Příloha č. 1

Klasifikace a ochrana informací

OBSAH

ČÁST I. ÚVODNÍ USTANOVENÍ

Kapitola 1 DEFINICE POJMŮ A ZKRATEK

Autorizace přístupu k informacím: proces udělení (v negativním případě odepření) přístupu k informacím.

Informační aktivum: jakákoli informace nebo prostředek pro práci s ní, který má pro MD nějakou hodnotu.

Informační systém (IS): informační infrastruktura, soustava aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací.

IS s řízeným přístupem: IS, v rámci něhož je řízený přístup uživatelů k aplikacím a informacím v závislosti na uživateli přidělené roli.

Integrita: zajištění důvěry v to, že informace nebyla neoprávněně změněna.

Klasifikace informací: proces, ve kterém je informaci přiřazen určitý stupeň klasifikace s ohledem na její význam pro MD.

Klasifikační stupně: škála, podle které se provádí klasifikace informací.

Nosič informací: médium, které slouží k ukládání a zpřístupnění informací uživatelům (např. papírová podoba, flash disk, CD nebo DVD disk, pevný disk počítače, a podobně).

„Potřebuje znát ke své práci“: princip, podle kterého je zaměstnancům a externím subjektům přidělován přístup k informacím (potřeba znát pro výkon pracovních povinností).

Zásada prázdného stolu: smyslem této zásady je zajistit rozumnou úroveň fyzické ochrany papírových dokumentů (resp. počítačových médií) zejména v době, kdy se s nimi dlouhodobě nepracuje (resp. se dlouhodobě nepoužívají).

Zpracovatel informace: zaměstnanec MD nebo externí subjekt, který z pověření vlastníka daného informačního aktiva zajišťuje zpracování informace v rámci jejího životního cyklu.

Uživatel informace: osoba, která je vlastníkem oprávněna k užívání informace**.**

Vlastník (garant) informace: vedoucí zaměstnanec, který odpovídá za zajištění rozvoje, použití a bezpečnosti informace.

Životní cyklus informace: vznik informace, manipulace s ní, archivace a likvidace informace.

Poznámka:
„Prázdný stůl“ není myšlen doslovně (v zásadě stačí zamykat při odchodu kancelář a nenechávat dokumenty volně dostupné na stole, v tiskárnách a podobně).

Kapitola 2 ROZSAH PŮSOBNOSTI

Tato příloha Bezpečnostní politiky MD (dále jen BPI MD) stanovuje základní pravidla, zásady a principy pro práci s informacemi v jakékoli podobě (mluvené slovo, papírová podoba, elektronická podoba). Řídí se jí všichni zaměstnanci MD. Externí subjekty jsou zavázány k plnění této přílohy smluvně.

ČÁST II. ROLE, ODPOVĚDNOSTI A PRAVOMOCI

Manažer KB:

- stanovuje požadavky na bezpečnou práci s informacemi a zajišťuje kontrolu jejich dodržování,
- řídí aktualizaci této přílohy.

Zaměstnanci chrání informace v rozsahu své působnosti před:

- neautorizovaným přístupem,
- neoprávněnou modifikací,
- zničením,
- vyzrazením.

Vlastník informace:

- klasifikuje informace (včetně případné změny klasifikace informace v závislosti na její aktuální hodnotě pro MD, nutnosti informaci zveřejnit a podobně),
- odpovídá za důvěryhodnost informace,
- dodržuje bezpečnostní požadavky na práci s informacemi v souladu s touto přílohou BPI MD a v případě potřeby i za určení požadavků na vyšší úroveň jejího zabezpečení,
- řídí přístup k informaci v souladu s principem „potřebuje znát ke své práci“.

Zpracovatel informace a uživatel informace zajišťuje dodržování bezpečnostních požadavků na práci s informací, stanovených jejím vlastníkem.

ČÁST III. KLASIFIKAČNÍ STUPNĚ A POŽADAVKY NA BEZPEČNOST

Kapitola 1 KLASIFIKAČNÍ STUPNĚ

Smyslem klasifikace informace je zajištění **odpovídající ochrany důvěrnosti** dané informace v celém jejím životním cyklu.

Pro tyto účely určí vlastník informace její klasifikační stupeň podle následující stupnice:

Tabulka 1: Stupnice pro klasifikaci informace (hodnocení důvěrnosti)

Klasifikační stupeň	Popis
CHRÁNĚNÉ	Informace, jejichž zveřejnění by mohlo závažným způsobem (s dlouhodobými důsledky) narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD značné finanční ztráty. Přístup k takové informaci se řídí principem „potřebuje znát ke své práci“.
PRO VNITŘNÍ POTŘEBU	Informace běžně používané pro vnitřní potřebu a pro výkon pracovních povinností na MD, jejichž zveřejnění by mohlo narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD finanční ztrátu. Přístup k takové informaci se řídí principem „potřebuje znát ke své práci“.
VEŘEJNÉ	Informace veřejně přístupné nebo určené ke zveřejnění. Narušení jejich důvěrnosti neznamená žádnou újmu MD. Neuplatňuje se u nich princip „potřebuje znát ke své práci“.

Každou informaci navíc, zejména pro potřeby analýzy rizik, ohodnotí její vlastník z pohledu dostupnosti a integrity podle níže uvedených stupnic:

Tabulka 2: Stupnice pro hodnocení dostupnosti

Stupeň	Popis
VYSOKÝ	Porušení dostupnosti informací by mohlo závažným způsobem (s dlouhodobými důsledky) narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD značné finanční ztráty.
STŘEDNÍ	Informace běžně používané pro vnitřní potřebu a pro výkon pracovních povinností na MD, u nichž by porušení dostupnosti mohlo narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD finanční ztrátu.
NÍZKÝ	Porušení dostupnosti takovýchto informací nemůže nijak narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD finanční ztrátu.

Tabulka 3: Stupnice pro hodnocení integrity

Stupeň	Popis
VYSOKÝ	Porušení integrity informací by mohlo závažným způsobem (s dlouhodobými důsledky) narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD značné finanční ztráty.
STŘEDNÍ	Informace běžně používané pro vnitřní potřebu a pro výkon pracovních povinností na MD, u nichž by porušení integrity mohlo narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD finanční ztrátu.
NÍZKÝ	Porušení integrity takovýchto informací nemůže nijak narušit fungování MD, poškodit dobré jméno MD nebo způsobit MD finanční ztrátu.

Kapitola 2 KLASIFIKACE INFORMACÍ ZÁVAZNÝCH PRÁVNÍCH PŘEDPISŮ

V níže uvedené tabulce je uveden základní přehled právních předpisů, souvisejících s ochranou informací, popis informací, na které se daný právní předpis vztahuje a slouží jako základní vodítko pro jejich klasifikaci.

Tabulka 2: Základní přehled právních předpisů

Předpis	Druh informace	Popis	Klasifikační stupeň
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (resp. nařízení GDPR)	OSOBNÍ ÚDAJE	Jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.	PRO VNITŘNÍ POTŘEBU
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (resp. nařízení GDPR)	CITLIVÉ OSOBNÍ ÚDAJE (resp. ZVLÁŠTNÍ OSOBNÍ ÚDAJE podle GDPR)	Osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.	Pole povahy a požadavků MD: PRO VNITŘNÍ POTŘEBU až CHRÁNĚNÉ

Předpis	Druh informace	Popis	Klasifikační stupeň
Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů	ZVLÁŠTNÍ SKUTEČNOSTI	Informace týkající se analýz rizik a plánu jejich zvládání, pokud tyto informace nejsou utajovanými informacemi ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti	Pole povahy a požadavků MD: PRO VNITŘNÍ POTŘEBU až CHRÁNĚNÉ
Zákon č. 89/2012 Sb., občanský zákoník	OBCHODNÍ TAJEMSTVÍ	Konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.	Pole povahy a požadavků MD: PRO VNITŘNÍ POTŘEBU až CHRÁNĚNÉ

Kapitola 3 MANIPULACE S INFORMACEMI A JEJICH OZNAČOVÁNÍ

Při vzniku informace nebo při jejím převzetí od externího subjektu vlastník informace rozhodne podle definice klasifikačních stupňů o úrovni její klasifikace a tím i o způsobu její ochrany. Pokud má k tomu důvod, může požadovat ochranu, která jde nad rámec ochrany definované v této příloze.

Klasifikační stupeň „PRO VNITŘNÍ POTŘEBU“ je základní stupeň klasifikace informací. Nevyžaduje-li informace zvýšenou ochranu nebo není-li jednoznačně stupně „VEŘEJNÉ“ (její případné zveřejnění nepůsobí MD žádnou újmu), musí být klasifikována jako „PRO VNITŘNÍ POTŘEBU“. Pokud není informace nijak označena, považuje se za informaci stupně „PRO VNITŘNÍ POTŘEBU“.

Pro každý klasifikační stupeň jsou níže definována pravidla, zásady a principy pro manipulaci s nimi. Výjimka z těchto pravidel, zásad a principů je možná v případě, že obecně závazný právní předpis stanoví jinak nebo v případě rozhodnutí vlastníka informace, který za toto rozhodnutí nese odpovědnost.

3.1 Informace v ústní podobě

Tabulka 3: Informace v ústní podobě

	CHRÁNĚNÉ	PRO VNITŘNÍ POTŘEBU	VEŘEJNÉ
Přenos mluveným slovem	Je nutné mít pod kontrolou okolí, ve kterém člověk hovoří. Pokud to je možné, je nutné využít prostředky fyzické ochrany, případně vhodné technické prostředky (místnost chráněná proti odposlechu).	Je nutné mít pod kontrolou okolí, ve kterém člověk hovoří.	Bez požadavků.

3.2 Informace v papírové podobě

Tabulka 4: Informace v papírové podobě

	CHRÁNĚNÉ	PRO VNITŘNÍ POTŘEBU	VEŘEJNÉ
Označování	V zápatí každé strany textem „Bezpečnostní klasifikace dokumentu: CHRÁNĚNÉ“.	V zápatí každé strany textem „Bezpečnostní klasifikace dokumentu: PRO VNITŘNÍ POTŘEBU“. Neoznačený dokument je implicitně chápán jako „PRO VNITŘNÍ POTŘEBU“.	Označení se nevyžaduje, pokud je z charakteru dokumentu nebo z jeho obsahu všem zcela zřejmé, že se jedná o dokument určený ke zveřejnění, resp. byl jednoznačně uskutečněn akt jeho zveřejnění. V ostatních případech je potřeba dát na vědomí, že se jedná o veřejnou informaci tím, že je dokument v zápatí každé strany označen textem „VEŘEJNÉ“.
Kopírování	Kopírování je možné pouze se souhlasem vlastníka. Kopie ani originály nesmějí být ponechávány bez dozoru, musí být číslovány a musí obsahovat rozdělovník.	Nenechávat bez dozoru v kopírce, pokud je na veřejně přístupném místě. Ke kopírování není nutný souhlas vlastníka.	Bez požadavků.
Posílání poštou nebo kurýrem	V zalepené obálce, bez označení stupně klasifikace, bude vložena obálka s označením "CHRÁNĚNÉ – pouze do vlastních rukou xx“. "CHRÁNĚNÉ" dokumenty je nutné posílat vždy do vlastních rukou.	V zalepené obálce.	V zalepené obálce.
Skartace	Fyzické zničení musí být provedeno a musí být o něm proveden záznam.	Jakékoli fyzické zničení.	Bez požadavků.
Ukládání dokumentů	V uzamykatelných skříních nebo zásuvkách a kontejnerech.	V uzamčené kanceláři při dodržování zásady prázdného stolu.	Bez požadavků.
Přístup k dokumentům	Přístup musí být definován rozdělovníkem. Dokumenty jsou přebírány výhradně proti podpisu.	Všem zaměstnancům MD (resp. externím subjektům) na základě principu „potřebuje znát ke své práci“.	Bez požadavků.

3.3 Informace v elektronické podobě

Tabulka 5: Informace v elektronické podobě

	CHRÁNĚNÉ	PRO VNITŘNÍ POTŘEBU	VEŘEJNÉ
Označení informace	V zápatí šablony dokumentu textem „Bezpečnostní klasifikace dokumentu: CHRÁNĚNÉ“ a názvem „Název „CHRÁNĚNÉ“ v souborové struktuře paměťových médií, pokud to způsob zpracování informace dovoluje. Pokud to způsob zpracování nedovoluje, musí náhradní způsob schválit Manažer KB.	V zápatí šablony dokumentu textem „Bezpečnostní klasifikace dokumentu: PRO VNITŘNÍ POTŘEBU“ Neoznačený dokument je implicitně chápán jako „PRO VNITŘNÍ POTŘEBU“.	Pokud to způsob zpracování informace dovoluje – textem v zápatí šablony dokumentu a názvem „Název „VEŘEJNÉ“ v souborové struktuře paměťových médií.
Označení média nebo nosiče informace	Štítkem s textem „Bezpečnostní klasifikace: CHRÁNĚNÉ“.	Štítkem s textem: „Bezpečnostní klasifikace dokumentu: PRO VNITŘNÍ POTŘEBU“ Neoznačený dokument je implicitně chápán jako „PRO VNITŘNÍ POTŘEBU“.	Štítkem s textem „VEŘEJNÉ“.
Způsob uložení informace na přenosných záznamových médiích společně s dalšími informacemi	Je nutné šifrování šifrovacím algoritmem schváleným Manažerem KB. Ukládání je povoleno pouze na zařízeních určených k tomuto účelu.	Šifrování není povinné, ale je doporučeno šifrování běžně dostupnými prostředky[1]. Ukládání je povoleno pouze na zařízeních přidělených pro výkon pracovních povinností.	Bez požadavků.
Způsob uložení informace na noteboocích	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Bez požadavků.
Způsob uložení informace na mobilních zařízeních (mobilní telefon, tablety atd.)	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Bez požadavků.
Výměna dat s využitím veřejného úložiště	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Je nutné šifrování šifrovacím algoritmem schválených Manažerem KB.	Je možné využít libovolné veřejné úložiště.
Způsob uložení informace v IS MD s řízeným přístupem	Výhradně na základě postupu, dohodnutého s Manažerem KB.	Bez požadavků.	Bez požadavků.
Způsob uložení informace v IS MD bez řízeného přístupu	Výhradně na základě postupu, dohodnutého s Manažerem KB.	Šifrování není povinné, ale je doporučeno šifrování běžně dostupnými prostředky[2].	Bez požadavků.

[1] Např. heslem v ZIP souboru. Heslo musí být doručeno jiným distribučním kanálem, např. formou SMS.

[2] Např. heslem v ZIP souboru. Heslo musí být doručeno jiným distribučním kanálem, např. formou SMS.

	CHRÁNĚNÉ	PRO VNITŘNÍ POTŘEBU	VEŘEJNÉ
Přístup k informaci, včetně jejího kopírování a mazání v IS MD	Vlastník určuje práva pro čtení, zápis a případné kopírování pro jednotlivé uživatele (sám nebo dává pokyn zpracovateli informace). Mazání musí probíhat se souhlasem vlastníka a způsobem schváleným Manažerem KB.	Vlastník určuje práva pro čtení a zápis (sám nebo dává pokyn zpracovateli informace). Je povoleno mazání běžným způsobem, ale pouze se souhlasem vlastníka.	Čtení se povoluje pro všechny, mazání je povoleno pouze se souhlasem vlastníka.
Tisk	Tisk provádí pouze vlastník na tiskárně, která je pod přímým dohledem nebo umožní vytisknutí až po zadání hesla. Při tisku je vlastník odpovědný za její dokončení a odebrání výstupu z tiskárny.	Při tisku je autor tiskové úlohy odpovědný za neodkladné odebrání výstupu z tiskárny.	Bez požadavků.
Likvidace elektronických médií	Fyzické zničení musí být provedeno způsobem, schváleným Manažerem KB a musí být o něm proveden záznam.	Jakékoli fyzické zničení.	Bez požadavků.
Auditování přístupu k IS	Logují se veškeré pokusy o přístup v úložištích určených pro „CHRÁNĚNÉ“ dokumenty.	Bez požadavků, pokud obecně závazné právní předpisy nestanoví jinak.	Bez požadavků.
Auditní záznamy	Zálohy auditních záznamů se archivují po dobu stanovenou obecně závaznými právními předpisy[3], minimálně však po dobu 12 měsíců.	Bez požadavků, pokud obecně závazné právní předpisy nestanoví jinak.	Bez požadavků.
Posílání faxem	Zakázáno.	Pouze při zajištění dohledu adresáta nad přijetím faxu.	Bez požadavků.
Síťové prostředí MD	Je na zvážení vlastníka, zda ho bude vyžadovat.	Bez požadavků.	Bez požadavků.
Posílání kurýrní službou nebo poštou	Na datovém médiu v zašifrované podobě (šifrovacím algoritmem schváleným Manažerem KB). Zásilka nesmí obsahovat použité šifrovací klíče.	V zalepené obálce.	V zalepené obálce.
Posílání e-mailem	Je nutné šifrování šifrovacím algoritmem schváleným Manažerem KB; odesílatel si vyžádá potvrzení o přijetí.	V rámci IS MD nejsou vyžadována žádná opatření. Informace předávané mimo MD musí být šifrovány běžně dostupnými prostředky[4].	Bez požadavků.
Telefonování a SMS	Zakázáno.	Je nutné mít pod kontrolou okolí, ve kterém člověk hovoří nebo přijímá SMS.	Bez požadavků.

ČÁST IV. PŘECHODNÁ USTANOVENÍ

Do doby zajištění technických prostředků a podmínek pro klasifikaci a ochranu informací je nutné postupovat v co největší možné míře souladu s touto přílohou BPI MD.

[3] Předpisy v oblasti bankovnictví, účetnictví, ochrany osobních údajů a podobně.

[4] Např. heslem v ZIP souboru. Heslo musí být doručeno jiným distribučním kanálem, např. formou SMS.