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

Verze dokumentu			
Datum	**Verze**	**Změněno**	**Provedená změna**
18. 9. 2021	1.0	Manažer kybernetické bezpečnosti	Vytvoření dokumentu
1. 10. 2021	1.0	Výbor 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 certifikací senzorů 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 apod.).

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

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

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 provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s § 4 písm. h) – j) VKB.

Pravidla ochrany jednotlivých úrovní aktiv musí být minimálně 1x za 2 roky přezkoumána manažerem kybernetické bezpečnosti. 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. Pravidla pro klasifikaci informací doporučují postupy pro řízení dokumentace dle přílohy č. 5 bodu 1.1 písm. c) VKB.

Pomocí klasifikační tabulky budou uživatelé snadněji schopni rozhodnout o klasifikaci aktiva. V případě nejasností mohou rozhodnutí konzultovat s manažerem kybernetické bezpečnosti.

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: WHITE**.	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 sdílená 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.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí musí být chráněny pomocí kryptografických prostředků. Zálohy by měly být zabezpečeny fyzicky nebo alespoň zaheslovány.

Úroveň důvěrnosti	Klasifikace informací	Popis	Požadovaná bezpečnostní opatření
		V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP: AMBER**.	
Kritická	Diskrétní	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). 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** nebo **TLP: AMBER**	Pro ochranu důvěrnosti musí být využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití informací ze 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 klasifikace informací. Původce informace je povinen vybrat označení podle příslušné kategorie. V případě nejasností může postup konzultovat s manažerem kybernetické bezpečnosti.

V případě, že neurčí původce informace její klasifikaci, nebo není původce znám, a neučiní tak ani osoba za dokument odpovědná, rozhoduje manažer kybernetické bezpečnosti o způsobu nakládání s informací.

3.1 Minimální označování informací a médií

Tabulka 2: Minimální označování informací a médií

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: stránka X z Y	Ve formátu: stránka X z Y	Ve formátu: stránka X z Y
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 a jednoznačné označení obsahu po otevření média	Všechna média a jednoznačné označení obsahu po otevření média

3.2 Manipulace s aktivy

Tabulka 3: Manipulace s aktivy

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Kopírování a skenování aktiv	Neřízené	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 aktiva	Neřízené	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
Sdílení aktiv interně	Neřízené	S kolegy v rámci organizace	S kolegy v rámci oddělení nebo pracovního týmu	Jen vybraná skupina lidí
Sdílení 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	Je doporučeno nevyužívat veřejné prostory, kde se mohou nacházet nepovolané osoby	Účastníci vybráni na základě principu potřeba-znát (need-to-know)	Přísně vybraní účastníci jednání
Předávání aktiv prostřednictvím sítí	Neřízené	Povoleno v rámci interních procesů	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 aktiv pomocí interní elektronické pošty	Neřízeno	Doporučeno šifrování	Informace nesmí být napsané v textu e-mailu, musí být uložené v zašifrované příloze	Informace nesmí být napsané v textu e-mailu, musí být uložené v zašifrované příloze, vyžadováno šifrování komunikace

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Předávání aktiv formou telefonického hovoru	Neřízeno	Je doporučeno nevyužívat veřejné prostory	V uzavřeném prostoru mimo doslechu nepovolaných osob	Zakázáno
Ochrana návrhů dokumentů, pracovních poznámek apod.	Neřízeno	Neřízeno	Stejné jako u schválených a platných dokumen tů	Stejné jako u schválených a platných dokumentů
Logické uložení 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 aktiv (ve formě dokumentu)	Neřízeno	V interní zóně, ve skříince na chodbě nebo v kanceláři	V důvěrné zóně, v uzamykatelné skříince v kanceláři	V důvěrné nebo kritické zóně, v trezoru nebo uzamykatelné plechové skříni v kanceláři nebo serverovně
Ukládání aktiv mimo prostory organizace	Neřízeno	V uzamčeném prostoru	Pod nepřetržitým dohledem	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 kybernetické bezpečnosti	Souhlas původce aktiv a výboru KB

3.3 Správa výměnných médií

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 výměnného média	Neřízeno	Pouze pro schválená média využívaná v rámci organizace (např. média pro zálohování)	Pouze pro schválená média využívaná v rámci organizace (např. média pro zálohování)	Pro všechna média
Evidence vyměnitelných médií	Neřízeno	Pouze pro schválená média využívaná v rámci organizace (např. média pro zálohování)	Pouze pro schválená média využívaná v rámci organizace (např. média pro zálohování)	Pouze pro schválená média využívaná v rámci organizace (např. média pro zálohování)
Řízení životnosti oficiálních médií	Neřízeno	Vyžadováno (dle spisového a skartačního řádu)	Vyžadováno (dle spisového a skartačního řádu)	Vyžadováno (dle spisového a skartačního řádu)
Evidence pohybu médií	Neřízeno	Neřízeno	Všechny nestandardní pohyby	Všechny pohyby
Ukládání dokumentů a médií v prostorách organizace	Neřízeno	Uvnitř zóny standardní fyzické ochrany	Úschovný objekt uvnitř zón standardní fyzické ochrany	Úschovný objekt schválený organizací uvnitř zón zvýšené fyzické ochrany
Ukládání dokumentů a médií mimo prostory organizace	Neřízeno	Pod intenzivním dohledem, je doporučeno využívat hotelový trezor apod.	Pod nepřetržitým dohledem, je přijatelné uložení v hotelovém trezoru apod.	Ukládání papírových dokumentů není přípustné, pro paměťová média je vyžadováno šifrování

4 PRAVIDLA PRO OCHRANU INTEGRITY

Tabulka 5: Pravidla pro ochranu integrity

Označování informací a médií	Popis opatření pro různé úrovně důvěrnosti			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Řízení přístupových práv	Neřízeno	Doporučeno omezení práv na změnu	Požadováno omezení práv na změnu	Požadováno striktní omezení práv na změnu a oddělení odpovědností
Omezení náhodných změn	Neřízeno	Doporučené aplikační kontroly	Požadované aplikační kontroly	Požadované aplikační kontroly
Princip čtyř očí	Neřízeno	Neřízeno	Neřízeno	Doporučeno zohlednit při návrhu aplikace či při řízení procesu
Sledovatelnost změn	Neřízeno	Doporučeno zaznamenání požadavků na změny	Požadováno zaznamenání požadavků na změny	Uložení alespoň 5 posledních změn každé datové položky
Evidence změn	Neřízeno	Doporučeno 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 důvěrnosti			
	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	Neřízeno	Neřízeno	Všeobecné plány, případně podrobné plány na základě požadavků gestora nebo manažera kybernetické bezpečnosti	Požadovány podrobné plány
Hloubka pravidelného testování plánů kontinuity	Neřízeno	Neřízeno	Teoretický nácvik nebo simulace obnovení důležitých prvků či dílčích činnosti	Integrovaná simulace obnovy nebo plný test obnovy, když je to možné, za účasti všech klíčových stran
Údržba plánů kontinuity	Neřízeno	Neřízeno	Každé dva roky nebo do šesti měsíců po významné změně nebo testu kontinuity	Každý rok nebo do tří měsíců po významné změně nebo testu kontinuity

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 důvěrnosti aktiva.

Tabulka 7: Pravidla pro likvidaci dat

Nosič informace	Přípustný způsob likvidace podle úrovně důvěrnosti aktiva			
	Nízká	Střední	Vysoká	Kritická
	Veřejné	Interní	Citlivé	Diskrétní
Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění. Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.
Mobilní zařízení (mobilní telefony, tablety)	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.
Síťová zařízení (router, switch, modem a podobně)	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně).	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.
Kancelářské vybavení (scannery, tiskárny, fax)	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně).	x	x

<table>
<tr><th rowspan="3">Nosič informace</th><th colspan="4">Přípustný způsob likvidace podle úrovně důvěrnosti aktiva</th></tr>
<tr><th>Nízká</th><th>Střední</th><th>Vysoká</th><th>Kritická</th></tr>
<tr><th>Veřejné</th><th>Interní</th><th>Citlivé</th><th>Diskrétní</th></tr>
<tr><td>Magnetická média (magnetické pásky, disky, HDD)</td><td>Odstranění:
Smazání dat na úrovni souborového systému.</td><td>Přepsání:
Přepsání dat.
V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td>x</td><td>x</td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td><td>Odstranění:
Smazání dat na úrovni souborového systému.</td><td>Přepsání:
Přepsání dat.
V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td>Fyzická likvidace:
Zničení nosiče informací.</td><td>Fyzická likvidace:
Zničení nosiče informací.</td></tr>
<tr><td>Elektronická média (flash paměti)</td><td>Odstranění:
Smazání dat na úrovni souborového systému.</td><td>Fyzická likvidace.</td><td>Fyzická likvidace:
Zničení nosiče informací.</td><td>Fyzická likvidace:
Zničení nosiče informací.</td></tr>
<tr><td rowspan="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění:
Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání:
Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.

Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.</td><td>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.</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
</table>