního řádu)	Vyžadováno (dle spisového a skartačního řádu)	Vyžadováno (dle spisového a skartačního řádu)
Evidence pohybu médií a nosičů	Neřízeno	Neřízeno	Všechny nestandardní pohyby	Všechny pohyby
Ukládání vyměnitelných médií a datových nosičů v prostorách organizace	Neřízeno	Uvnitř fyzického bezpečnostního perimetru	Úschovný objekt uvnitř fyzického bezpečnostního perimetru	Úschovný objekt uvnitř fyzického bezpečnostního perimetru se zvýšenou úrovní ochrany
Ukládání vyměnitelných médií a datových nosičů mimo prostory organizace	Neřízeno	Uzamčená úschova, trezor, bezpečnostní schránka	Šifrování obsahu, uzamčená úschova, trezor, bezpečnostní schránka	Šifrování obsahu, pod neustálým dohledem zodpovědné osoby (která ji nosí s sebou)

4 Pravidla pro ochranu integrity

Tabulka 5: Pravidla pro ochranu integrity

Označování informací a médií	Popis opatření pro různé úrovně integrity			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Řízení přístupových práv	Neřízeno	Omezení práv na změnu	Vynucené omezení práv na změnu	Vynuceno striktní omezení práv na změnu a oddělení odpovědností
Omezení nežádoucích změn integrity informací a dat	Neřízeno	Aplikační kontroly	Vynucené aplikační kontroly	Vynucené aplikační kontroly, verifikace hashů
Princip čtyř očí	Neřízeno	Neřízeno	Neřízeno	Zohlednit při návrhu aplikace či při řízení procesu
Sledovatelnost změn	Neřízeno	Zaznamenání požadavků na změny	Požadováno zaznamenání požadavků na změny	Uložení alespoň 5 posledních změn každé datové položky
Evidence změn	Neřízeno	Zaznamenání požadavků na změny	Požadováno zaznamenání požadavků na změny	Požadováno zaznamenání požadavků na změny

5 Pravidla pro ochranu dostupnosti

Tabulka 6: Pravidla pro ochranu dostupnosti

Označování informací a médií	Popis opatření pro různé úrovně dostupnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Použitý režim pravidelného zálohování	Nejméně 1 za týden	Nejméně jednou za 24 hodin	Podle sjednaných požadavků, ale vždy nejméně jednou za 24 hodin	Podle sjednaných požadavků, ale vždy nejméně jednou za 12 hodin
Prověření použitelnosti provedených záloh	Jednou ročně náhodně vybrané části záloh	Jednou ročně celá sada záloh	Jednou za půl roku celá sada záloh	Jednou za čtvrt roku celá sada záloh
Existence plánů kontinuity činností	Neřízeno	Neřízeno	Všeobecné plány, případně podrobné plány na základě požadavků gestora nebo manažera KB	Požadovány podrobné plány kontinuity činností
Hloubka pravidelného testování plánů kontinuity činností	Neřízeno	Neřízeno	Teoretický nácvik nebo simulace obnovení důležitých prvků či dílčích činností	Integrovaná simulace obnovy nebo plný test obnovy, když je to možné, za účasti všech klíčových stran
Údržba plánů kontinuity činností	Neřízeno	Neřízeno	Každé 2 roky nebo do 6 měsíců po významné změně nebo testování plánů kontinuity činností	Každý rok nebo do 3 měsíců po významné změně nebo testování plánů kontinuity činností

6 Pravidla pro likvidaci dat

V případě úrovně důvěrnosti Nízká (Veřejné) a Střední (Interní) je za zvolenou metodu likvidace odpovědný garant aktiva. V případě úrovně důvěrnosti Vysoká (Citlivé) a Kritická (Diskrétní) je za zvolenou metodu likvidace odpovědný gestor aktiva. Do okamžiku předání média k likvidaci je za informace odpovědný garant nebo gestor aktiva dle příslušného stupně.

V případě, kdy je nosič informace předáván k likvidaci a obsahuje informace s označením Střední (Interní), Vysoká (Citlivé) nebo Kritická (Diskrétní), musí být o tomto předání vyhotoven protokol a uložen v souladu se spisovým řádem. Nosiče s označením Nízká (Veřejné) mohou likvidovat původci nebo garanti aktiv, ostatní aktiva musí být odborně zlikvidována.

V případě, že jsou nosiče informací používány pro více úrovní důvěrnosti aktiv, je nutné postupovat v souladu s nejvyšší úrovní, která se na nosiči nachází.

Následující tabulka definuje přípustné způsoby likvidace nosiče informace podle úrovně důležitosti aktiva.

Tabulka 7: Pravidla pro likvidaci dat

Typ nosiče informací	Přípustný způsob likvidace podle úrovně důvěrnosti aktiva			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Informace v listinné podobě (např. tištěné dokumenty, psané poznámky, ruční zápisy)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění informací.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.	
Mobilní a koncová zařízení (např. počítače, telefony, tablety, IoT, tiskárny)	Odstranění: Smazání dat, reset zařízení do továrního nastavení.	Přepsání: Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem. Pro zařízení s šifrovaným úložištěm – odstranění dat a reset do továrního nastavení. Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně).		Fyzická likvidace: Rozebrání zařízení a mechanické zničení nosiče informací.
Síťová zařízení (např. router, switch, modem)	Odstranění: Smazání dat, reset do továrního nastavení.			
Datová média (např. magnetické pásky, HDD, SSD, USB flash disk, paměťové karty)	Odstranění: Smazání dat	Přepsání: Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů.		Fyzická likvidace: Mechanické zničení nosiče informací
Přepisovatelná optická média (např. CD-RW, DVD-RW, BD-RE)	Odstranění: Smazání dat			

Nepřepisovatelná optická média (např. CD-R, DVD-R, BD-ROM)	Odstranění: Vyhození do odpadu.	Fyzická likvidace: Mechanické zničení nosiče informací.		
Virtuální úložiště a cloudové služby pod kontrolou organizace	Odstranění: Smazání dat z úložiště	Přepsání: Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů.		Fyzická likvidace: Mechanické zničení zařízení nebo nosiče informací
Technická aktiva mimo kontrolu organizace	Pokud jsou informace nebo nosiče mimo přímou kontrolu organizace (např. u dodavatele), musí být způsob likvidace stanoven smluvně a odpovídat úrovni aktiva.			
	Odstranění: Požadavek na dodavatele, aby data smazal běžným způsobem	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.	Fyzická likvidace: Při ukončení služby je provedena dokumentovaná celková sanitace všech použitých paměťových médií dodavatelem.
		V případě dedikovaného paměťového média dodavatel provede dokumentované přepsání dat		